REPORT SULLE MINACCE INFORMATICHE

Giugno 2024

Informazioni raccolte dalla rete globale di esperti, sensori, dati di telemetria e Threat Intelligence

CONTENUTI:

Cambiamenti rapidi e significativi del panorama APT

L'ecosistema ransomware sconvolto da LockBit

Ampliamento dell'arsenale degli autori degli attacchi

Presentato da

Trellix ADVANCED RESEARCH CENTER

Uno strumento di elusione specifico è stato usato con successo per bloccare le funzionalità EDR (Endpoint Detection and Response) di un'azienda del tuo settore.

La corsa alla sicurezza informatica per impedire l'utilizzo di strumenti di sicurezza legittimi a fini dolosi è sempre più complicata.

In qualità di CISO, devi dimostrare agilità, rapidità, fiducia e controllo. Il tuo CEO e il tuo consiglio di amministrazione desiderano saperne di più sui tuoi strumenti di allerta e registrazione. Incarichi il tuo team di identificare le vulnerabilità e hai un piano per correggerle.

La corsa alla sicurezza informatica è un vero e proprio triathlon, in cui le discipline sono SecOps, tecnologie e Threat Intelligence. La corsa è iniziata, e la resistenza è fondamentale.

> Se i meccanismi di difesa sono sempre più sofisticati, gli strumenti e le tattiche d'attacco dei criminali informatici e dei gruppi sponsorizzati dagli Stati non sono da meno.

REPORT SULLE MINACCE INFORMATICHE

Redatto dal nostro team Trellix Advanced Research Center, questo rapporto (1) mette in evidenza gli approfondimenti, la Threat Intelligence e i consigli raccolti da molte fonti di dati critici sulle minacce alla sicurezza informatica e (2) propone interpretazioni esperte, razionali e ragionevoli di tali dati per informare e favorire le migliori pratiche per la difesa informatica. Questa edizione si concentra sulle informazioni e sui dati acquisiti fra il 1° ottobre 2023 e il 31 marzo 2024.

1. Cambiamenti rapidi e significativi del panorama APT
2. L'ecosistema ransomware sconvolto da LockBit
3. Comparsa degli strumenti di disattivazione dell'EDR
4. Truffe sul tema delle elezioni presidenziali americane
5. L'IA generativa e il mercato clandestino dei criminali informatici

PREMESSA

La Threat Intelligence operativa e la capacità di contestualizzare le minacce globali in funzione del tuo ambiente aziendale non sono mai state più importanti per il ruolo del CISO.

Dovendo fare di più con meno, i CISO e i loro team SecOps hanno bisogno della Threat Intelligence per anticipare le minacce, identificare quelle che più probabilmente prenderanno di mira la loro azienda e prepararsi, allineare i programmi e il budget alle minacce e ai criminali informatici più pertinenti e, infine, passare da un approccio reattivo a uno proattivo.

In qualità di "cliente zero" di Trellix, ritengo che le informazioni rilevanti sulle minacce abbiano, più che mai, il potenziale maggiore per trasformare il modo in cui i team di risposta agiscono e creano le loro strategie.

Consulta queste informazioni, assimilale e tienine conto nella tua pianificazione strategica, razionalizzazione del budget e supporto operativo. Mi auguro che queste informazioni ti saranno utili e ti permettano di indirizzare meglio la tua pianificazione, preparazione e difesa contro le minacce APT.

Harold Rivas
CISO, TRELLIX

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

PREFAZIONE

Questo report ha l'obiettivo di strutturare la nostra Threat Intelligence e di contestualizzare ciò che osserviamo.

Il panorama

Gli ultimi sei mesi sono stati incredibili: il perdurare della policrisi ha accelerato le attività dei criminali informatici a livello globale. Abbiamo osservato dei cambiamenti radicali nei comportamenti, tra cui:

- L'ecosistema ransomware è atipico a seguito di diverse operazioni delle forze dell'ordine
- I gruppi autonomi stanno vendendo i loro test di penetrazione e i loro metodi di attacco alternativi ai gruppi di ransomware
- La guerra in Israele ha innescato attacchi e attivismo informatico sponsorizzati dagli Stati
- I criminali informatici cercano di essere più sofisticati e hanno accesso a strumenti basati sull'IA generativa economici o gratuiti che permettono loro di diventare velocemente esperti
- Gli strumenti di elusione e disattivazione dell'EDR sono sempre più diffusi tra i criminali informatici

Un gioco del gatto col topo

Data la più ampia adozione dell'EDR (Endpoint Detection and Response), il gioco del gatto col topo che è la sicurezza informatica si fa più complesso. L'aumento del numero di criminali informatici che utilizzano strumenti dannosi per neutralizzare le soluzioni EDR ha catturato il nostro interesse perché rappresenta un cambio di rotta netto dall'uso dei tradizionali strumenti basati su malware.

Come responsabili della difesa, dobbiamo cambiare rotta anche noi. Le soluzioni EDR si sono dimostrate efficaci nel rilevamento di ransomware, malware e attività APT: ma se vengono disattivati, cosa devono fare un'azienda e il suo CISO? Devono disporre di registrazioni, sistemi di avviso e Threat Intelligence operativa per avere visibilità sui comportamenti anomali nel loro ambiente. È chiaramente necessario elevare il livello di gioco.

Trellix lavora in modo coscienzioso per condividere le informazioni sulle minacce con la comunità della sicurezza - uno dei nostri valori fondamentali per mantenere il vantaggio sui criminali informatici - e tracciare le campagne e i gruppi criminali su larga scala.

Il panorama è più che mai mutevole. Il nostro obiettivo è supportare i nostri clienti e il settore in generale fornendo loro le informazioni necessarie per migliorare le loro difese, creare contromisure e identificare le vulnerabilità.

In questo gioco del gatto col topo, dobbiamo giocare per vincere.

John Fokker
DIRETTORE DELLA THREAT INTELLIGENCE, TRELLIX

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

INTRODUZIONE: REPORT SULLE MINACCE INFORMATICHE: GIUGNO 2024

L'impatto degli eventi geopolitici sul dominio informatico

Le ricerche condotte da Trellix Advanced Research Center dal 1° ottobre 2023 al 31 marzo 2024 hanno rivelato un cambiamento delle attività legate alle minacce, con un evidente aumento delle minacce informatiche con motivazioni geopolitiche. Importanti eventi a livello regionale e globale - come esercitazioni militari, summit politici o economici e elezioni - hanno accelerato le attività delle minacce informatiche.

Gli analisti di Trellix pensano sia probabile che i criminali informatici si siano concentrati su questi eventi per acquisire informazioni rilevanti sulle loro controparti, sondare le reti in modo proattivo per alimentare la loro consapevolezza della situazione o per infiltrarsi sulle reti IT in modo strategico in vista di attacchi futuri.

- **Incontro tra i presidenti Biden e Xi a San Francisco:** nel novembre 2023, i dati di telemetria di Trellix hanno rilevato un aumento delle attività dannose dei gruppi APT affiliati alla Cina solo pochi giorni prima dell'incontro tra il presidente degli Stati Uniti Biden con il suo omologo cinese Xi Jinping a San Francisco in occasione del summit della Cooperazione economica per l'Asia- Pacifico (APEC). Il numero di attività legate alle minacce è diminuito in modo significativo a seguito dell'incontro Biden-Xi e durante il summit.

  Al termine dell'evento, il livello di minaccia è sceso al minimo a novembre 2023. Questa evoluzione delle attività delle minacce da parte di gruppi di criminali informatici affiliati alla Cina sembra suggerire che tali gruppi siano fortemente influenzati dagli eventi geopolitici come il summit dell'APEC. È anche possibile che i gruppi APT associati alla Cina possono aver deliberatamente sospeso la loro attività di pirateria durante un importante evento politico, probabilmente per preservare la loro immagine pubblica e la loro reputazione internazionale.
- **Guerra tra Israele e Hamas:** le minacce da parte dei gruppi di criminali informatici APT affiliati all'Iran sono state rafforzate anche dagli sviluppi politici relativi alla guerra tra Israele e Hamas. Negli Stati Uniti, i dati di telemetria globali di Trellix mostrano picchi periodici di attività dannose da parte dei gruppi APT affiliati all'Iran negli ultimi sei mesi (con l'eccezione di fine novembre e dicembre 2023). Nello specifico, i nostri dati di telemetria globali mostrano un calo dell'attività delle minacce da parte dei gruppi APT legati all'Iran che prendono di mira aziende statunitensi durante i periodi di scambio di ostaggi e accordi di cessate il fuoco con Israele a fine novembre 2023 e nel dicembre 2023, quando gli Stati Uniti hanno fatto pressione per un cessate il fuoco umanitario nella striscia di Gaza, dato che l'Iran sostiene apertamente Hamas. Inoltre, i dati di telemetria globali di Trellix indicano che i gruppi APT legati all'Iran hanno utilizzato diverse TTP, tra cui phishing, stealer di informazioni, backdoor, strumenti di download, webshell dannose e vulnerabilità comunemente sfruttate per colpire le aziende in Israele durante il periodo considerato.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- **Esercitazioni militari:** inoltre, le esercitazioni militari multinazionali per migliorare la preparazione ai combattimenti possono innescare un aumento delle attività dannose. Nel marzo 2024, i dati di telemetria globali di Trellix hanno mostrato picchi ripetuti nelle attività delle minacce in Corea del Sud durante le esercitazioni militari congiunte tra Stati Uniti e Corea del Sud su larga scala, note come Freedom Shield, che si sono tenute tra il 4 marzo e il 14 marzo. Queste esercitazioni militari sono studiate per riflettere il teatro delle operazioni coreane e contrastare la crescente minaccia nucleare della Corea del Nord. Nello specifico, i rilevamenti di minacce in Corea del Sud hanno superato i 150.000 il 7 e il 13 marzo 2024, rispettivamente, vale a dire circa sette volte i 20.000 rilevamenti quotidiani usuali nel Paese.
- **Guerra tra Russia e Ucraina:** Il proseguimento della guerra cinetica nella regione è stata affiancata da iniziative informatiche di diversa grandezza. In particolare, criminali informatici affiliati alla Russia hanno sfruttato dei malware wiper nuovi e più avanzati per cancellare migliaia di server e PC virtuali attaccando l'operatore di servizi di telecomunicazioni ucraino Kyivstar. L'attacco contro Kyivstar è uno degli attacchi informatici a impatto più elevato in Ucraina dall'invasione da parte della Russia nel 2022.

Fatti salienti delle minacce in breve

Sebbene questo report metta in evidenza le ricerche condotte da Trellix, ci sono temi chiave che rimangono costanti:

1. **Cambiamenti rapidi e significativi del panorama APT**
    a. **Il collettivo Sandworm, affiliato alla Russia, intensifica le sue attività:** con l'inasprirsi delle tensioni geopolitiche, aumenta anche l'attività delle minacce APT all'interno dell'intero ecosistema. Se le minacce APT crescono complessivamente, il team Sandworm legato alla Russia è stato rilevato molto più frequentemente (+40%) nel periodo preso in considerazione in questo report.
    b. **La Cina rimane prolifica:** i gruppi di criminali informatici legati alla Cina si confermano gli autori più prolifici di minacce APT. Trellix ha infatti osservato più di 21 milioni di rilevamenti provenienti da gruppi di criminali informatici affiliati alla Cina. Oltre il 23% dei rilevamenti di attività dannose è indirizzato contro il settore della pubblica amministrazione in tutto il mondo.
    c. **Aumento delle attività di Volt Typhoon:** gruppo APT finanziato dalla Cina relativamente nuovo, Volt Typhoon si distingue per il suo schema di comportamento e per le pratiche per individuare gli obiettivi unici. A partire da metà gennaio 2024, i dati di telemetria di Trellix hanno rilevato oltre 7.100 attività dannose associate a Volt Typhoon, con picchi periodici tra gennaio e marzo 2024.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

2. **L'ecosistema ransomware sconvolto da LockBit**
    a. **Impostori influenzano la reputazione delle bande:** a seguito di un'azione di una task force che riuniva le forze dell'ordine di diversi paesi, Operation Cronos, Trellix ha rilevato degli impostori che si facevano passare per LockBit, mentre il gruppo cercava febbrilmente di salvare la faccia e ripristinare la loro operazione redditizia.
    b. **Gli Stati Uniti rimangono il Paese più bersagliato:** gli Stati Uniti si confermano i più colpiti dai gruppi ransomware, seguiti da Turchia, Hong Kong, India e Brasile.
    c. **Il settore trasporti e spedizioni è il più colpito:** i ransomware si sono concentrati maggiormente sul settore trasporti e spedizioni nel quarto trimestre 2023 e nel primo trimestre 2024. Il settore ha generato il 53% e il 45% dei rilevamenti globali di ransomware, rispettivamente, seguito dal settore finanziario.
    d. **Un intervento delle forze dell'ordine porta a una condanna:** prima della finalizzazione di questo report, le forze dell'ordine a livello globale hanno rivelato la reale identità del capobanda di LockBit. Ulteriori azioni contro i criminali che operano il ransomware sono state condotte il 1° maggio. Un affiliato del gruppo REvil, che ha attaccato Kaseya e molte altre aziende, è stato condannato a 13 anni di prigione e al risarcimento di 16 milioni di dollari.
3. **Comparsa degli strumenti di disattivazione dell'EDR**
    a. **Comparsa della banda ransomware D0nut:** la comparsa della banda ransomware D0nut è stata particolarmente degna di nota per il suo innovativo utilizzo di uno strumento di disattivazione delle soluzioni EDR, una tattica avanzata per eludere il rilevamento sugli endpoint e migliorare l'efficacia degli attacchi.
    b. **Lo strumento di elusione dei sistemi EDR Spyboy utilizzato per colpire il settore delle telecomunicazioni:** uno strumento di disattivazione delle soluzioni EDR "Terminator" sviluppato da Spyboy è stato utilizzato in una nuova campagna a gennaio 2024. Lo strumento viene utilizzato per eludere le soluzioni EDR e l'80% dei rilevamenti erano rivolti contro il settore delle telecomunicazioni.
4. **Truffe sul tema delle elezioni presidenziali americane**
    a. **Il phishing rimane diffuso:** mentre tutto il mondo è in attesa di conoscere l'esito delle elezioni presidenziali degli Stati Uniti a novembre, abbiamo iniziato a osservare truffe a tema elettorale studiate per spingere i cittadini a fare donazioni.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

5. **L'IA generativa e il mercato clandestino dei criminali informatici**
    a. **Strumenti gratuiti basati sull'IA:** uno strumento Jabber gratuito basato su ChatGPT 4.0 e disponibile nel mercato clandestino della criminalità informatica permette allo sviluppatore di aiutare i criminali informatici a sfruttare l'IA generativa nelle loro operazioni e creare una knowledge base alimentata dall'IA generativa per apprendere da altri gruppi di criminali informatici o addirittura rubare le loro idee e strumenti.
    b. **Aumento dell'adozione di infostealer:** abbiamo osservato i criminali informatici utilizzare due infostealer (strumenti per l'esfiltrazione di informazioni) con funzionalità basate sull'IA generativa. MetaStealer e LummaStealer sfruttano l'IA generativa rispettivamente per eludere il rilevamento e individuare i bot nell'elenco dei registri. Grazie alle funzionalità di IA generativa queste tattiche criminali sono difficili da individuare e da bloccare.

Metodologia: come raccogliamo e analizziamo i dati

Gli esperti del nostro team Trellix Advanced Research Center raccolgono le statistiche, le tendenze e i risultati delle analisi che compongono questo report da un'ampia gamma di fonti globali, sia bloccate sia aperte. I dati aggregati alimentano le nostre piattaforme Insights e ATLAS. Sfruttando l'apprendimento automatico, l'automazione e l'acutezza umana, il team svolge una serie di processi intensivi, integrati e iterativi per normalizzare i dati, analizzare le informazioni e sviluppare approfondimenti significativi per i responsabili della sicurezza informatica e i team SecOps, in prima linea contro le minacce in tutto il mondo. Per una descrizione più dettagliata della nostra metodologia, vedere in fondo a questo report.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

SEGNALAZIONI, DATI E ANALISI

Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)

Tra ottobre 2023 e marzo 2024, Trellix ha osservato un aumento del 17% dei rilevamenti di minacce APT rispetto ai sei mesi precedenti. Nel nostro ultimo report riportavamo già un impressionante aumento del 50% di questi rilevamenti. L'ecosistema di APT è sostanzialmente diverso rispetto a un anno fa: è più aggressivo, ingegnoso e attivo.

Nel panorama delle minacce informatiche in rapida evoluzione, i gruppi APT continuano a rappresentare una sfida importante e sofisticata per la sicurezza informatica globale.

