REPORT SULLE MINACE INFORMATICHE

Giugno 2023

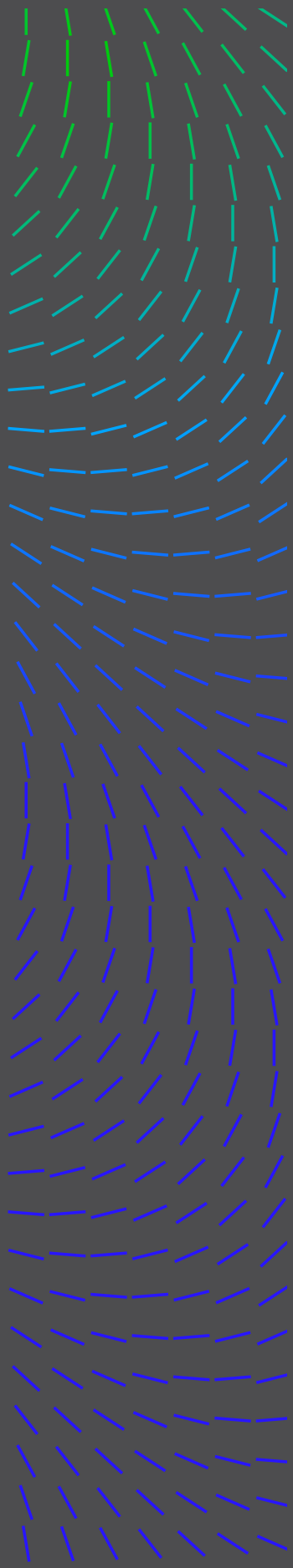
Informazioni raccolte dalla rete globale di esperti, sensori, dati di telemetria e Threat Intelligence

Presentato da

Trellix ADVANCED RESEARCH CENTER

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 sui dati e le informazioni acquisiti fra il 1° gennaio e il 31 marzo 2023.



Le minacce informatiche continuano a evolversi e a moltiplicarsi, a ritmo sostenuto e su vasta scala.

I team SecOps fanno il possibile per difendere informazioni, risorse e operazioni, ma nessuno di loro ha una visibilità completa sul panorama delle minacce.

In effetti, per avere una tale visibilità è necessaria una prospettiva ampia, numerose fonti, molteplici flussi di dati, una threat intelligenze grezza e importanti volumi di dati di telemetria.

Per ottenere informazioni fruibili, è necessario disporre di una visione strategica su un gran numero di aziende, settori, regioni e superfici d'attacco.

Benvenuto nell'edizione di giugno 2023 del Report sulle minacce informatiche.

COMPRENDERE I RISCHI, LE MINACCE E LE VULNERABILITÀ PRESE DI MIRA DAI PIRATI INFORMATICI

Passo molto tempo a parlare con membri del consiglio d'amministrazione, CEO, CISO, CIO, CTO e altri responsabili della difesa informatica di nazioni, enti governativi e aziende private di diversi settori.

La gamma degli argomenti che trattiamo è ampia: dalla ricerca mondiale, all'innovazione alla Threat Intelligence fino alle più recenti prassi di difesa informatica dei rispettivi Team SecOps. Parliamo delle problematiche che si trovano ad affrontare, recentemente identificate da Trellix nel suo report "La mente dei CISO": troppe fonti di informazione diverse (35%), l'evoluzione degli obblighi normativi e dei requisiti legali (35%), l'ampliamento delle superfici di attacco (34%), la carenza di personale qualificato (34%) e la mancanza di supporto da parte degli altri dipartimenti aziendali (31%)[1].

Praticamente tutte queste interazioni riguardano, direttamente o indirettamente, la natura del panorama delle minacce. Quali tipi di attacco sono più diffusi? Quali sono i gruppi di ransomware più pericolosi? Quali sono le vulnerabilità prese di mira? Quali nazioni sembrano essere le più attive? Quali tendenze in materia di minacce osserviamo tramite i nostri sistemi di sicurezza di email e rete?

"Queste conoscenze, disponibili in questo report e nella ricca libreria di risorse di Trellix, sono spesso fondamentali per la missione di dirigenti, CEO, CISO, CIO, CTO e team SecOps".

Essendo tutti i giorni in prima linea, noi di Trellix abbiamo molto da dire al riguardo. Attingiamo a un enorme archivio di Threat Intelligence, analisi e dati ottenuti da oltre un miliardo di sensori in tutto il mondo. Queste conoscenze, disponibili in questo report e nella ricca libreria di risorse di Trellix, sono spesso fondamentali per la missione di dirigenti, CEO, CISO, CIO, CTO e team SecOps.