Il nostro obiettivo è analizzare a fondo le attività associate alle minacce APT (Advanced Persistent Threat) rilevate tra il quarto trimestre 2023 e il primo trimestre 2024. Questa analisi si concentra sulle origini di queste minacce, i loro principali obiettivi e gli strumenti utilizzati nelle loro operazioni. Mettiamo a confronto questi risultati con i dati raccolti nella prima metà del 2023 (secondo e terzo trimestre) utilizzando due metriche fondamentali: varianza percentuale e varianza del contributo proporzionale.

- Varianza percentuale: questo parametro ci aiuta a capire se l'attività di un gruppo APT specifico, la presa di mira di alcuni Paesi o l'utilizzo di strumenti particolari è aumentato, diminuito o rimasto invariato nel tempo. In questo modo possiamo tracciare l'evoluzione dei comportamenti di questi criminali informatici e come il panorama complessivo delle minacce informatiche si evolve.
- Varianza del contributo percentuale: questo parametro aggiunge contesto e non si limita a mostrare l'evoluzione grezza delle attività, ma mostra come questa evoluzione si colloca sullo sfondo dell'intero ambiente delle minacce informatiche. Per esempio, anche se i rilevamenti di un particolare criminale informatico sono aumentati in modo significativo, può essere che rappresenti solo una piccola parte del numero totale delle minacce informatiche se l'ambiente delle minacce complessivo è diventato più attivo. Al contrario, se i rilevamenti di questo criminale informatico sono diminuiti, ma il resto dell'ambiente delle minacce ha subito un rallentamento ancora maggiore, è possibile che l'importanza relativa di questo criminale aumenti.

Utilizzando questi parametri, desideriamo fornire un quadro sfumato degli sviluppi delle attività APT, il che ci permette di trarre spunti di riflessione relativi ai loro obiettivi strategici, le metodologie preferite e le sfide della sicurezza informatica che pongono. Le seguenti sezioni analizzano questi risultati, facendo luce sull'intricato mondo delle APT e gli sforzi continui richiesti per offrire protezione contro le loro minacce sofisticate.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

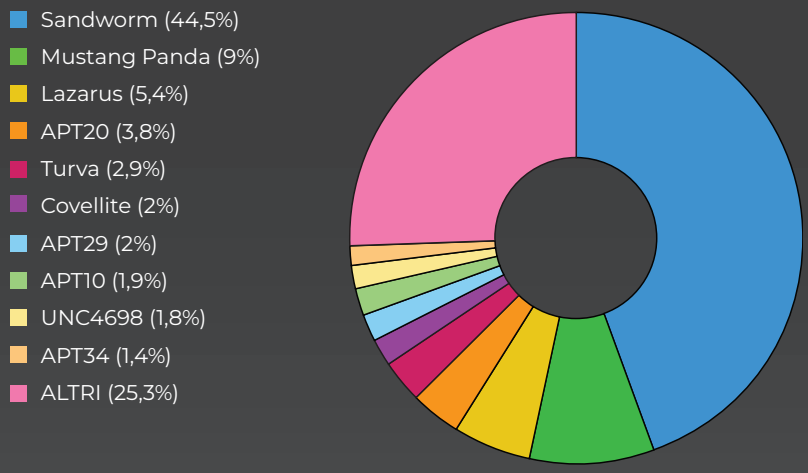
Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Gruppi sponsorizzati dagli Stati e APT attivi

Inoltre, il periodo che va dall'ottobre 2023 a marzo 2024 è stato testimone di oscillazioni significative delle attività dei vari gruppi APT. Queste oscillazioni non solo sottolineano la natura dinamica delle minacce informatiche ma evidenziano anche cambiamenti del focus operativo e delle tecniche utilizzate da questi criminali sofisticati.

I 10 GRUPPI APT PIÙ ATTIVI IN BASE AI RILEVAMENTI TRA IL 4° TRIMESTRE DEL 2023 E IL 1° TRIMESTRE DEL 2024.



EVOLUZIONE DELLE ATTIVITÀ DEI GRUPPI DI CRIMINALI INFORMATICI: VARIANZA E CONTRIBUTO PROPORZIONALE

Minacce APT	Varianza percentuale	Varianza del contributo percentuale
Sandworm	1.669,43%	40,34%
Mustang Panda	-2,19%	-6,14%
Lazarus	66,87%	0,07%
APT28	18,67%	-1,49%
Turla	2,95%	-1,74%
Covellite	85,30%	0,23%
APT29	123,98%	0,53%
APT10	80,46%	0,17%
UNC4698	368,75%	1,14%
APT34	96,73%	0,23%
Altri	-28,99%	-33,33%

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- **Evoluzione delle tattiche:** i rilevamenti delle minacce legate a Sandworm, gruppo storicamente noto per le sue operazioni informatiche dirompenti, hanno fatto rilevare un impressionante incremento pari al 1.669%, con una varianza del contributo proporzionale del 40%. Questo incredibile aumento suggerisce un'escalation senza precedenti nelle attività informatiche da parte del gruppo legato alla Russia.
- **Espansione aggressiva delle operazioni:** I rilevamenti delle attività del gruppo APT29, molto attivo nello spionaggio informatico, sono aumentati del 124%. Analogamente, i rilevamenti associati a APT34 e Covellite sono aumentati sostanzialmente, rispettivamente del 97% e dell'85%, indicando tempi operativi maggiori o l'avvio di nuove campagne.
- **Omeostasi:** per contro, i livelli di attività di gruppi come Mustang Panda, Turla e APT28 sono rimasti a livelli minimi, con Mustang Panda che ha mostrato un leggero calo (-2%) e Turla un aumento modesto (3%).
- **Comparsa di nuovi criminali informatici:** degna di nota la comparsa di UNC4698, i cui rilevamenti sono aumentati del 363%, suggerendo l'ascesa di un nuovo protagonista potenzialmente significativo nel panorama delle APT.

COSA SAPPIAMO DEL GRUPPO UNC4698?

Non si sa molto di questo gruppo, ma i ricercatori sono riusciti a riconoscere il suo comportamento come attività di gruppo e non sanno ancora come definirlo.

Detto ciò, sappiamo che il gruppo UCN4698 si concentra sullo spionaggio industriale; raccoglie dati operativi sensibili che potrebbero essere utilizzati per supportare obiettivi di sicurezza nazionale o economici dello Stato a cui è affiliato, presumibilmente legato alla Cina data la natura e la focalizzazione regionale degli attacchi.

I suoi obiettivi abituali sono le aziende dell'industria del petrolio e del gas in Asia.

Il collettivo è noto anche per utilizzare un malware denominato "SNOWYDRIVE".

Il gruppo UNC4698 utilizza una varietà di tattiche, tecniche e procedure (TTP) incentrate sull'uso di malware distribuito tramite chiavette USB. Ecco alcune delle TTP associate a questo gruppo di criminali informatici:

- **Accesso iniziale tramite dispositivi USB infetti:** il metodo d'infezione principale prevede l'utilizzo di chiavette USB che contengono software dannoso progettato per creare una backdoor sul sistema host.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

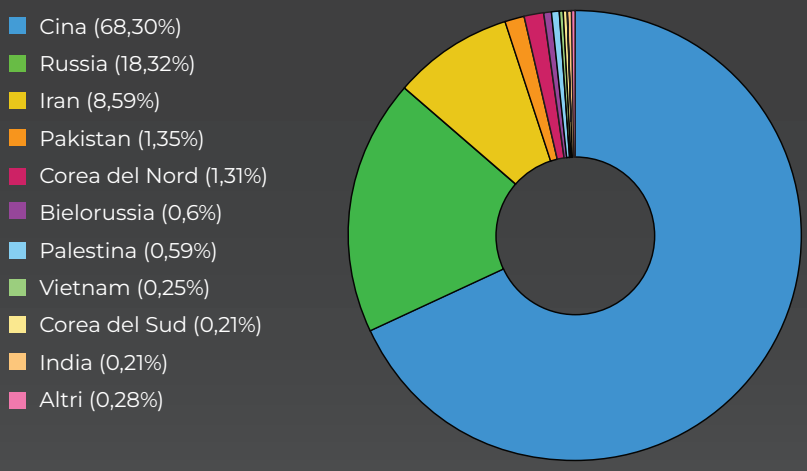
COSA SAPPIAMO DEL GRUPPO UNC4698? *(segue)*

- **Esecuzione tramite file dannosi:** il malware generalmente include un file dropper che scrive eseguibili e DLL dannosi sul disco. Questi file spesso nascondono un software legittimo per evitare il rilevamento e vengono eseguiti per ottenere maggior controllo.
- **Persistenza e modifica del registro:** il gruppo UNC4698 assicura la persistenza sui sistemi infetti modificando il Registro di Windows. Ciò permette al malware di avviarsi automaticamente non appena il sistema si avvia.
- **Comunicazione con il server di Comando e controllo (C&C):** il malware configura un metodo di comunicazione da remoto, permettendo agli autori dell'attacco di impartire comandi e controllare i sistemi compromessi a distanza.
- **Spostamento laterale tramite supporti rimovibili:** il malware può copiarsi su altri dispositivi USB connessi al computer infetto, diffondendo l'infezione su altri sistemi.

I rilevamenti associati a gruppi meno noti o non identificati, hanno registrato un aumento del 62%, indicando l'esistenza di una gamma di minacce diversificata e in crescita al di là di entità APT ben documentate. Questo aumento dell'8% del loro contributo proporzionale rispetto al numero complessivo di rilevamenti evidenzia la costante evoluzione e diversificazione delle minacce informatiche.

Gruppi APT e Paesi di origine

PRIMI 10 PAESI DEI GRUPPI APT CON IL MAGGIOR NUMERO DI RILEVAMENTI LEGATI ALLE CAMPAGNE, TRA IL 4° TRIMESTRE 2023 E IL 1° TRIMESTRE 2024



SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Se si prendono in esame i Paesi di origine, i dati di telemetria di Trellix da ottobre 2023 a marzo 2024 mostrano anche notevoli cambiamenti nel panorama delle attività dei gruppi di criminali informatici sponsorizzati dagli stati.

I gruppi di criminali informatici legati alla Cina rimangono gli autori più prolifici di attività APT

- **Escalation considerevole delle operazioni:** le motivazioni geopolitiche e le competenze di sicurezza informatica evolvono nelle diverse nazioni. I nostri dati di telemetria indicano quanto segue:
  a. I rilevamenti di minacce APT imputabili a gruppi legati alla Russia sono aumentati in modo significativo (+31%), mentre il loro contributo proporzionale è aumentato del 4%. Ciò indica un'escalation considerevole delle operazioni informatiche, che potrebbe riflettere l'ampliamento degli obiettivi strategici o delle risposte alle dinamiche globali della sicurezza informatica.
  b. Le attività informatiche dei gruppi legati all'Iran si sono intensificate, con un aumento dell'8% dei rilevamenti e del 3,89% del contributo proporzionale. Questi dati mettono in luce un'espansione significativa delle operazioni informatiche dell'Iran, in linea con i suoi obiettivi geopolitici e il suo coinvolgimento nella guerra tra Israele e Hamas.
- **Una più ampia diversificazione:** la Cina rimane l'artefice più prolifico di attività APT, con rilevamenti in leggero aumento (1%). Tuttavia, il suo contributo proporzionale al numero complessivo di rilevamenti ha visto un leggero calo (-1%), che potrebbe suggerire una più ampia diversificazione delle origini di APT in questo periodo. Nel febbraio 2024, il gruppo APT Volt Typhoon affiliato alla Cina ha implementato tentativi importanti per colpire le infrastrutture critiche statunitensi. Maggiori informazioni su questo punto sono incluse nella sezione seguente.
- **Cambio di strategia:** al contrario, le attività APT dei gruppi legati a Corea del Nord, Vietnam e India si sono ridotte drasticamente: i rilevamenti legati alla Corea del Nord sono calati dell'82%, quelli imputabili al Vietnam dell'80% e quelli imputabili all'India dell'82%. La significativa diminuzione del contributo proporzionale della Corea del Nord (-6%) è particolarmente degna di nota, a indicare probabilmente un cambio in termini di focalizzazione, strategia o competenze.
- **Comparsa di altri Paesi:** i gruppi legati al Pakistan e alla Bielorussia hanno registrato incrementi significativi delle loro attività APT, con un aumento dei rilevamenti, del 55% e addirittura del 2.019%, rispettivamente. Tali aumenti, in particolare il rialzo esponenziale associato alla Bielorussia, sottolinea la comparsa di nuovi criminali informatici o precedentemente non noti nell'arena delle APT.

  La categoria "Altri" mostra un i incremento del 121% dei rilevamenti, a indicare che le attività APT non sono limitate alle nazioni menzionate più di frequente. Questa diversità mette in luce la natura globale delle minacce informatiche e la necessità di adottare un approccio alla sicurezza informatica adattivo e di ampio respiro.

Seguiremo da vicino queste nuove tendenze nei prossimi mesi.

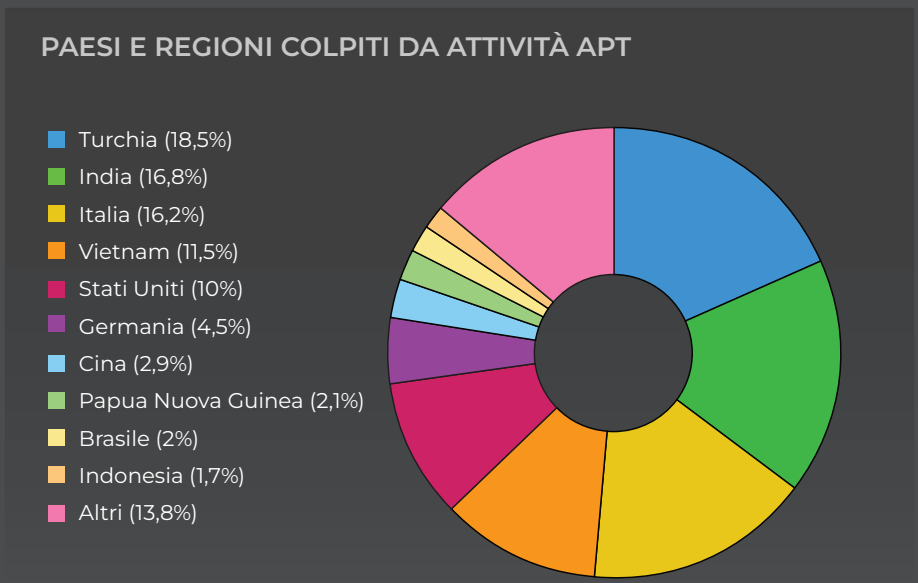
SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix



Paesi e regioni colpiti

Questa sezione si concentra sulle aree geografiche in cui Trellix ha rilevato attività correlate a gruppi APT tra il quarto trimestre 2023 e il primo trimestre 2024, rivelando cambiamenti significativi in termini di focalizzazione e strategia tra questi criminali informatici sofisticati.

> I dati sottolineano la natura globale delle minacce informatiche e i diversi livelli di attenzione che le varie nazioni ricevono dai gruppi APT.

Gli esperti del Trellix Advanced Research Center stimano con un moderato livello di fiducia che i seguenti fattori abbiano avuto un impatto sulle attività rilevate in alcuni paesi e regioni.

La Turchia è stata presa di mira da un numero senza pari di minacce APT

Obiettivi operativi:
i rilevamenti di minacce che prendono di mira la Turchia sono aumentati del 1.458%, che si traduce in un incremento del 16% del loro contributo proporzionale ai rilevamenti totali. Questo incremento significativo indica un importante rafforzamento dell'attenzione delle minacce informatiche verso la Turchia, a riflettere probabilmente tensioni geopolitiche più ampie o obiettivi operativi specifici dei gruppi APT.

- **Importanza strategica:** anche le minacce contro India e Italia hanno registrato incrementi considerevoli, con rilevamenti in aumento rispettivamente del 614% e del 308%. La crescente importanza di questi Paesi nell'elenco degli obiettivi può indicare la loro crescente importanza strategica nel mondo informatico, dovuta a fattori economici, politici o tecnologici.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

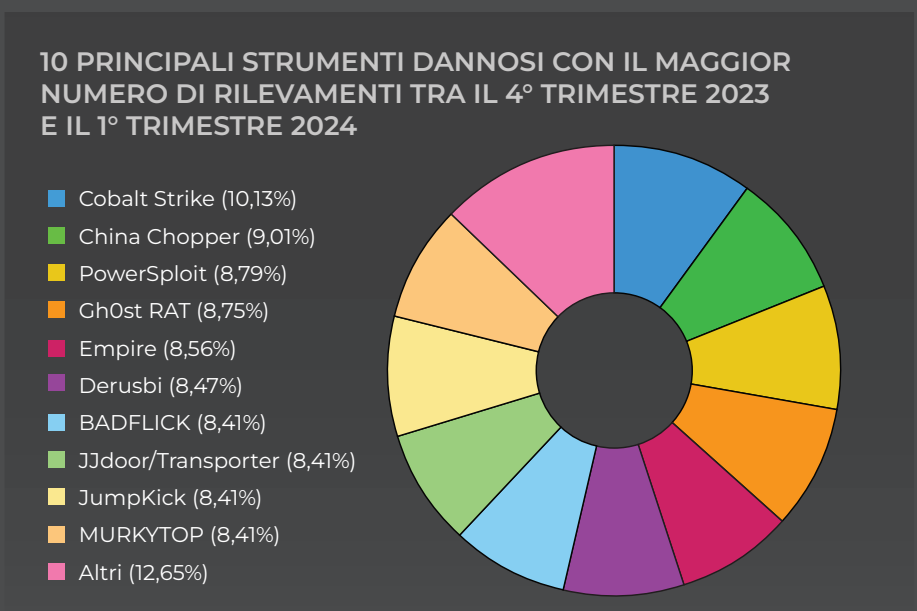
Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- **Un panorama sempre più ampio:** curiosamente, Vietnam e Stati Uniti, pur continuando a generare rilevamenti APT significativi, mostrano tendenze diverse. I rilevamenti in Vietnam sono aumentati del 9%, anche se il loro contributo proporzionale è sceso del -9%, a indicare un ampliamento del panorama preso di mira. I rilevamenti delle minacce contro gli Stati Uniti hanno osservato un moderato aumento del 15% ma un calo del -7% nel loro contributo proporzionale, suggerendo una diversificazione nelle strategie di targeting dei gruppi APT.
- **Sviluppi geopolitici:** i rilevamenti di minacce contro Germania, Cina, Papua Nuova Guinea e Brasile sono aumentati, con la Germania e la Cina con modifiche significative in termini di contributo proporzionale. Questa diversificazione del targeting riflette gli adeguamenti strategici e opportunistici dei gruppi APT in risposta ai livelli di sicurezza informatica globali e agli sviluppi geopolitici.
- **Miglioramento della sicurezza nazionale:** al contrario, i rilevamenti di minacce contro l'Indonesia hanno registrato un calo degno di nota del 48%, unito a un contributo proporzionale ridotto del 4%. Questa riduzione può suggerire un temporaneo calo di priorità o un efficace potenziamento delle misure nazionali di sicurezza informatica.
- **Consolidamento del focus:** la categoria "Altri", che rappresenta l'insieme di diversi altri Paesi in cui Trellix ha rilevato attività APT, ha registrato un calo del 23% dei rilevamenti a un calo del 21% in termini di contributo proporzionale. Questa diminuzione evidenzia un potenziale consolidamento dell'attenzione da parte dei gruppi APT su obiettivi specifici di elevato interesse durante questo periodo.

Riteniamo che il panorama possa continuare a cambiare rapidamente a causa delle tendenze geopolitiche.

Strumenti dannosi

10 PRINCIPALI STRUMENTI DANNOSI CON IL MAGGIOR NUMERO DI RILEVAMENTI TRA IL 4° TRIMESTRE 2023 E IL 1° TRIMESTRE 2024



SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

L'analisi degli strumenti dannosi utilizzati nelle campagne APT tra il quarto trimestre 2023 e il primo trimestre 2024 rivela tendenze degne di nota nelle preferenze e nelle tattiche operative dei criminali informatici. La varianza dei tassi di rilevamento e del loro contributo proporzionale fornisce informazioni sul panorama delle minacce informatiche in continua evoluzione e sulle mutevoli dinamiche nell'utilizzo degli strumenti da parte di questi gruppi sofisticati.

Abbiamo osservato le seguenti tendenze:

- **Rafforzamento degli strumenti d'attacco:** Cobalt Strike rimane lo strumento preferito per molti gruppi di criminali informatici, nonostante un calo del 17% dei rilevamenti. Il suo calo relativamente contenuto del suo contributo proporzionale (-1%) suggerisce che mantiene la sua popolarità ed efficacia nelle operazioni informatiche, sottolineando la difficoltà di difendersi da strumenti d'attacco versatili e ampiamente utilizzati.
- **Utilizzo di attacchi web shell, PowerShell e con accesso remoto:** China Chopper, PowerSploit e Gh0st RAT hanno altresì registrato cali significativi, rispettivamente del 23%, 24% e 24%. Nonostante tali cali, questi lievi cambiamenti nella varianza del contributo proporzionale indicano che rimangono parte integrante del kit di strumenti dei criminali informatici. Questi strumenti, noti per le loro funzionalità negli attacchi web shell, exploit PowerShell e attacchi di accesso remoto, evidenziano il continuo utilizzo di strumenti collaudati e versatili per condurre operazioni informatiche.
- **Strumenti meno rilevabili:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick e MURKYTOP hanno registrato un'analoga tendenza di calo dei rilevamenti, con diminuzioni superiori al 25%. Questo declino uniforme potrebbe riflettere un più ampio cambiamento negli strumenti preferiti dai gruppi di criminali informatici o un adattamento alle contromisure e alle tecniche di rilevamento, con conseguente passaggio a strumenti più nuovi e meno rilevabili.
- **Innovazione costante:** la categoria "Altri" degli strumenti dannosi ha mostrato un aumento significativo dei rilevamenti, pari al 30%, e un incremento del 6% del contributo proporzionale. Tale incremento sottolinea l'innovazione e l'adattamento costante tra i criminali informatici, che esplorano nuovi strumenti e tecniche per eludere il rilevamento e raggiungere i loro obiettivi.

Le mutevoli preferenze in termini di utilizzo di strumenti dannosi indica la natura adattiva dei criminali informatici in risposta agli sviluppi nella sicurezza informatica.

> Man mano che i meccanismi di difesa diventano più sofisticati, lo stesso fanno le tattiche e gli strumenti d'attacco dei gruppi APT.

Il passaggio a una gamma più ampia di strumenti, come indicato dall'aumento dei rilevamenti nella categoria "Altri", evidenzia la necessità di ricerche continue, di una Threat Intelligence pertinente e di strategie di difesa adattive per mitigare il rischio posto da queste minacce informatiche in costante evoluzione.

SOMMARIO

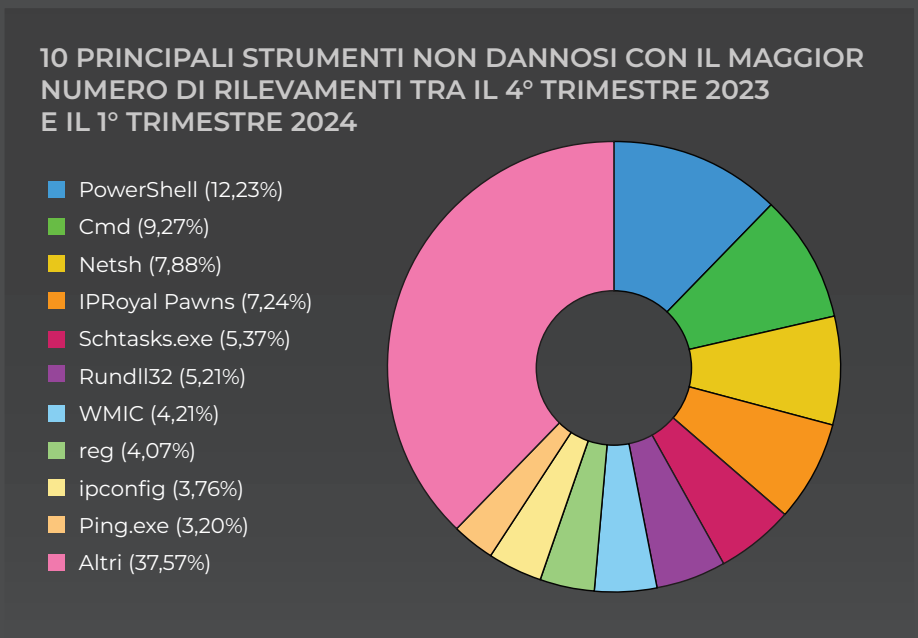
Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Strumenti non dannosi



> Questa pratica, nota come sfruttamento delle risorse locali LOTL, Living Off The Land), complica le attività di rilevamento e sottolinea la sofisticazione di questi criminali informatici.

L'utilizzo di strumenti non dannosi nelle operazioni informatiche dei gruppi APT tra il quarto trimestre 2023 e il primo trimestre 2024 evidenzia un aspetto importante delle minacce informatiche moderne: lo sfruttamento di strumenti di sistema legittimi a fini dolosi. Questa pratica, nota come sfruttamento delle risorse locali LOTL, Living Off The Land), complica le attività di rilevamento e sottolinea la sofisticazione di questi criminali informatici. Le statistiche rivelano variazioni significative nell'utilizzo di questi strumenti, a riflettere l'importanza strategica nelle operazioni informatiche.

- **Versatilità:** i rilevamenti di PowerShell sono aumentati in modo significativo (105%), con una varianza del contributo proporzionale pari all'1%. Questa impennata sottolinea la sua versatilità e la sua efficacia nell'automatizzare un'ampia gamma di attività dannose, dalla ricognizione alla distribuzione di payload.
- **Focalizzazione sulla manipolazione della rete:** i rilevamenti di Netsh e IPRoyal Pawns hanno registrato un aumento significativo, pari al 99% e al 102%, rispettivamente. Questi strumenti sono spesso utilizzati per la configurazione della rete e il traffico proxy, indicando una focalizzazione strategica sulla manipolazione della rete e le tecniche di elusione.
- **Automazione su larga scala:** Schtasks.exe ha registrato la varianza percentuale maggiore (138%) tra gli strumenti elencati, riflettendo la crescente dipendenza da attività pianificate per la persistenza e l'esecuzione di payload dannosi senza intervento diretto dell'utente.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- **Adeguamenti tattici:** al contrario, l'utilizzo di Rundll32 e WMIC è aumentato, ma le varianze del loro contributo proporzionale sono diminuite, indicando un cambiamento nelle preferenze tattiche dei gruppi APT nonostante l'utilizzo di questi strumenti.
- **Diversificazione degli strumenti:** i nostri dati mostrano un aumento importante dell'utilizzi di Cmd, il noto interprete di comandi sui sistemi Windows, con un incremento dei rilevamenti del 65%. Nonostante il suo utilizzo sia aumentato, la sua varianza del contributo proporzionale è diminuita del 2,5%, suggerendo una più ampia diversificazione nell'utilizzo degli strumenti tra i gruppi di APT.

  I rilevamenti della categoria "Altri", che rappresenta una gamma di strumenti usati meno di frequente o più specializzati, sono aumentati del 42%. Tuttavia, ha fatto rilevare un calo significativo della varianza del contributo proporzionale (-21%), sottolineando l'espansione dell'arsenale di strumenti a disposizione dei criminali informatici.

L'evoluzione del panorama degli strumenti non dannosi utilizzati dai gruppi APT illustra la complessità di rilevare e neutralizzare le minacce informatiche sofisticate. La selezione strategica e all'applicazione di questi strumenti rivela una profonda conoscenza degli ambienti presi di mira e dei metodi per non eludere il rilevamento.

> **CONSIGLIO PER IL CISO:** le difese di sicurezza informatica devono andare oltre il tradizionale rilevamento del malware e includere l'analisi comportamentale e il rilevamento delle anomalie per contrastare l'uso improprio di strumenti legittimi nelle operazioni informatiche.

I dati raccolti attraverso i sensori globali di Trellix ATLAS sono associati alle informazioni strategiche di report convalidati dal settore e pubblicati dal Trellix Advanced Research Center per consentire ai nostri clienti di identificare i criminali informatici che colpiscono i loro rispettivi settori e utilizzare la nostra analisi comportamentale per rilevare i comportamenti anomali all'interno del loro ambiente.

SOMMARIO

Premessa

Prefazione

Introduzione: Report sulle minacce informatiche Giugno 2024

- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi

- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione

Metodologia

- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse

- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Conclusione

L'analisi dell'attività delle attività APT tra il quarto trimestre 2023 e il primo trimestre 2024 ha fatto luce sulla natura dinamica e sempre più complessa del panorama delle minacce informatiche. La nostra disamina delle statistiche legate alle origini dei gruppi APT, ai Paesi presi di mira, all'utilizzo di strumenti dannosi e non dannosi rivela numerose importanti tendenze che sottolineano le strategie in evoluzione dei criminali informatici.

I gruppi APT continuano a:

1. mostrare adattabilità e sofisticatezza;
2. utilizzare un mix di strumenti dannosi;
3. sfruttare utilità di sistema legittime per eseguire attività di spionaggio, interrompere le operazioni e rubare informazioni sensibili.

Le significative variazioni osservate nel targeting e nelle tattiche operative di questi gruppi riflettono non solo i loro obiettivi strategici, ma anche la loro risposta agli sviluppi della sicurezza informatica globale e alle misure difensive.

I drastici cambiamenti nelle pratiche di targeting, con alcuni Paesi che hanno registrato un aumento sostanziale delle attività legate alle APT, evidenziano le motivazioni geopolitiche che guidano queste operazioni informatiche. Allo stesso modo, i cambiamenti nell'utilizzo degli strumenti, tra cui un aumento significativo nelle tattiche di sfruttamento delle risorse locali, enfatizza la difficoltà a rilevare e contrastare le minacce APT in un panorama dove le attività legittime e dannose sono sempre più legate tra loro.

Inoltre, la diversificazione nella provenienza dei gruppi APT e l'ampliamento delle loro strategie di targeting indicano una proliferazione globale di funzionalità informatiche e la necessità di un approccio unificato e collaborativo alla sicurezza informatica.

> È chiaro che nessuna nazione o azienda è immune dalla portata di questi criminali informatici sofisticati.

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina

I gruppi di criminali informatici sponsorizzati dagli Stati hanno continuato a rappresentare una grave minaccia per le aziende del settore pubblico e privato in tutto il mondo durante l'ultimo trimestre del 2023 e il primo trimestre del 2024. Questi collettivi, spesso ben equipaggiati e esperti in minacce informatiche sofisticate, prendono di mira senza sosta le reti per periodi prolungati grazie a competenze e risorse superiori rispetto ai criminali informatici e agli attivisti informatici.

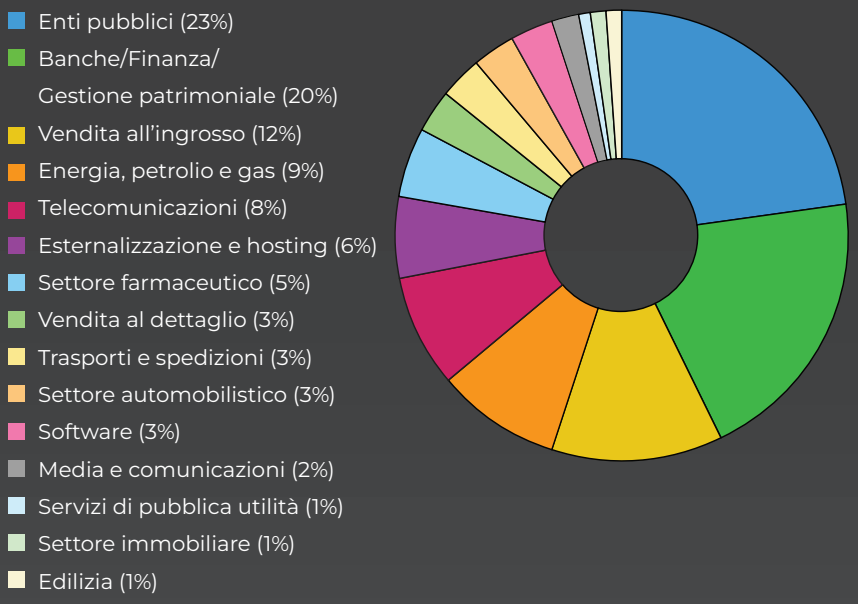
23%

Oltre il 23% dei rilevamenti di attività dannose sono indirizzati contro il settore della pubblica amministrazione a livello mondiale

Sono stati rilevati oltre 21 milioni di attività di minacce provenienti da gruppi criminali affiliati alla Cina

Nello specifico, in base ai rilevamenti basati sui dati della telemetria di Trellix, i gruppi di criminali informatici sponsorizzati dagli Stati affiliati alla Cina hanno rappresentato una minaccia crescente per il settore pubblico in tutto il mondo. I nostri dati mostrano oltre 21 milioni di rilevamenti di attività dannose da gruppi allineati alla Cina tra ottobre 2023 e marzo 2024.