Questo eccellente rapporto è stato compilato dal mio collega John Fokker, responsabile della Threat Intelligence nel team esperto Trellix Advanced Research Center. Sfrutta queste informazioni ricche e pertinenti per concentrare le attività del tuo team, consolidare i tuoi processi e implementare le giuste tecnologie XDR. Facci sapere quali argomenti vorresti venissero trattati nelle prossime edizioni per aiutarti a proteggere e a far crescere la tua azienda.

Joseph (Yossi) Tal
SVP, DIRETTORE DEL TRELLIX ADVANCED RESEARCH CENTER

A SOSTEGNO DEGLI EROI IN PRIMA LINEA NELLA LOTTA CONTRO LA CRIMINALITÀ INFORMATICA

Io lavoro con degli eroi. Non mi riferisco però al mio gruppo, nonostante le loro brillanti carriere nel settore pubblico e privato.

Mi riferisco a te. Parlo delle persone e dei team di tutto il mondo che utilizzano le funzionalità di ricerca avanzata di Trellix (i nostri sistemi, le nostre informazioni e la nostra Threat Intelligence) per proteggere le loro aziende dagli attacchi informatici. CISO, CTO e CIO certo, ma anche i nostri colleghi presso agenzie quali Europol, FBI, NSA, CISA (Cybersecurity and Infrastructure Security Agency), ACSC (Australian Cyber Security Centre) e NCSC (National Cyber Security Centre) del Regno Unito. Altrettanto importante, e forse anche di più, parlo di ogni membro del tuo team SecOps.

"Come ben sai dal tuo lavoro quotidiano, la sicurezza informatica si sta evolvendo molto rapidamente: innovazioni tecnologiche, adozione dell'XDR."

Quali pensi che siano i fattori determinanti per la tua missione SecOps? i responsabili della sicurezza informatica di tutto il mondo hanno condiviso le loro opinioni nel report Trellix sopra menzionato dal mio collega Yossi. Hanno citato migliore visibilità (44%), migliore prioritizzazione (42%), collaborazione più ampia per contrastare gli attacchi multivettore (40%) e una maggiore precisione (37%)[2].

Ciascuno di questi fattori si basa fondamentalmente su informazioni e dati accurati, come i contenuti di questo report.

Come ben sai dal tuo lavoro quotidiano, la sicurezza informatica si sta evolvendo molto rapidamente: innovazioni tecnologiche, adozione dell'XDR, evoluzioni delle normative e delle leggi, cambiamenti nel panorama delle minacce, ecc. È in corso una rivoluzione, una trasformazione nel modo in cui i team SecOps possono stare un passo più avanti rispetto alla prossima generazione di attacchi informatici. La vittoria comincia sempre dalle informazioni e da una precisa comprensione dello stato attuale.

Uniamo le nostre forze. Puoi fare affidamento su Trellix. Questo report è destinato a te.

John Fokker
RESPONSABILE DELL'INTELLIGENCE SULLE MINACCE E PRINCIPAL ENGINEER
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, "2023 Report: The Mind of the CISO," 2023.
[2] Trellix, "2023 Report: The Mind of the CISO," 2023.

INTRODUZIONE

Contesto strategico: un mondo inquieto

Per interpretare i dati presenti in questo report è necessario avere una visione d'insieme su scala globale. In effetti le minacce informatiche che prendono di mira le aziende di tutto il mondo non esistono nel nulla. Fra i fattori principali dei rischi informatici rientrano le guerre e altri casi di forza maggiore, i cambiamenti economici e le nuove vulnerabilità che possono emergere ogni volta che un team apporta dei cambiamenti a modelli aziendali, partner chiave, processi fondamentali, adozione di tecnologie e conformità normative. Ecco alcuni dei fattori che hanno influenzato i dati sulle minacce nel primo trimestre 2023.

L'invasione russa dell'Ucraina e la guerra asimmetrica contro l'Occidente: gli attacchi informatici lanciati da stati-nazione a scopo di spionaggio, guerra e disinformazione al servizio di ambizioni politiche, economiche e territoriali continua a intensificarsi. Gli hacker sferrano attacchi informatici sempre più sofisticati contro imprese, infrastrutture ed enti pubblici occidentali.