RILEVAMENTI GLOBALI DI MINACCE DA GRUPPI APT AFFILIATI ALLA CINA



(Fonte: ATLAS)

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

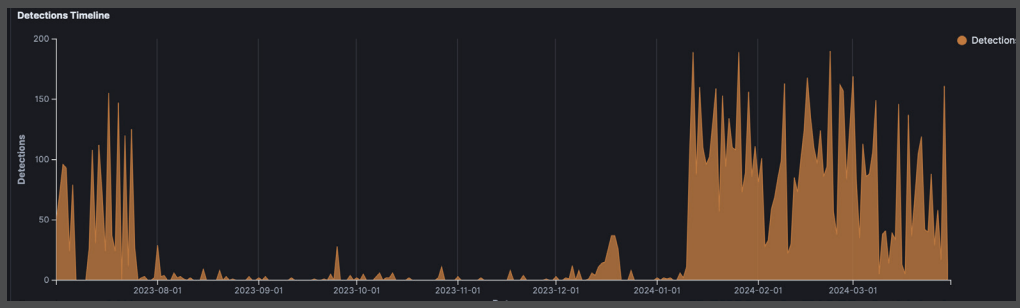
Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Panoramica

Gruppo APT sponsorizzato dalla Cina relativamente nuovo, Volt Typhoon si distingue per il suo comportamento unico e i profili che prende di mira unici, che differiscono dalle attività di spionaggio informatico convenzionale e raccolta di informazioni di altri gruppi APT associati alla Cina. Precedenti report open source suggeriscono che questo gruppo APT cinese si è pre-posizionato sulle reti IT di controllo industriali per facilitare gli spostamenti laterali al fine di bloccare le risorse e le funzioni OT in caso di crisi geopolitica o guerra. I dati della telemetria di Trellix mostrano che dalla ripresa delle attività nel gennaio 2024, Volt Typhoon ha ripetutamente preso di mira enti del settore pubblico in tutto il mondo, tra cui gli Stati Uniti, adottando tecniche di sfruttamento delle risorse locali.

Calendario operativo

Secondo i dati della telemetria globale di Trellix, Volt Typhoon è stato rilevato la prima volta a metà del 2021, ma è rimasto in gran parte inattivo, con attività scarse o nulle, dall'agosto 2023 al gennaio 2024. Questo periodo di inattività potrebbe essere conseguente al culmine delle indagini sulle minacce nei mesi successivi alla pubblicazione del primo report di un fornitore di sicurezza su Volt Typhoon nel maggio 2023, che ha attirato l'attenzione del mondo intero. Un'evoluzione delle infrastrutture d'attacco di Volt Typhoon durante questo periodo, data la sua esposizione pubblica, potrebbe spiegare il basso volume di attività delle minacce rilevato.



Cronologia dei rilevamenti di Volt Typhoon tra luglio 2023 e marzo 2024 (Fonte: Trellix ATLAS)

Volt Typhoon ha ripreso le operazioni intorno a metà gennaio 2024, in base ai dati di telemetria di Trellix. A partire da metà gennaio 2024, i dati di telemetria di Trellix hanno rilevato oltre 7.100 attività dannose associate a Volt Typhoon, con picchi periodici tra gennaio e marzo 2024.

Dettagli dei rilevamenti di Volt Typhoon tra gennaio a marzo 2024

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Tattiche, tecniche e procedure (TTP)

I nostri dati di rilevamento suggeriscono che, da quando è tornato operativo a metà gennaio 2024, Volt Typhoon ha costantemente sfruttato una serie di strumenti e funzionalità nativi dei sistemi Windows per eseguire comandi a fini dannosi. Questi strumenti di sfruttamento delle risorse locali permettono un doppio uso, perché si tratta di software e funzioni legittime integrate nel sistema e sono diventati sempre più popolari tra i gruppi affiliati alla Cina, tra cui Volt Typhoon. Netsh.exe è uno di questi strumenti che può essere utilizzato per diversi fini dannosi, come disabilitare le impostazioni del firewall o configurare un tunnel proxy per consentire l'accesso remoto a un host infetto. Ldifde è un altro strumento sfruttato dai criminali informatici di Volt Typhoon per la raccolta di informazioni.

Una volta ottenuto l'accesso a un controller di dominio, gli autori degli attacchi possono utilizzare Ldifde.exe per esportare i dati sensibili o eseguire modifiche autorizzate alla directory. Analogamente, i criminali informatici di Volt Typhoon possono utilizzare anche ntdsutil per le loro attività d'attacco. Ntdsutil è uno strumento legittimo che serve per la manutenzione del database; tuttavia, può anche essere sfruttato per creare un'estrazione di Active Directory per raccogliere credenziali ed esfiltrare dati sensibili.

Il gruppo Volt Typhoon ha continuato a utilizzare strumenti open source, come FRP, Impacket e Mimikatz. I dati di telemetria di Trellix hanno anche rilevato che Volt Typhoon ha utilizzato i seguenti strumenti e comandi di sfruttamento delle risorse locali tra febbraio e marzo 2023:

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- ping
- PowerShell
- PsExec

SOMMARIO

Premessa

Prefazione

Introduzione: Report sulle minacce informatiche Giugno 2024

- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi

- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione

Metodologia

- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse

- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

In base ai nostri dati di telemetria, i principali strumenti MITRE ATT&CK sfruttati da Volt Typhoon sono i seguenti:

- Accesso iniziale – T1190: Sfruttamento di applicazioni per il pubblico
- Esecuzione – T1106: API nativa
- Persistenza – T1546: Esecuzione attivata dagli eventi
- Aumento dei privilegi – T1546: Esecuzione attivata dagli eventi
- Elusione delle difese – T1070.001: Cancellazione dei registri eventi di Windows
- Elusione delle difese – T1070: Cancellazione dei file
- Elusione delle difese – T1027: Offuscamento di file o informazioni
- Accesso alle credenziali – T1003.003: NTDS
- Accesso alle credenziali – T1003: Estrazione delle credenziali dal sistema operativo
- Accesso alle credenziali – T1110: Attacco di forza bruta
- Accesso alle credenziali – T1555: Credenziali estratte da archivi di password
- Rilevamento – T1069.002: Gruppi di dominio
- Rilevamento – T1069.001: Gruppi locali
- Rilevamento – T1083: Rilevamento di file e directory
- Rilevamento – T1057: Rilevamento del processo
- Rilevamento – T1010: Rilevamento delle finestre dell'applicazione
- Acquisizione – T1560: Archiviazione dei dati acquisiti
- Acquisizione – T1560.001: Archiviazione tramite utility
- Comando e controllo – T1090.002: Proxy esterno
- Comando e controllo – T1105: Trasferimento di strumenti all'ingresso
- Comando e controllo – T1132: Codifica dei dati

Evoluzione del panorama del ransomware

Nel quarto trimestre 2023, il panorama delle minacce informatiche ha visto un'escalation degli attacchi ransomware, con nuove famiglie di ransomware apparse nell'anno con un impatto sempre più significativo.

- **Strumenti di disattivazione dell'EDR:** la comparsa della banda ransomware D0nut è stata particolarmente degna di nota per il suo innovativo utilizzo di uno strumento di disattivazione delle soluzioni EDR, una tattica avanzata per eludere il rilevamento sugli endpoint e migliorare l'efficacia degli attacchi. Maggiori informazioni su questo tema sono nella sezione seguente.
- **Exploit delle vulnerabilità:** in questo periodo è proseguita anche la tendenza a sfruttare le vulnerabilità critiche per facilitare la diffusione del ransomware. In particolare, CVE-2023-4966, nota come Citrix Bleed, è stata sfruttata dagli affiliati di LockBit 3.0, evidenziando la costante vulnerabilità delle infrastrutture critiche agli attacchi informatici sofisticati. Inoltre, lo sfruttamento della CVE-2023-22518 in Confluence Data Center e Confluence Server ha evidenziato la volontà di infiltrarsi in piattaforme aziendali ampiamente utilizzate per distribuire il ransomware.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

La campagna ransomware Cactus, che ha preso di mira le installazioni Qlik Sense sfruttando vulnerabilità appena scoperte, dimostra ulteriormente l'agilità degli autori degli attacchi nell'adattarsi al panorama delle minacce e a sfruttare le vulnerabilità emergenti. Ciò ha contribuito a rendere il quarto trimestre del 2023 un trimestre attivo per i gruppi di ransomware.

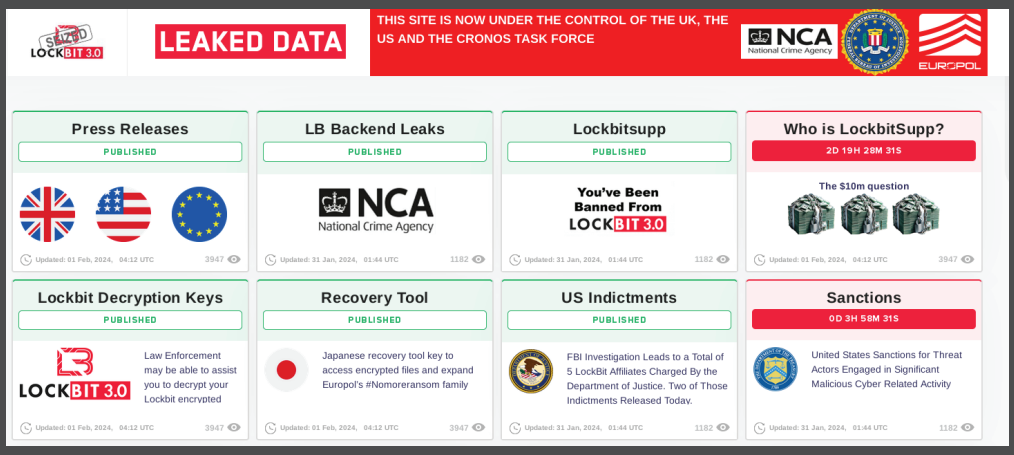
Tuttavia, lo status quo stava per essere scosso nel primo trimestre del 2024 da un'azione delle forze dell'ordine degna di nota.

Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit

L'azione di polizia internazionale denominata Operation Cronos è stata avviata il 19 febbraio 2024. Ha bloccato le attività della famigerata banda LockBit, dando al gruppo criminale di lunga data un assaggio della sua stessa medicina. Le forze dell'ordine non si sono limitate a mostrare gli avvisi di smantellamento, ma alla fine hanno avuto il controllo completo del sito di divulgazione del gruppo e hanno anche divulgato informazioni per esporre il gruppo criminale al mondo intero. Sono state presentate diverse incriminazioni e gli affiliati attivi hanno ricevuto un messaggio di benvenuto quando hanno effettuato l'accesso al backend di LockBit, chiarendo che le loro identità erano note.

Queste azioni erano volte non solo a smantellare l'operazione di LockBit, ma anche a danneggiarne la reputazione e a minare la fiducia all'interno della banda.

Al momento della stesura di questo report, Operation Cronos ha avuto un altro colpo di scena. La task force internazionale ha messo a segno un secondo colpo rivelando la vera identità del capobanda di LockBit. Questa non è stata l'unica vittoria per le forze dell'ordine; il 1° maggio l'affiliato di REvil che ha attaccato Kaseya e molte altre aziende è stato condannato a 13 anni di carcere e dovrà rimborsare 16 milioni di dollari in danni. Per saperne di più su come Trellix Advanced Research Center ha partecipato al caso REvil consultare questo articolo.



SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Lo scorso anno, il nostro report di febbraio aveva identificato LockBit come il gruppo più aggressivo nelle sue richieste di riscatto. Questi criminali informatici utilizzano diverse tecniche per eseguire le loro campagne, incluso lo sfruttamento di vulnerabilità scoperte già nel 2018. Nel corso del 2023, LockBit è rimasto costantemente il gruppo di ransomware più diffuso con il maggior numero di vittime pubblicate sul loro sito di divulgazione. Questo gruppo ha preso principalmente di mira aziende europee e nordamericane in vari settori, colpendo maggiormente il settore dei beni e servizi industriali. Nel 2023, LockBit ha continuato a evolversi e a introdurre nuovi strumenti e metodi al proprio programma ransomware. Tra gli eventi rilevanti, il lavoro di LockBit per sviluppare lo strumento di crittografia LockBit Green basato sul codice trapelato dal ransomware Conti nonché sulle varianti che prendono di mira macOS. Inoltre, il RaaS LockBit ha accolto nel 2023 gli affiliati di altri programmi RaaS come ALPHV e NoEscape, le cui strutture sono state smantellate.

All'indomani di un'importante operazione delle forze dell'ordine, abbiamo assistito al frenetico tentativo di LockBit di salvare le apparenze e ripristinare la redditizia operazione. Questo era prevedibile data la pubblicità intorno alle attività criminali di LockBit, ma nel mondo della criminalità informatica è più facile ripristinare un server che anni di fiducia. Resta da vedere quante informazioni siano state ottenute dalle forze dell'ordine sulle operazioni di LockBit, sulla sua immagine pubblica e sui suoi affiliati.

> Questa incertezza crea un rischio elevato per qualsiasi criminale informatico desideroso di collaborare con LockBit e il suo (ex) team.

Dopo le azioni delle forze dell'ordine è emerso chiaramente che il mondo dei criminali è un mondo estremamente competitivo. Gli esperti del Trellix Advanced Research Center hanno osservato altri criminali utilizzare la versione divulgata da LockBit Black per rubare l'identità del celebre gruppo per il proprio tornaconto economico.

Impostori o meno, le loro vittime erano reali e tutti questi eventi hanno reso gli ultimi due trimestri degni di un film.

Prospettiva globale sul ransomware

Durante le nostre ricerche sull'attività dei ransomware nel primo trimestre del 2024, abbiamo analizzato diverse fonti: siti di divulgazione, dati di telemetria e report pubblici. Descriviamo brevemente queste categorie.

- **Siti di divulgazione:** questi siti sono studiati per esporre le vittime ricattate che non hanno pagato il riscatto richiesto. Offrono anche una panoramica dell'attività della banda criminale. Inoltre, è importante notare che i siti di divulgazione non necessariamente riflettono in modo preciso il panorama delle minacce informatiche. Dato che sono gestiti da criminali, non tutte le dichiarazioni sono necessariamente attendibili o corrette. Inoltre, se le bande mantengono la loro parola, le vittime che pagano il riscatto non vengono elencate, fornendo così un quadro incompleto. I dati utilizzati in questo report fanno riferimento alle tendenze generali dei siti di divulgazione e non forniscono un quadro rappresentativo della realtà.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

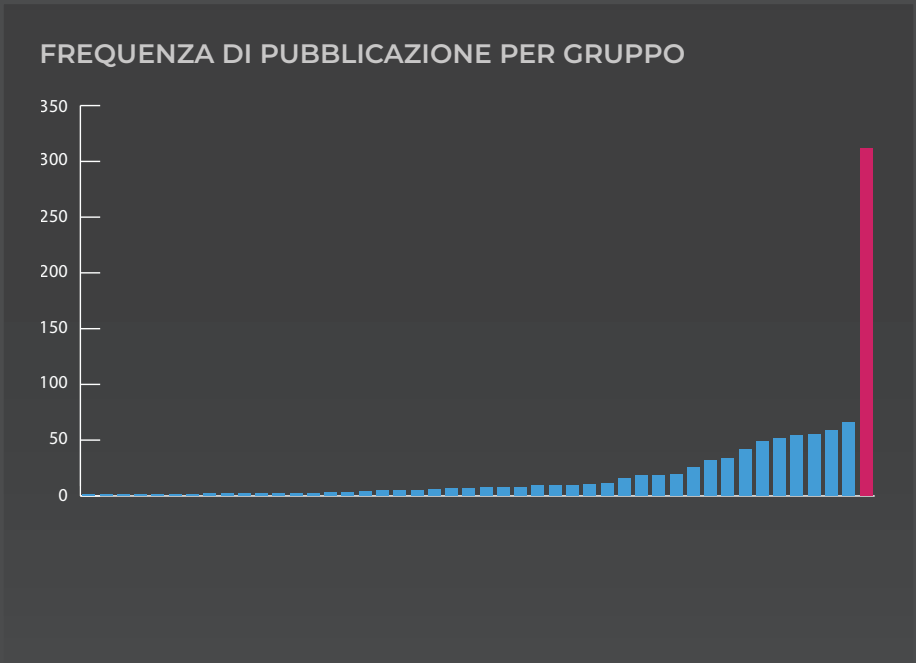
Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- **Dati di telemetria:** i dati di telemetria provengono dall'ecosistema di sensori di Trellix e i rilevamenti indicano quando un file, un URL, un indirizzo IP o un altro indicatore viene rilevato da uno dei nostri prodotti e riportato a noi. Ciò non significa che ogni rilevamento sia un'infezione, poiché i clienti testano il rilevamento di certi file per ottimizzare le loro regole interne, e tali dati compaiono nei file delle registrazioni aggregati. Perciò, tali dati sono utili quando si guarda al quadro generale, perché permettono di identificare le tendenze.
- **Report pubblici:** i report di fornitori e singoli sono stati elaborati dal nostro Advanced Research Center per analizzare le caratteristiche e riassumere le tendenze. Ogni report presenta un bias intrinseco, ad esempio la presenza geografica dominante di un fornitore rispetto a un altro. Questa differenza si tradurrà anche nei tip di incidenti segnalati. Data la varietà di bias presenti nei report inclusi, non applichiamo un filtro specifico.