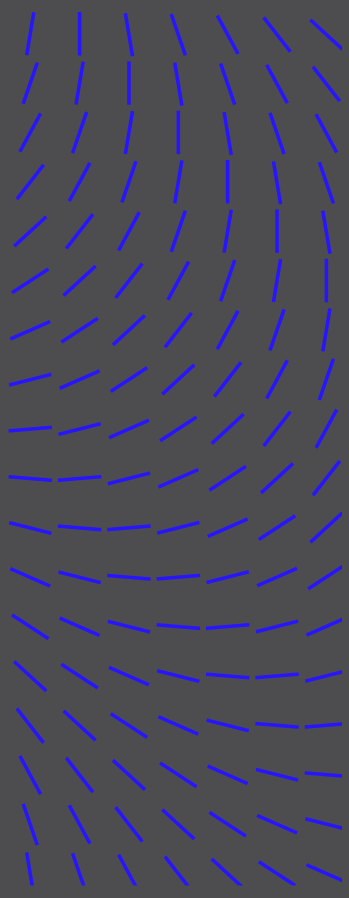
La morsa di Xi Jinping sulla Cina e le sue ambizioni geopolitiche: gli obiettivi nazionalistici, la politica estera decisa e le pratiche di spionaggio industriale della Cina continuano ad aumentare i rischi informatici, mentre i gruppi APT affiliati alla Cina dominano il panorama globale.

Le economie in via di sviluppo e la rapida espansione delle infrastrutture: molti paesi in via di sviluppo stanno ampliando infrastrutture e tecnologia di pari passo alla loro crescita economica, ma spesso la sicurezza informatica viene trascurata, portando a numerose vulnerabilità informatiche nelle infrastrutture critiche.

L'inflazione globale e il suo impatto politico ed economico: questo trimestre ha visto volatilità del mercato, crisi finanziarie e politiche e pressioni sulle priorità di spesa e sui budget per la sicurezza informatica.

La supply chain ancora scossa dopo il COVID: nuove viene d'accesso al mercato in tutte le regioni hanno portato a cambiamenti nei partner, nelle reti di trasporto, nella condivisione delle informazioni e, di conseguenza, nei rischi informatici. Poiché le minacce informatiche hanno un impatto quotidiano sulla filiera, la necessità di funzionalità Zero Trust rimane forte in tutti i settori.

Il mito della superiorità dell'ambiente di sicurezza di Apple: questo mito persiste, nonostante gli ambienti macOS non possano più essere considerati sicuri. I criminali informatici sfruttano su vasta scala il malware basato su Golang e moltiplicano i vettori di attacco per coprire numerosi sistemi operativi.



L'intelligenza artificiale è arrivata sulla scena mondiale, promettendo sconvolgimenti: machine learning ottimizzato, elaborazione del linguaggio naturale e altri progressi dello stesso genere hanno un impatto sia positivo che negativo sulla sicurezza informatica. A fronte di un'evoluzione mondiale delle minacce informatiche molto più rapida di quanto possa essere gestibile dalle persone, le soluzioni di intelligenza artificiale diventano vitali per la difesa informatica delle aziende.

Sicurezza informatica: le sfide per i CISO e la rivoluzione SecOps

Qual è una delle sfide più critiche per professionisti della sicurezza informatica e team SecOps? Assimilare l'intelligence sulle minacce, in modo rapido e su larga scala, e trasmettere immediatamente informazioni fruibili ai team di ricerca delle minacce nonché alle task force all'interno delle aziende.

L'obiettivo di Trellix? Semplificare questo processo.

Come? Fornendo il livello di automazione necessario per ottenere le risposte su cui le aziende devono concentrarsi, utilizzando le nostre funzionalità di intelligence sulle minacce, tracciamento delle minacce e sicurezza avanzata, integrate nei nostri prodotti XDR, protezione di host, sicurezza di rete e dell'email.

Il panorama delle minacce nel primo trimestre 2023 è stato influenzato anche da fattori interni, molti dei quali riflettono i continui venti contrari che i responsabili della sicurezza informatica e i team in prima linea si trovano ad affrontare.

Tecnologie obsolete: molte aziende continuano a fare affidamento su tecnologie obsolete come gli strumenti SOAR e SIEM. Infatti il 96% dei CISO afferma di aver bisogno di soluzioni migliori per proteggere la propria azienda dalle minacce informatiche[3].