Gruppi di ransomware attivi

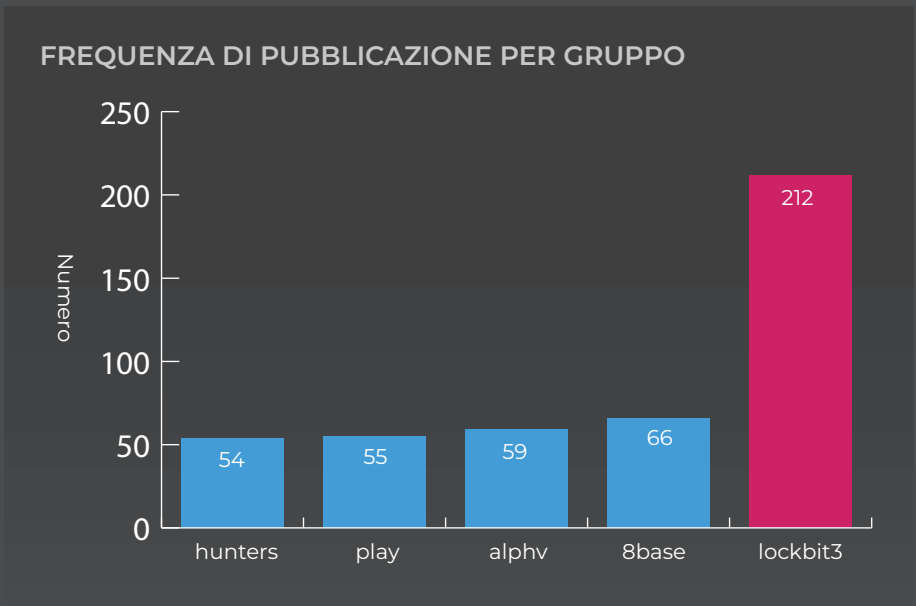
Molte delle pubblicazioni aggregate dei siti di divulgazione dal primo trimestre 2024 mostrano segni d'attività. A volte queste pubblicazioni sono annunci generici, ma la maggior parte sono "prove" di estorsione o fughe di dati dalle loro vittime. Spesso la stessa vittima è oggetto di più pubblicazioni, il che può distorcere i risultati perché viene conteggiata più di una volta nei dati.



SOMMARIO

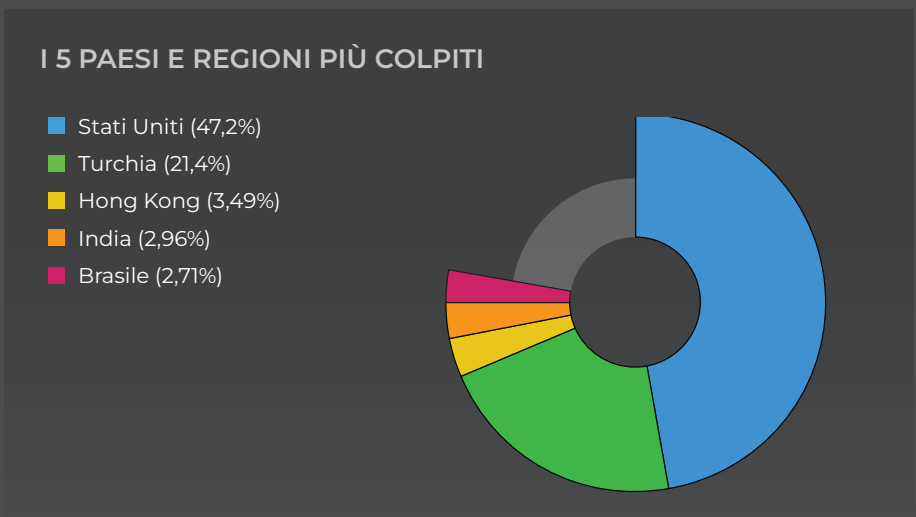
Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
L'impatto degli eventi geopolitici sul dominio informatico
Fatti salienti delle minacce in breve
Metodologia: come raccogliamo e analizziamo i dati
Segnalazioni, dati e analisi
Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
Gruppi sponsorizzati dagli Stati e APT attivi
Gruppi APT e Paesi di origine
Paesi e regioni colpiti
Strumenti dannosi
Strumenti non dannosi
Conclusione
Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
Panoramica
Calendario operativo
Tattiche, tecniche e procedure (TTP)
Evoluzione del panorama del ransomware
Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
Prospettiva globale sul ransomware
La comparsa di strumenti di elusione e disattivazione dell'EDR
Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
Moltiplicazione degli strumenti di disattivazione dell'EDR
L'email è ancora lo strumento preferito dagli autori degli attacchi
Truffe delle donazioni elettorali
Phishing delle imposte
L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
Integrazione dell'IA generativa negli infostealer
Progetto "Telegram Pro Poster"
Conclusione
Metodologia
Applicazione: come utilizzare queste informazioni
Come comprendere l'analisi presentata in questo report
Risorse
Informazioni su Trellix Advanced Research Center
A proposito di Trellix

Se si osserva la frequenza di pubblicazione dei cinque siti di divulgazione più attivi gestiti da bande di ransomware, l'attività di LockBit spicca nettamente sui grafici. L'attività delle bande, a parte LockBit, supera in media le 50 pubblicazioni in un trimestre, il che significa che il tempo medio tra la pubblicazione dei dati di due vittime è mediamente inferiore a due giorni. Come detto sopra, questi numeri rispecchiano le vittime che non pagano il riscatto, il che significa che il numero reale di vittime potrebbe essere più elevato sebbene non sia possibile stabilire il numero esatto.



Paesi e regioni colpiti

Basandosi sull'attività costante delle bande di ransomware, possiamo ricavare i rilevamenti di ransomware dai dati della telemetria di Trellix. Gli Stati Uniti generano il maggior numero di rilevamenti, seguiti da Turchia, Hong Kong, India e Brasile.



SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

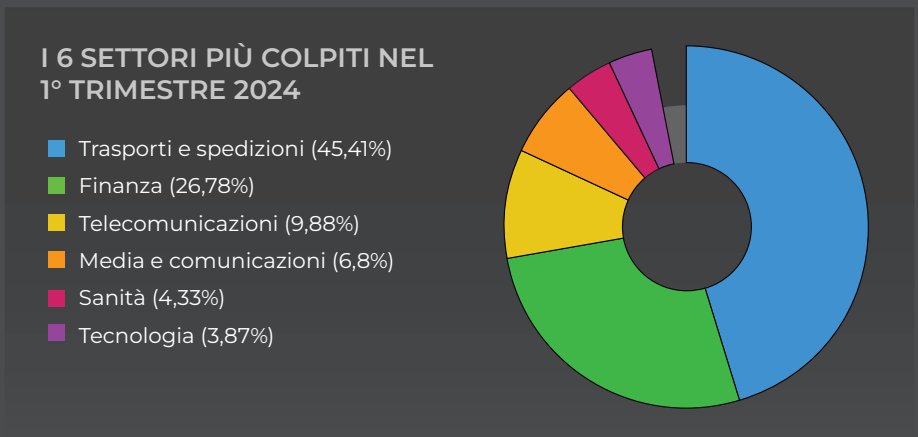
Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Dato che il ransomware rappresenta una minaccia per tutti i settori praticamente in ogni area geografica, i parametri di rilevamento sono coerenti con la popolazione di clienti.

Nel trimestre precedente, i dati di telemetria sono piuttosto simili, eccetto l'aumento dei rilevamenti in India e Cina. Non abbiamo indicazioni che si sia svolta una campagna specifica contro queste aree geografiche. Sospettiamo che siano stati effettuati dei test del malware che hanno portato a un maggior numero di rilevamenti in tali aree.

Settori colpiti

L'aggregazione dei dati globali di telemetria per settore mostrano che metà dei rilevamenti provengono dal settore trasporti e spedizioni, e oltre un quarto proviene dal settore dei servizi finanziari. Questi due settori rappresentano oltre il 72% di tutti i rilevamenti, il che ha un senso: la disponibilità dei loro servizi è di estrema importanza. Se un'azienda di trasporti non è in grado di spostare le merci a causa di un attacco ransomware, il loro processo operativo viene interrotto, causando enormi perdite finanziarie. Parimenti, il settore finanziario si basa sulla fiducia, per cui la divulgazione di dati sensibili e/o l'inoperatività dell'azienda a causa di un attacco ransomware, colpisce al cuore le società finanziarie.



Nel quarto trimestre del 2023, i principali settori colpiti erano leggermente diversi, ad eccezione dei primi due posti. Questi due settori sono stati responsabili di una quota ancora maggiore, per un totale del 78% di tutti i rilevamenti nel periodo preso in esame. I rilevamenti associati ai settori della tecnologia e della sanità sono diminuiti nel primo trimestre del 2024 rispetto al trimestre precedente, ma la differenza non può essere attribuita a uno o più eventi specifici.

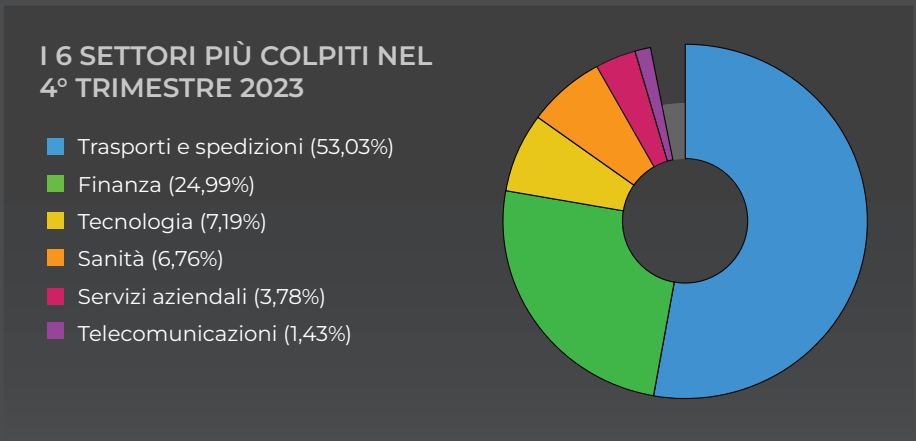
SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix



Strumenti e tecniche

L'ultima delle tre fonti menzionate sono report pubblici. Sulla base dei report raccolti, è possibile riassumere le tecniche MITRE, le linee di comando e gli strumenti associati.

> **CONSIGLIO PER IL CISO:** questi dati possono essere utilizzati dai team della sicurezza per il rilevamento: concentrarsi sulle tecniche e sugli strumenti più utilizzati aiuta a prevenire molteplici tipi di attacchi lanciati da diversi criminali, partendo dai più efficaci. Inoltre, gli esercizi di simulazione di attacchi possono concentrarsi su queste tecniche per testare le misure di rilevamento presenti.

La seguente tabella mostra le tecniche utilizzate più frequenti, elencate in ordine decrescente.

Tecniche MITRE ATT&CK	Campagne uniche
Crittografia dei dati per impatto	31
Rilevamento di file e directory	23
PowerShell	23
Trasferimento di strumenti all'ingresso	21
Rilevamento delle informazioni di sistema	21
Offuscamento di file o informazioni	19
Modifica del Registro	18
Windows Command Shell	17
Deoffuscamento/decodifica di file o informazioni	16
Arresto del servizio	16

Considerato l'obiettivo dei ransomware, non sorprende che le tecniche di tipo Crittografia dei dati e Rilevamento di file e directory siano ai primi posti. Confrontando queste tecniche con quelle più diffuse nel quarto trimestre del 2023, si nota che la maggior parte delle tecniche in cima alla classifica sono simili, anche se la loro posizione specifica potrebbe differire.

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

Tecniche MITRE ATT&CK	Campagne uniche
Crittografia dei dati per impatto	45
PowerShell	29
Offuscamento di file o informazioni	25
Rilevamento di file e directory	24
Windows Command Shell	24
Inibizione del ripristino del sistema	23
Sfruttamento di applicazioni per il pubblico	21
Trasferimento di strumenti all'ingresso	21
Rilevamento dei processi	21
Arresto del servizio	21

Come il modus operandi delle minacce APT, i criminali informatici continuano a sfruttare strumenti legittimi a fini criminosi. Gli strumenti utilizzati influenzano le tecniche osservate, perché sono un mezzo per raggiungere un fine (in questo caso è una tecnica). Per esempio, PowerShell e Windows Command Shell sono spesso utilizzati per eseguire comandi aggiuntivi sul sistema, come la rimozione di copie "shadow", una strategia più comunemente associata alla tecnica di Inibizione del ripristino di sistema. Questo è anche il motivo per cui sono gli strumenti più utilizzati, come mostrato nell'immagine sottostante.

Nome dello strumento a linea di comando (attr)	Campagne uniche
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

L'utilizzo di VSSAdmin, BCDEdit e wevtutil indica che il ransomware si assicura che il sistema della vittima non possa tornare allo stato normale precedente all'attacco. L'utilizzo dello strumento reg mostra le modifiche apportate al Registro, che possono essere fatte per diversi motivi. I malware spesso utilizzano il Registro per stabilire una persistenza, ma per i ransomware non è così importante, poiché non ha alcuno scopo una volta terminata la crittografia. Piuttosto, può alterare altri parametri, per autorizzare alcune azioni che non sarebbero solitamente possibili. Rundll32 viene spesso utilizzato per caricare e eseguire una DLL, ma spesso è anche l'obiettivo di un'iniezione di processo.

Proprio come nel trimestre precedente a quello sopra citato, PowerShell e CMD sono in cima all'elenco esattamente per lo stesso motivo. Sono presenti anche VSSAdmin e BCDEdit, sebbene wevtutil (Windows Event Log Utility) non sia presente nell'elenco dei principali strumenti. Dato il basso numero di occorrenze degli strumenti citati, con la frequenza più alta di 13 in tutti i trimestri, non sorprende che non tutte le campagne utilizzino gli stessi strumenti. Un leggero scostamento può portare all'esclusione di tali strumenti.

Nome dello strumento a linea di comando (attr)	Campagne uniche
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

La minaccia del ransomware persiste.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

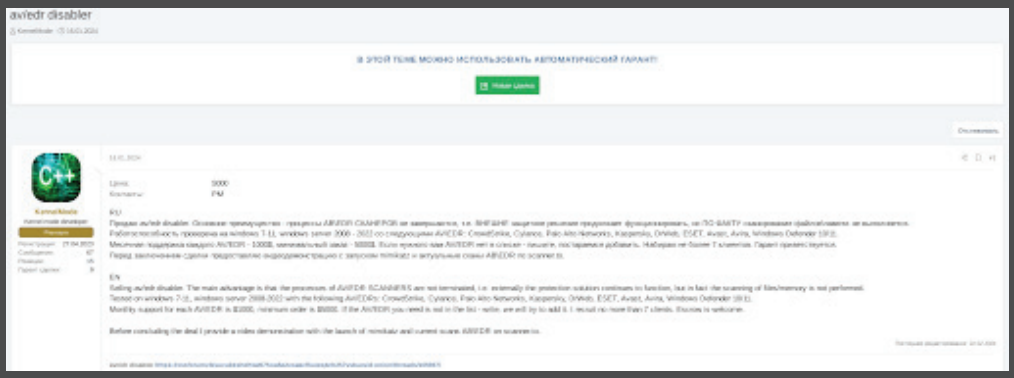
Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

La comparsa di strumenti di elusione e disattivazione dell'EDR

L'adozione delle soluzioni EDR da parte di numerose aziende nel mondo ha contribuito a migliorare il rilevamento, la comprensione e la risposta agli attacchi più sofisticati. I criminali informatici oggi spesso si affidano a file binari di sfruttamento delle risorse locali (LOLBin) e metodi di attacco più complessi, ma grazie alla presenza della tecnologia EDR è diventato più difficile eludere il rilevamento.

La sicurezza, tuttavia, rimane l'eterna lotta del gatto col topo e gli autori degli attacchi cercano nuovi modi per eludere o disabilitare le soluzioni EDR. Questo desiderio ha dato vita a una nuova generazione di strumenti e tecniche di elusione delle soluzioni EDR, alcune delle quali sono offerte su forum clandestini di criminali informatici. Come abbiamo visto prima, per esempio, il gruppo di ransomware D0nut si è fatto notare proprio grazie al suo strumento di disattivazione di EDR.