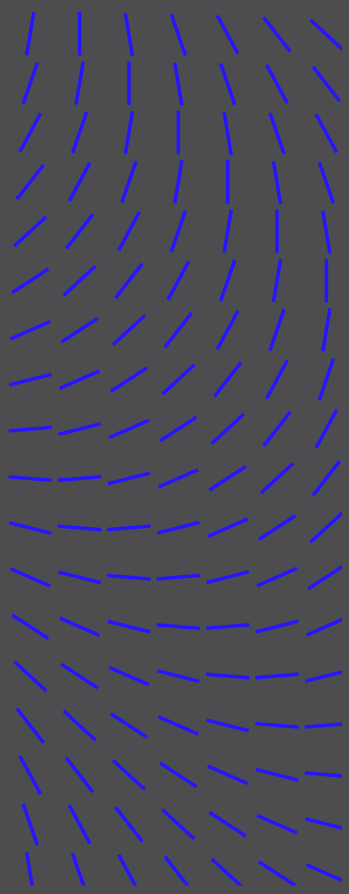
Una moltitudine di strumenti di sicurezza: i team SecOps sono sommersi di avvisi e non riescono a stabilire le priorità necessarie per gestire in modo efficace il loro tempo. In media, le aziende utilizzano non meno di 25 fra soluzioni e strumenti di sicurezza[4].

Desensibilizzazione agli avvisi: inondati di avvisi, i team SecOps sono in difficoltà in termini di priorità, falsi positivi e avvisi mancati. Secondo IDC, il 35% degli analisti ignora gli avvisi, forse in parte perché il 45% di questi sono falsi positivi[5].

Risorse insufficienti: con risorse e competenze limitate, i team SecOps faticano a contrastare efficacemente le minacce. Ad esempio, in media, un analista SOC rimane al suo posto per circa due anni[6].

Metodologia: come raccogliamo e analizziamo i dati

Trellix e gli esperti dell'avanzato 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, vedi in fondo a questo report.



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.

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.

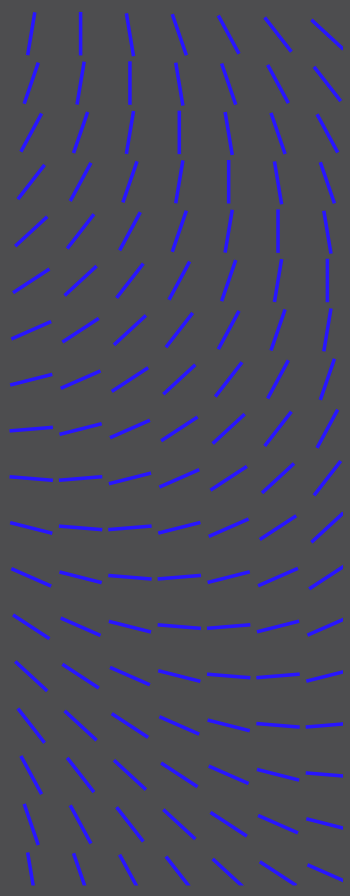
Gli elementi fondamentali di questa etica investigativa sono:

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 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 telecomunicazioni, ad esempio, includono la telemetria dei clienti ISP che operano in molti altri settori.

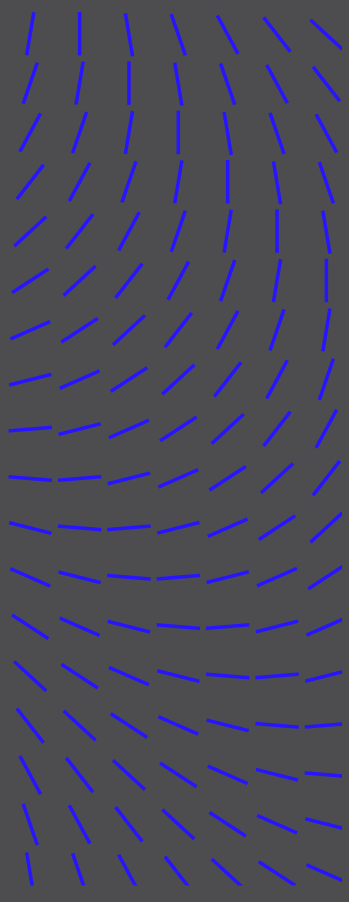


Assegnazione degli attacchi sponsorizzati dagli Stati: analogamente, attribuire la responsabilità di vari attacchi e minacce informatiche a un gruppo sponsorizzato dallo stato può essere molto difficile, data la pratica comune fra questi gruppi di usurpare l'identità di un altro collettivo o di far sembrare le attività dannose come provenienti da una fonte affidabile.