Annuncio relativo allo strumento di disattivazione delle soluzioni EDR sul forum clandestino XSS

Campagna di gennaio che utilizza lo strumento Terminator di Spyboy

Una tecnica d'attacco comune, definita BYOVD (Bring Your Own Vulnerable Driver), consiste nello sfruttare driver vulnerabili per ottenere l'esecuzione di codice con l'elevazione dei privilegi.

Un esempio di questo metodo è lo strumento di disattivazione di EDR "Terminator", sviluppato dal criminale informatico Spyboy. Lo strumento Terminator sfrutta un driver Windows legittimo ma vulnerabile che appartiene allo strumento antimalware Zemana per eseguire codice arbitrario dal kernel Windows sfruttando probabilmente la vulnerabilità CVE-2021-31728. Terminator è comparso online a metà del 2023 e Trellix ha pubblicato un articolo dettagliato sul suo centro informazioni in merito ai prodotti interessati, disponibile qui.

Dall'11 al 17 gennaio 2024, il Trellix Advanced Research Center ha rilevato una serie insolita di rilevamenti dello strumento Terminator di Spyboy nei dati di telemetria di Trellix, che sembra indicare una nuova campagna. Durante questi 6 giorni, la campagna Terminator ha avuto un picco per tre giorni ed è stata rilevata più volte in un unico ente della pubblica amministrazione, in una azienda di pubblica utilità nazionale e in una società di comunicazioni satellitari. Data la specificità degli obiettivi, Trellix stima con un elevato livello di fiducia che l'attacco sia legato al conflitto russo-ucraino.

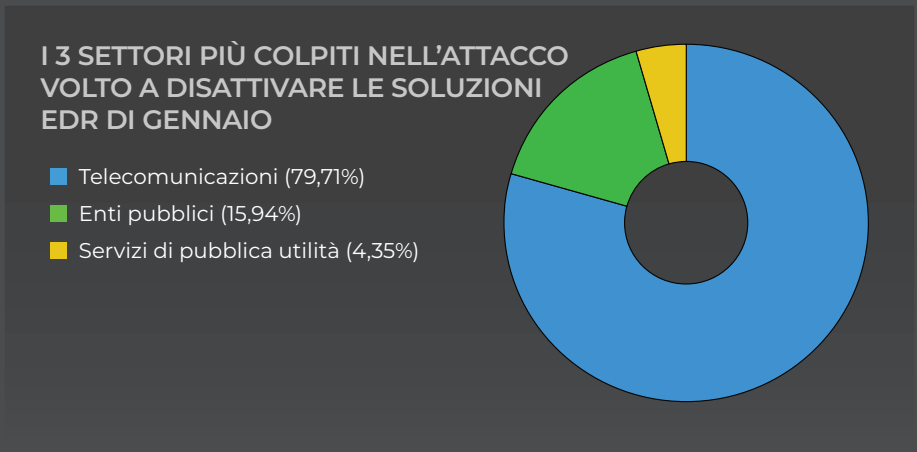
SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

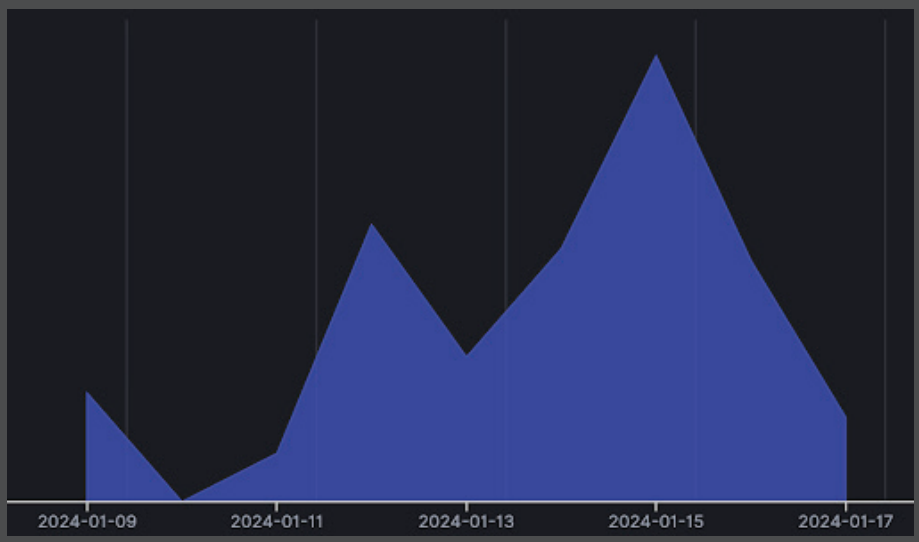
Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix



Rilevamenti di Trellix ATLAS degli attacchi contro l'Ucraina durante la campagna Terminator di gennaio

Moltiplicazione degli strumenti di disattivazione dell'EDR

All'inizio del 2023, AuKill, uno strumento con uno scopo simile era stato descritto da Sophos. Utilizzava, anche lui, un driver vulnerabile (BYOVD). I driver utilizzati da Terminator e AuKill sono diversi, ma sono entrambi innocui. Per contro, in alcune campagne nel 2022 strumenti simili avevano utilizzato driver dannosi personalizzati che dovevano essere caricati.



SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

L'uso improprio di driver legittimi per tali attacchi li rende più difficili da rilevare e coincide con il già citato utilizzo di LOLBin. Sebbene un codice binario e un driver siano tecnicamente diversi, l'intento e la motivazione sono simili, se non identici. Quando si parla dell'utilizzo di un driver legittimo, ricordiamo HermeticWiper apparso nel 2022. In quel caso, il driver è stato utilizzato per cancellare i dati di una macchina, piuttosto che disabilitare l'antivirus. Un altro punto in comune tra lo strumento Terminator di cui sopra e HermeticWiper è che sono entrambi attribuiti a un criminale informatico filorusso.

Abbiamo osservato anche un esempio dell'utilizzo della rete Discord per la distribuzione di malware presso uno dei nostri clienti in America Latina. Il nostro team ha rilevato che Discord continua a essere utilizzato per la distribuzione di malware come parte degli attacchi.

> **CONSIGLIO PER IL CISO:** è assolutamente imperativo che ogni SOC monitori attentamente le proprie soluzioni EDR. È necessario impostare avvisi e registrazioni in modo che se gli strumenti EDR vengono disattivati, il SOC ne venga immediatamente informato e possa intraprendere le azioni appropriate. La disattivazione degli strumenti EDR può essere un indicatore di manomissione e agire rapidamente è fondamentale per limitare l'accesso dell'autore dell'attacco alla rete. È inoltre fondamentale utilizzare una strategia di difesa in profondità che permette di fare ricorso ad altri strumenti, come la piattaforma NDR (Network Detection and Response), per rilevare potenziali incidenti.

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

L'email è ancora lo strumento preferito dagli autori degli attacchi

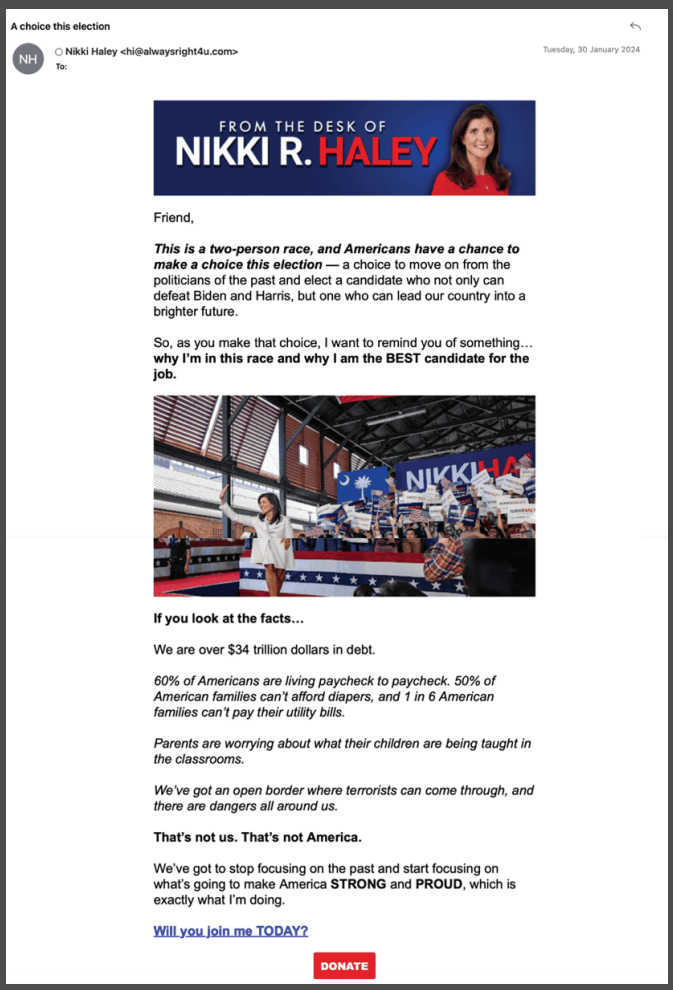
Trellix analizza due miliardi di campiono di email e 93 milioni di allegati email ogni giorno. Disponiamo così di un volume considerevole di dati e abbiamo molteplici occasioni di osservare le nuove tecniche utilizzate dagli autori degli attacchi per colpire le vittime via email.

Truffe delle donazioni elettorali

Le truffe di phishing legate alla raccolta dei fondi per le elezioni sfruttano le simpatie e il supporto per i candidati politici facendo leva sul patriottismo e utilizzando nomini di candidati noti. Nel primo trimestre 2024, i nostri ricercatori hanno scoperto che i criminali informatici utilizzano abusivamente servizi di marketing legittimi per creare pagine di raccolta fondi convincenti, abbellite con immagini di candidati accanto a bandiere americane, invitando i destinatari a fare una donazione.

Queste truffe utilizzano URL di servizi di marketing autentici per ingannare i destinatari, inducendoli a credere che le email siano legittime. In realtà, le email vengono inviate per sfruttare la generosità delle persone a loro vantaggio. I link all'interno delle email indirizzano gli utenti su pagine per la donazione, dove viene loro richiesto di inserire i dettagli finanziari o inviare contributi sul conto del mittente o su indirizzi del suo wallet.

I nostri ricercatori hanno osservato le seguenti email dannose che sfruttano la raccolta fondi per le elezioni.


A choice this election

NH Nikki Haley <hi@alwaysright4u.com>
To:
Tuesday, 30 January 2024

FROM THE DESK OF
NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Phishing delle imposte

Quando si parla di imposte fiscali, gli attacchi di phishing sono particolarmente preoccupanti. I truffatori si fingono agenzie governative, enti fiscali o società che offrono servizi di assistenza fiscale per spingere le persone a divulgare le proprie informazioni personali. I motivi sono molteplici: un debito di imposte arretrate, dichiarazioni dei redditi non presentate o il diritto a un rimborso fiscale. Il loro obiettivo finale è ottenere il tuo codice fiscale, i dettagli del tuo conto bancario o altri dati preziosi. L'email include link che sembrano portare su siti web della pubblica amministrazione o dell'Agenzia delle entrate ma che in realtà reindirizzano le vittime su siti fraudolenti studiati per rubare i dati.

Nel primo trimestre 2024, Trellix ha inoltre osservato un aumento delle email di questo tipo che sembravano provenire dall'Agenzia delle entrate australiana e le ha individuate con successo.

SOMMARIO

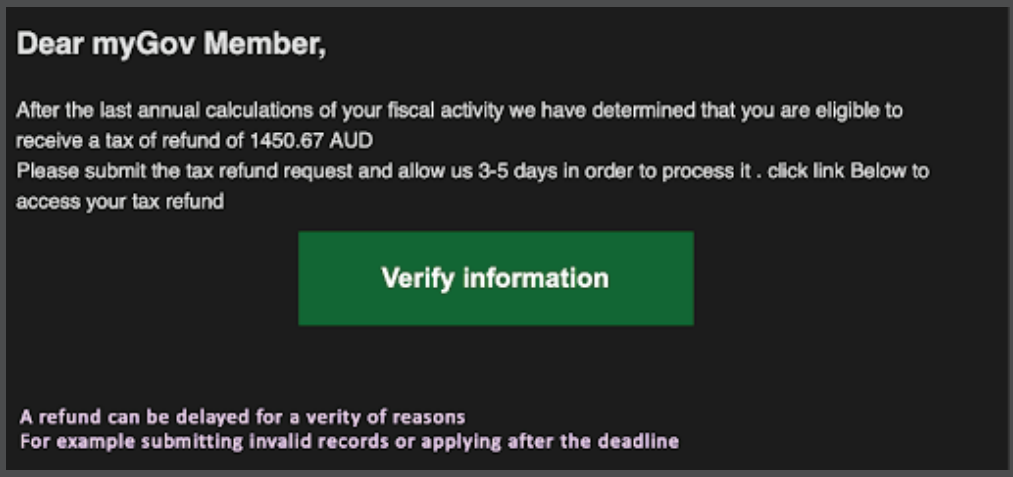
Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

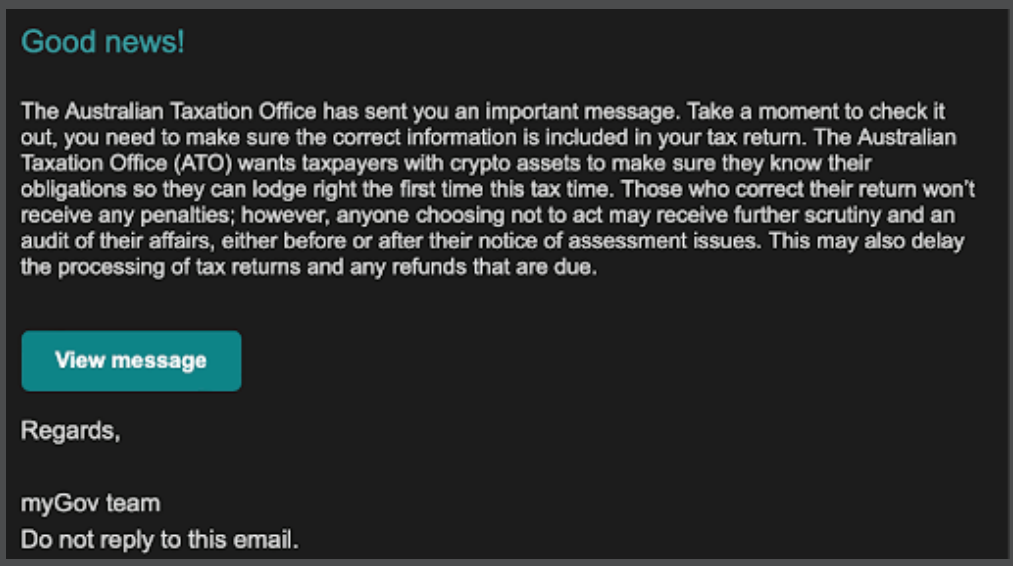
Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

Di seguito un esempio della campagna in cui si evince chiaramente che gli autori degli attacchi sollecitano con urgenza a fare clic sul link relativo al rimborso fiscale.





L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici

Intelligenza artificiale (IA) e machine learning non sono più accessibili solo alle aziende che dispongono di grandi budget. ChatGPT e simili possono essere utilizzati da chiunque, criminali inclusi, per cui l'intelligenza artificiale è diventata una corsa alle armi tra i criminali informatici e i professionisti della sicurezza. L'IA è uno strumento potente e dovrebbe essere sfruttata in modo responsabile per sviluppare gli obiettivi aziendali, ma è fondamentale che le aziende impediscano agli autori degli attacchi di avvantaggiarsene. È necessario utilizzare le nuove funzionalità per vincere in astuzia i criminali dal momento che le loro tattiche si affinano e le loro armi diventano più pericolose.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

CONSIGLIO PER IL CISO: il ruolo del CISO è diventato sempre più fondamentale perché deve guidare l'azienda in questo panorama in continua evoluzione. Con l'aumento degli attacchi informatici, le pressioni dell'IA e le responsabilità, non sorprende che il 90% dei CISO sia sempre più sotto pressione. Tenere il passo con l'IA e l'IA generativa è fondamentale. A questo proposito, la maggior parte dei CISO concorda sul fatto che le loro aziende potrebbero fare di più. Per saperne di più consulta l'ultimo report di Trellix Mind of the CISO: Decoding the GenAI Impact.

I criminali informatici adottano l'IA generativa per le sue funzionalità di apprendimento accelerate e la convenienza economica. In particolare, fornisce competenza: i criminali informatici posso creare email di spearphishing in qualsiasi lingua con una grammatica perfetta, loghi e informazioni di collegamento. I criminali informatici possono trovare, scrivere e testare exploit 10 volte più rapidamente senza particolari abilità.

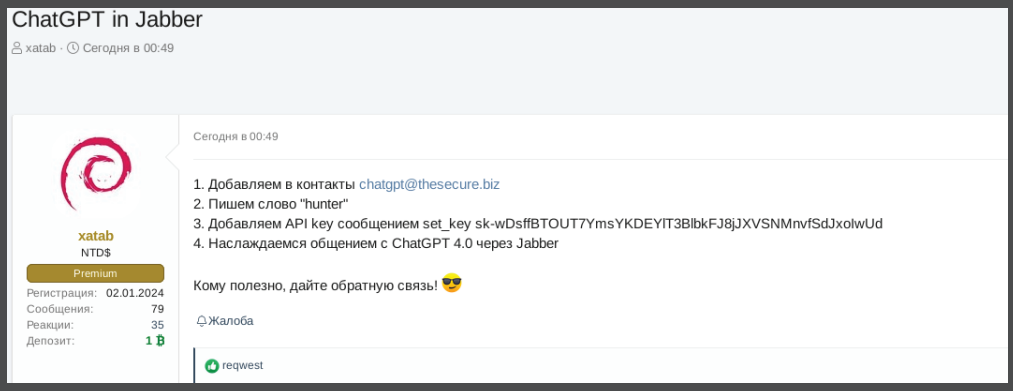
Il nostro team Advanced Research Center è regolarmente impegnato nella ricerca di tendenze nei mercati clandestini della criminalità informatica. L'IA generativa si sta diffondendo tra i criminali informatici che condividono i loro successi e vendono i loro strumenti. Dal nostro ultimo report, abbiamo osservato quanto segue dall'inizio del 2024.

Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo

A gennaio, abbiamo osservato che **xatab**, un autore di attacchi importante sul forum clandestino XSS, che cercava uno sviluppatore per creare un progetto "ChatGPT 4.0 in Jabber" insieme a un'API e alle istruzioni d'uso.

Oltre al fatto che i criminali informatici adottano le integrazioni LLM, è possibile che l'intento o la motivazione di **xatab** per il progetto fosse di intercettare e acquisire la corrispondenza di altri criminali informatici, per ascoltare di nascosto le loro richieste e ottenere informazioni e conoscenze sui loro interessi, i loro obiettivi e la portata delle loro attività illecite con il supporto dell'IA generativa.

Abbiamo osservato quanto segue:



Istruzioni e chiave dell'API del progetto "ChatGPT in Jabber" condivise da **xatab** sul forum XSS

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

```
Python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

Il 31 gennaio 2024, **xatab** ha offerto 2.000 dollari per il suo progetto 'ChatGPT in Jabber' sul forum XSS. Sulla base del recente reclamo XSS sollevato dal criminale informatico **germans**, che aveva creato il bot richiesto ma era stato inizialmente ignorato da **xatab**, sembra che **germans** abbia alla fine accettato di sviluppare un bot per 1.500 dollari. Creato per i server Jabber dei forum Exploit (@exploit[.]im) e XSS (@thesecure[.]biz) il bot è stato pubblicato sui forum Darknet Exploit e XSS da **xatab**, presumibilmente per testarlo e conoscere il parere dei membri del forum. Il bot potrebbe essere basato sul progetto xmppgpt.

Nei messaggi pubblicati sui forum Exploit e XSS, l'autore dell'attacco **xatab** si presenta come un gruppo APT (noto in certi ambienti come esperti in test di penetrazione) interessato ad assumere un broker di accessi aziendali per gli Stati Uniti, Regno Unito, Canada e Australia al fine di una proficua collaborazione. Ha offerto il 20% dei ricavi generati da ogni accesso e ha depositato un bitcoin su entrambi i forum, Exploit e XSS, per dimostrare la serietà della sua offerta.

Fornendo uno strumento ChatGPT 4.0 gratuitamente alla comunità di criminali informatici **xatab** ottiene due cose:

1. Gioca un ruolo di catalizzatore e facilitatore, desideroso di aiutare i criminali informatici a innovare e a adottare l'IA generativa nelle loro operazioni.
2. Tentare di creare una base/vivaio di conoscenze di IA generativa per trarre vantaggio dalle conoscenze di altri criminali informatici o addirittura appropriarsi delle loro idee e dei loro strumenti innovativi.

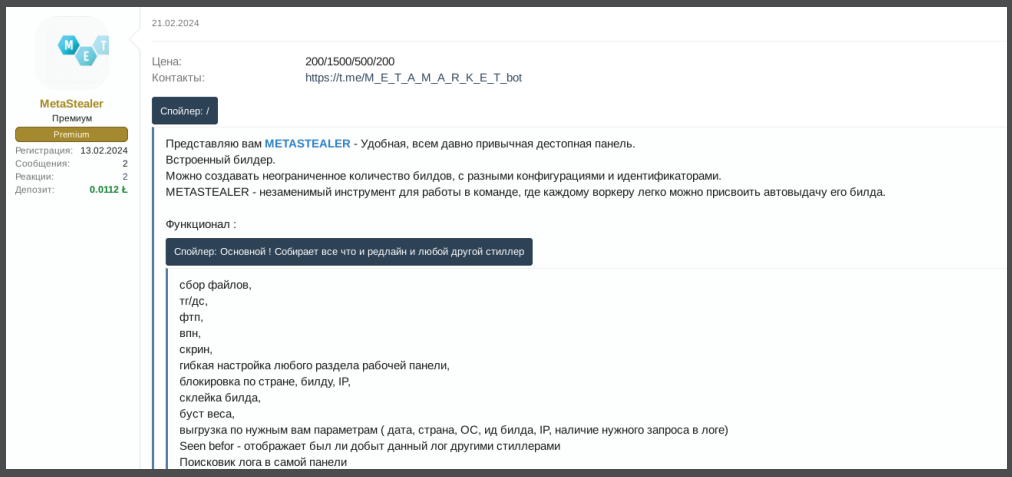
Trellix ha testato il progetto "ChatGPT in Jabber" utilizzando le istruzioni fornite, e sembra che funzioni come previsto dal criminale informatico.

Integrazione dell'IA generativa negli infostealer

Il 21 febbraio 2024, il criminale informatico MetaStealer ha pubblicizzato una nuova versione migliorata di **MetaStealer** sul forum XSS. MetaStealer è un infostealer (strumento di esfiltrazione delle informazioni) apparso per la prima volta nel 2021, che si ritiene sia derivato dal famoso Redline. Sono state osservate diverse versioni di **MetaStealer** nell'ambiente reale, tuttavia la versione recente individuata da Trellix ha una funzione basata sull'IA generativa per evitare il rilevamento.

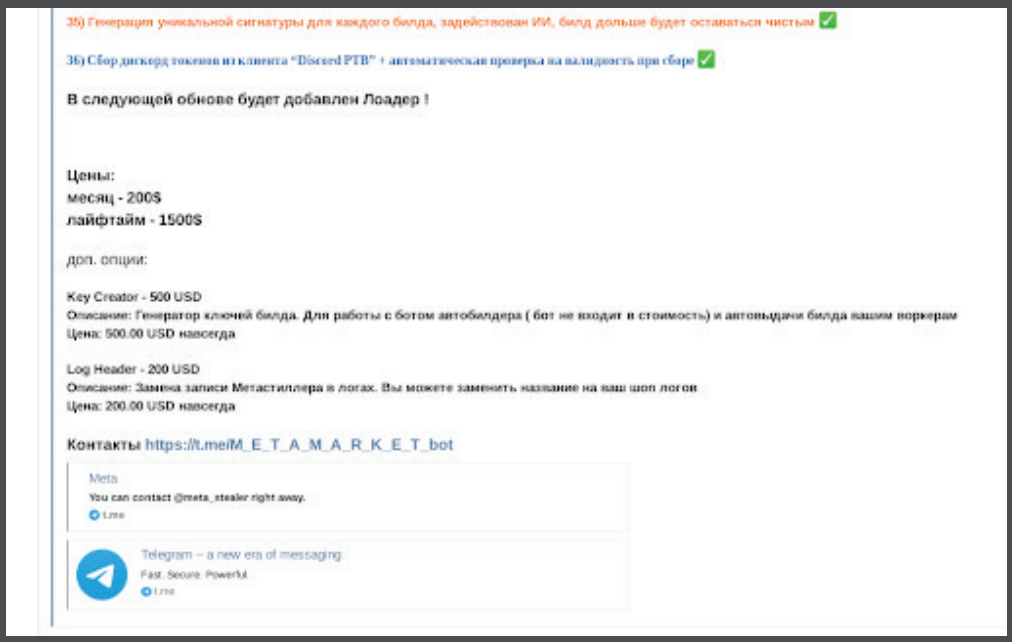
SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix



Pubblicazione della versione rinnovata di MetaStealer da parte del criminale informatico **MetaStealer** sul forum XSS

Nella schermata qui di seguito, il testo arancione al punto 35) si traduce come segue: "Firme uniche vengono generate per ogni build. Poiché viene utilizzata l'IA, la build elude il rilevamento per un periodo di tempo più lungo". Ciò suggerisce che gli sviluppatori di MetaStealer hanno incorporato una nuova funzionalità basata sull'IA generativa nel loro strumento che consente loro di creare build uniche di MetaStealer per eludere il rilevamento da parte delle soluzioni antivirus e EDR per un periodo di tempo più lungo rispetto a prima.



Integrazione di una funzione basata sull'IA generativa nella versione rinnovata di MetaStealer per eludere le difese

Un altro esempio è un infostealer consolidato denominato LummaStealer. A partire dall'agosto 2023, il team LummaStealer testa una funzione basata sull'IA che permette agli utenti di questo infostealer di rilevare i bot nell'elenco dei registri. Il sistema basato sull'IA incorporato in LummaStealer è una rete neurale personalizzata, addestrata a rilevare se un registro utente sospetto è un bot o meno. LummaStealer utilizza un'etichetta **AI!Bot.<numero>** per categorizzare il registro rilevato come bot.

SOMMARIO

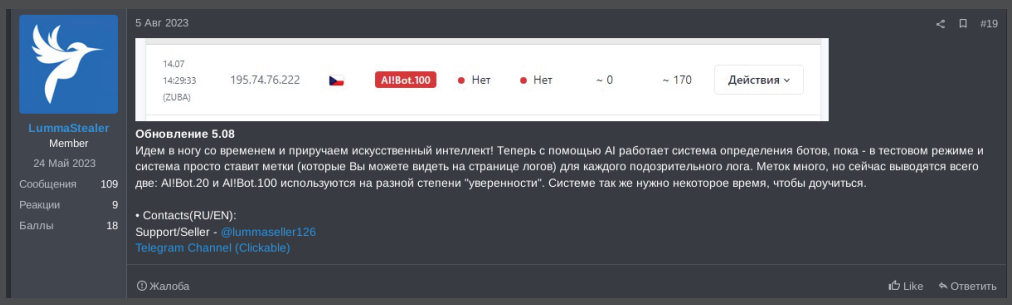
Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

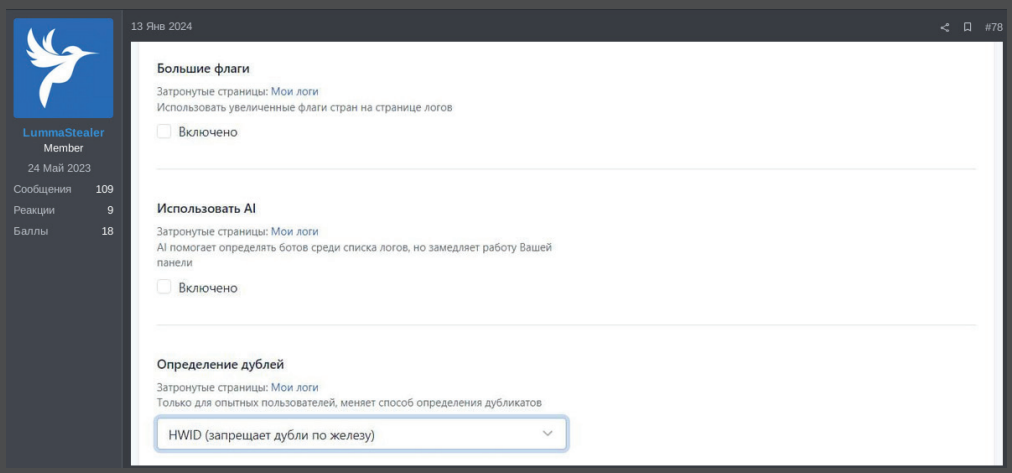
Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

La variabile <numero>, il cui raggio d'azione sembra essere compreso tra 0 e 100, rappresenta la certezza del rilevamento di un bot:



Messaggio di LummaStealer sul forum RAMP in cui l'autore dell'attacco ha annunciato l'integrazione di una funzione basata sull'IA per rilevare i bot nell'elenco dei registri dell'infostealer

LummaStealer ha avvisato i suoi utenti che la rete neurale è ancora in fase di addestramento e che sarà necessario del tempo per migliorare la precisione del rilevamento. Inoltre, nel gennaio 2024, **LummaStealer** ha avvisato di aver disabilitato la funzione basata sull'IA generativa per impostazione predefinita perché rallenta le prestazioni di esecuzione di LummaStealer.



Messaggio di LummaStealer sul forum RAMP in cui l'autore dell'attacco segnala che il rilevamento dei bot è disattivato per impostazione predefinita

Progetto "Telegram Pro Poster"

All'inizio di marzo 2024, il criminale informatico pepe ha pubblicato il suo progetto "Telegram Pro Poster" sul forum XSS come parte di una gara clandestina di strumenti/software dannosi. Telegram Pro Poster è un bot destinato "all'automazione avanzata dei messaggi Telegram". Questo bot sviluppato con Python permette agli utenti di gestire molteplici (una quantità illimitata di) canali Telegram in modo autonomo, copiando automaticamente i post dai canali Telegram "distributori" sui canali di destinazione. Tra le numerose funzionalità di filtraggio dei messaggi, questo bot ha due funzioni di IA generativa integrate per la traduzione dei messaggi Telegram e la parafrasi di un determinato messaggio utilizzando ChatGPT.

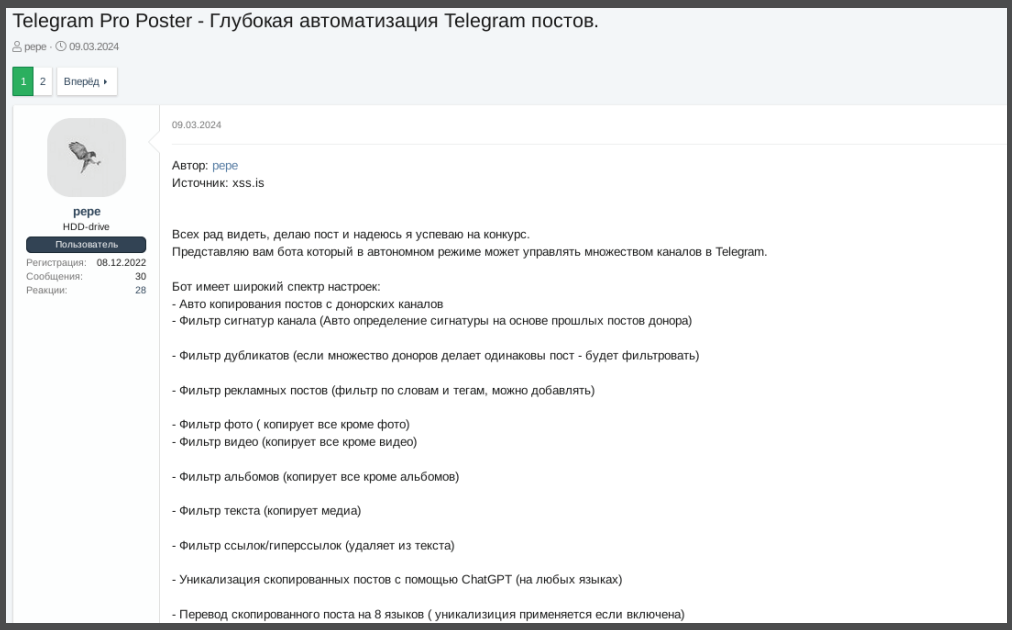
SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

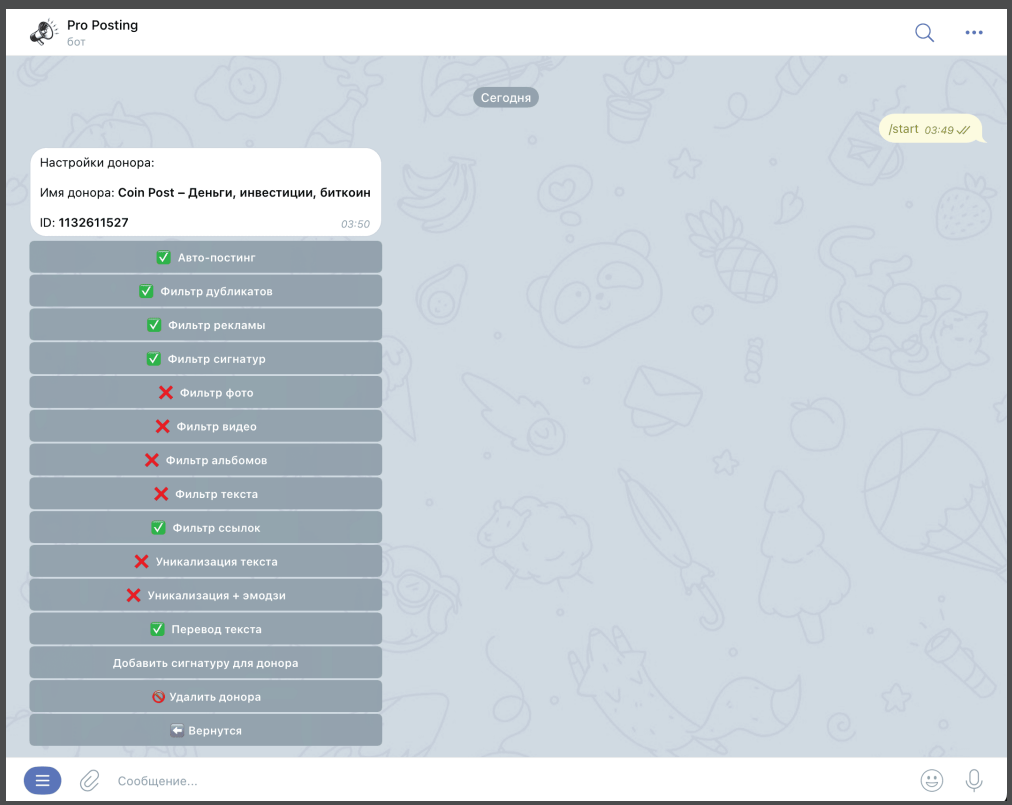
Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix



Messaggio sul forum XSS relativo al bot basato sull'IA generativa del progetto "Telegram Pro Poster"



Funzionalità di filtraggio di Telegram Pro Poster, compresa la funzione di personalizzazione/parafrasi," disattivata per impostazione predefinita

Trellix ha ottenuto il codice sorgente di Telegram Pro Poster e identificato i seguenti segmenti di codice, responsabili della traduzione dei messaggi copiati dai canali "distributori" tramite l'API di ChatGPT nelle otto lingue indicate prima di inviarli ai canali Telegram di destinazione:

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

La seconda funzione, volta a personalizzare in modo unico il messaggio, è disabilitata per impostazione predefinita. Tuttavia, quando è attiva utilizza OPEN_AI_KEY per richiedere a ChatGPT di parafrasare il testo dato nella lingua desiderata e aggiungere opzionalmente un'emoji.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

SOMMARIO

- Premessa
- Prefazione
- Introduzione: Report sulle minacce informatiche Giugno 2024
  - L'impatto degli eventi geopolitici sul dominio informatico
  - Fatti salienti delle minacce in breve
  - Metodologia: come raccogliamo e analizziamo i dati
- Segnalazioni, dati e analisi
  - Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
    - Gruppi sponsorizzati dagli Stati e APT attivi
    - Gruppi APT e Paesi di origine
    - Paesi e regioni colpiti
    - Strumenti dannosi
    - Strumenti non dannosi
    - Conclusione
  - Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
    - Panoramica
    - Calendario operativo
    - Tattiche, tecniche e procedure (TTP)
  - Evoluzione del panorama del ransomware
    - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
    - Prospettiva globale sul ransomware
  - La comparsa di strumenti di elusione e disattivazione dell'EDR
    - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
    - Moltiplicazione degli strumenti di disattivazione dell'EDR
  - L'email è ancora lo strumento preferito dagli autori degli attacchi
    - Truffe delle donazioni elettorali
    - Phishing delle imposte
  - L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
    - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
    - Integrazione dell'IA generativa negli infostealer
    - Progetto "Telegram Pro Poster"
- Conclusione
- Metodologia
  - Applicazione: come utilizzare queste informazioni
  - Come comprendere l'analisi presentata in questo report
- Risorse
  - Informazioni su Trellix Advanced Research Center
  - A proposito di Trellix

I commenti della comunità XSS di criminali informatici sta già condividendo riscontri positivi sul "progetto Telegram Pro Poster", affermando che è un progetto interessante e che in mani capaci questo strumento sarà sicuramente utile. Su un thread del forum XSS, un altro criminale informatico ha indicato che questo bot era già stato adottato da diversi canali Telegram.

CONCLUSIONE

La corsa è iniziata

La Threat Intelligence operativa fornisce informazioni sulla natura, l'intento e i periodi di attività di minacce informatiche specifiche. È più dettagliata e ricca di contesto rispetto alla Threat Intelligence tattica, poiché include informazioni sulle tattiche, tecniche e procedure (TTP) dei criminali informatici.

Le aziende possono utilizzare questa Threat Intelligence operativa per comprendere il contesto più ampio degli attacchi informatici, come le motivazioni alla base o i metodi utilizzati, aiutando i team della sicurezza ad anticipare e prepararsi ai tipi di attacchi specifici.

Lavorando con i clienti, so che l'obiettivo più importante di ogni CISO è limitare i rischi per la propria azienda. L'utilizzo della Threat Intelligence operativa è un modo tangibile per limitare quel rischio poiché permette ai CISO e ai loro team SecOps di anticipare e porre le basi necessarie. Permette loro di identificare le lacune nelle loro misure di sicurezza sull'intera superficie d'attacco dell'azienda e di entrare nella mente dei loro avversari, per cercare di metterli fuori strada.

Condividiamo la nostra Threat Intelligence per fornirti le informazioni oggettive di cui hai bisogno per le decisioni più importanti che dovrai prendere. Il nostro obiettivo è aiutarti a migliorare considerevolmente le tue difese informatiche e mantenere un vantaggio sui criminali informatici.

Partiamo!

Ashok Banerjee,
CHIEF TECHNOLOGIST, TRELLIX

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione

Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

METODOLOGIA

Acquisizione: Trellix e gli esperti del team Trellix Advanced Research Center raccolgono le statistiche, le tendenze e i risultati delle analisi che compongono questo report da un'ampia gamma di fonti globali.

- **Fonti bloccate:** in alcuni casi i dati di telemetria sono generati dalle soluzioni di sicurezza Trellix presenti nelle reti di sicurezza informatica dei clienti, nonché nei framework di difesa impiegati in tutto il mondo nelle reti del settore pubblico e privato, comprese quelle che distribuiscono servizi tecnologici, di infrastruttura o di dati. Questi sistemi, nell'ordine di milioni, generano dati a partire da un miliardo di sensori.
- **Fonti aperte:** in altri casi, Trellix si avvale di una combinazione di strumenti brevettati, proprietari e open source per esaminare siti, registri e archivi di dati presenti in Internet oltre che nel dark web, come i "siti di divulgazione", o i gruppi di ransomware che pubblicano informazioni riguardanti le vittime del ransomware o di proprietà di queste ultime.

Normalizzazione: i dati aggregati alimentano le nostre piattaforme Insights e ATLAS. Sfruttando il machine learning, l'automazione e l'acutezza umana, il team passa attraverso una serie di processi intensivi, integrati e iterativi per normalizzare i dati, arricchire i risultati, rimuovere i dati personali e identificare le correlazioni fra i vari metodi di attacco, agent, settori, regioni, strategie e risultati.

Analisi: in seguito, Trellix analizza questo ampio archivio di informazioni, confrontandole con: (1) la sua ampia knowledgebase di Threat Intelligence, (2) i report di settore sulla sicurezza informatica prodotti da fonti molto autorevoli e accreditate, (3) l'esperienza e gli approfondimenti dei propri analisti, investigatori, specialisti in reverse engineering, analisi forense e vulnerabilità.

Interpretazione: infine, il team di Trellix estrae, rivede e convalida i dati significativi che aiuteranno i responsabili e i loro team SecOps a: (1) comprendere le ultime tendenze nell'ambiente delle minacce informatiche e (2) a utilizzare queste informazioni per migliorare la capacità di prevedere, prevenire e bloccare i futuri attacchi.

Applicazione: come utilizzare queste informazioni

È fondamentale che qualsiasi team di valutazione, leader del settore, comprenda, riconosca e, ove possibile, mitighi l'effetto del pregiudizio, ossia l'inclinazione naturale, insita o invisibile, ad accettare, rifiutare o manipolare i fatti e il loro significato. Lo stesso principio vale per i consumatori dei contenuti.

A differenza di un test o esperimento matematico altamente strutturato e basato su controlli, questo report è per sua natura un esempio di comodità: un tipo di studio non probabilistico spesso utilizzato nei test medici, psicologici e sociologici che si basa su dati disponibili e accessibili.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

- In breve, i risultati qui esposti si basano su ciò che possiamo osservare e, chiaramente, non includono prove relative alle minacce, agli attacchi o alle tattiche che hanno eluso il rilevamento, la segnalazione e l'acquisizione dei dati.
- In assenza di informazioni "complete" o di una visibilità "perfetta", questo è il tipo di studio più adatto all'obiettivo del presente report: identificare fonti note di dati critici sulle minacce alla sicurezza informatica e sviluppare interpretazioni razionali, esperte ed etiche di questi dati per informare e mettere in atto le migliori pratiche di difesa informatica.

Come comprendere l'analisi presentata in questo report

Per comprendere gli approfondimenti e i dati contenuti in questo report è necessario rivedere brevemente le seguenti linee guida:

- **Un'istantanea temporale:** nessuno ha accesso a tutti i registri di tutti i sistemi connessi a Internet, non tutti gli incidenti di sicurezza vengono segnalati e non tutte le vittime vengono ricattate e pubblicate sui siti di divulgazione. Tuttavia, monitorando e tracciando ciò che sappiamo, possiamo ottenere una migliore comprensione delle varie minacce, riducendo al contempo i punti ciechi nell'analisi e nelle indagini.
- **Falsi positivi e falsi negativi:** tra le caratteristiche tecniche ad alte prestazioni degli speciali sistemi di tracciamento e telemetria di Trellix per la raccolta dei dati ci sono meccanismi, filtri e tattiche che aiutano a ridurre o rimuovere i falsi positivi e falsi negativi. Ciò permette di elevare il livello di analisi e la qualità dei nostri risultati.
- **Rilevamenti, non infezioni:** per dati di telemetria intendiamo i dati relativi ai rilevamenti, non alle infezioni. Un rilevamento viene registrato quando un file, URL, indirizzo IP o altri indicatori viene rilevato da uno dei nostri prodotti e ci viene poi segnalato.
- **Acquisizione non uniforme dei dati:** alcune serie di dati richiedono un'attenta interpretazione. I dati del settore delle telecomunicazioni, ad esempio, includono la telemetria dei clienti ISP che operano in molti altri settori.
- **Assegnazione degli attacchi sponsorizzati dagli Stati:** analogamente, attribuire la responsabilità di vari attacchi e minacce informatiche a un gruppo sponsorizzato dallo stato può essere molto difficile, data la pratica comune fra questi gruppi di usurpare l'identità di un altro collettivo o di far sembrare le attività dannose come provenienti da una fonte affidabile.

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
L'impatto degli eventi geopolitici sul dominio informatico
Fatti salienti delle minacce in breve
Metodologia: come raccogliamo e analizziamo i dati
Segnalazioni, dati e analisi
Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
Gruppi sponsorizzati dagli Stati e APT attivi
Gruppi APT e Paesi di origine
Paesi e regioni colpiti
Strumenti dannosi
Strumenti non dannosi
Conclusione
Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
Panoramica
Calendario operativo
Tattiche, tecniche e procedure (TTP)
Evoluzione del panorama del ransomware
Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
Prospettiva globale sul ransomware
La comparsa di strumenti di elusione e disattivazione dell'EDR
Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
Moltiplicazione degli strumenti di disattivazione dell'EDR
L'email è ancora lo strumento preferito dagli autori degli attacchi
Truffe delle donazioni elettorali
Phishing delle imposte
L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
Integrazione dell'IA generativa negli infostealer
Progetto "Telegram Pro Poster"
Conclusione
Metodologia
Applicazione: come utilizzare queste informazioni
Come comprendere l'analisi presentata in questo report
Risorse
Informazioni su Trellix Advanced Research Center
A proposito di Trellix

RISORSE

Archivi dei Report sulle minacce

The Mind of the CISO

SEGUI TRELLIX ARC SU X

Trellix ARC

Consulta l'archivio dei report sulle minacce informatiche

Trellix Advanced Research Center

SOMMARIO

Premessa

Prefazione

Introduzione: Report sulle minacce informatiche Giugno 2024

- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi

- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione

Metodologia

- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse

- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix

INFORMAZIONI SU TRELLIX ADVANCED RESEARCH CENTER

Il Trellix Advanced Research Center è all'avanguardia nello studio di metodi, tendenze e strumenti utilizzati dai gruppi di criminali informatici nel panorama delle minacce. Il nostro team d'elite di ricercatori è il partner imprescindibile di CISO, responsabili della sicurezza e dei loro team SecOps in tutto il mondo. Il Trellix Advanced Research Center fornisce una Threat Intelligence operativa e strategica di prim'ordine agli analisti di sicurezza. Alimenta la nostra avanzata piattaforma XDR, basata sull'IA, e offre prodotti e servizi di Threat Intelligence ai clienti in tutto il mondo. Per saperne di più, visita il sito https://www.trellix.com/it-it/advanced-research-center.html.

A PROPOSITO DI TRELLIX

Trellix è un'azienda internazionale che ridefinisce il futuro della cyber security. La piattaforma XDR (eXtended Detection and Response) aperta e nativa di Trellix aiuta le aziende a proteggersi dalle minacce sempre più sofisticate che ogni giorno si trovano ad affrontare, e a gestire le proprie attività di business in modo sicuro e con resilienza. Gli esperti di sicurezza di Trellix, insieme all'ampio ecosistema di partner, accelerano l'innovazione tecnologica attraverso l'intelligenza artificiale, l'automazione e le analisi per supportare oltre 40.000 clienti in ambito privato e pubblico. Per saperne di più, visita il sito https://trellix.com.

Questo documento e le informazioni in esso contenute descrivono le ricerche sulla sicurezza informatica e sono fornite esclusivamente a titolo informativo a beneficio dei clienti di Trellix. Trellix conduce ricerche in conformità con la sua Policy di divulgazione responsabile delle vulnerabilità | Trellix. Qualsiasi tentativo di ricreare in tutto o in parte le attività descritte è esclusivamente a rischio dell'utente. Trellix e le sue società affiliate declinano ogni responsabilità al riguardo.

Trellix è un marchio registrato di Musarubra US LLC o sue affiliate negli Stati Uniti e/o in altri paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi.

Trellix

Copyright © 2024 Musarubra US LLC

SOMMARIO

Premessa
Prefazione
Introduzione: Report sulle minacce informatiche Giugno 2024
- L'impatto degli eventi geopolitici sul dominio informatico
- Fatti salienti delle minacce in breve
- Metodologia: come raccogliamo e analizziamo i dati

Segnalazioni, dati e analisi
- Attacchi sponsorizzati dagli Stati e minacce persistenti avanzate (APT)
  - Gruppi sponsorizzati dagli Stati e APT attivi
  - Gruppi APT e Paesi di origine
  - Paesi e regioni colpiti
  - Strumenti dannosi
  - Strumenti non dannosi
  - Conclusione
- Volt Typhoon: gruppo sponsorizzato dallo stato affiliato alla Cina
  - Panoramica
  - Calendario operativo
  - Tattiche, tecniche e procedure (TTP)
- Evoluzione del panorama del ransomware
  - Operation Cronos, l'operazione delle forze dell'ordine che ha colpito duramente LockBit
  - Prospettiva globale sul ransomware
- La comparsa di strumenti di elusione e disattivazione dell'EDR
  - Campagna di gennaio che utilizza lo strumento Terminator di Spyboy
  - Moltiplicazione degli strumenti di disattivazione dell'EDR
- L'email è ancora lo strumento preferito dagli autori degli attacchi
  - Truffe delle donazioni elettorali
  - Phishing delle imposte
- L'IA generativa al cuore di una corsa agli armamenti: osservazioni sul mercato clandestino dei criminali informatici
  - Il progetto 'ChatGPT in Jabber' verosimilmente utilizzato da un gruppo APT russo
  - Integrazione dell'IA generativa negli infostealer
  - Progetto "Telegram Pro Poster"

Conclusione
Metodologia
- Applicazione: come utilizzare queste informazioni
- Come comprendere l'analisi presentata in questo report

Risorse
- Informazioni su Trellix Advanced Research Center
- A proposito di Trellix