Il futuro che ci attende: consigli e risorse

Cosa significano le informazioni presenti in questo report per gli eroi della sicurezza informatica in prima linea? Le informazioni e i dati sulla sicurezza informatica sono utili solo se vengono trasformati in azioni e permettono di ridurre i rischi, migliorare i processi decisionali o aumentare l'efficacia delle attività SecOps. Per ulteriori informazioni e risorse, visita il sito www.trellix.com.

[3] Trellix, "2023 Report: The Mind of the CISO," 2023
[4] Trellix, "2023 Report: The Mind of the CISO," 2023
[5] IDC, The Voice of the Analysts, 2021
[6] Ponemon Institute, 2020



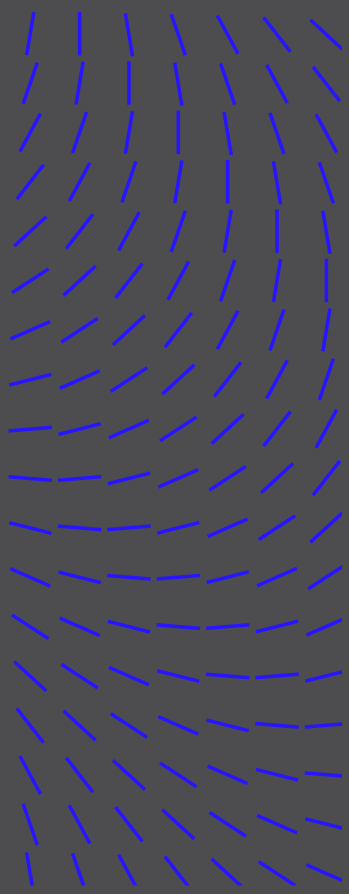
FATTI SALIENTI DELLE MINACCE IN BREVE: 1° TRIMESTRE 2023

Il panorama dei ransomware

- **L'ondata del ransomware:** il ransomware continua a dominare il paesaggio mondiale degli attacchi informatici. Gli schemi di social engineering per ingannare e manipolare le persone e indurle a divulgare informazioni riservate o personali, come il phishing, sono più prevalenti e sofisticati che mai.
- **La predominanza di Cuba e Play:** sebbene all'inizio dell'anno abbiamo osservato un calo dell'attività di criminalità informatica legata ai ransomware, le famiglie di ransomware più diffuse nel primo trimestre sono state Cuba (9%) e Play (7%).
- **La persistenza di LockBit:** nonostante una riduzione dell'attività per due trimestri consecutivi, LockBit continua a essere il ransomware più aggressivo nello spingere le vittime a soddisfare le richieste di riscatto.
- **La potenziale ascesa di Magecart Group:** secondo i report pubblici indicano, l'attività di questo gruppo specializzato nel furto di dati delle carte di credito e nelle truffe di ecommerce è aumentata enormemente nel primo trimestre del 2023. Questa minaccia raramente opera sulla stessa scala di attività delle altre principali APT sponsorizzate dagli Stati, il che indica potenzialmente un riemergere di Magecart Group in tutto il mondo.

L'evoluzione delle tattiche del ransomware

- **Obiettivi economici:** non sorprende che i moventi del ransomware rimangano principalmente economici. I settori delle assicurazioni (20%) e dei servizi finanziari (17%) hanno rilevato il maggior numero di potenziali attacchi.
- **Grande impatto sulle aziende di medie dimensioni:** l'analisi dei dati associati ai siti di divulgazione rivela che le vittime di questi attacchi sono più principalmente le aziende di medie dimensioni con 51 - 200 dipendenti (32%) e da 10 a 50 milioni di dollari di fatturato (38%).
- **Gli Stati Uniti, l'obiettivo principale:** gli Stati Uniti (15%) sono stati il paese più colpito dai gruppi di ransomware. Sono stati anche il paese con la percentuale più alta di vittime aziendali (48%) che hanno deciso di "riacquistare i propri dati" dai ricattatori, una cifra sei volte superiore a quello del secondo paese nell'elenco, il Regno Unito.
- **Cobalt Strike è l'arma preferita:** i dati di telemetria di Trellix identificano questo strumento come di gran lunga il preferito dai gruppi di ransomware (28% degli incidenti). Sembra che tra questi gruppi stia crescendo in popolarità e utilizzo, nonostante i tentativi del fornitore Fortra alla fine del quarto trimestre del 2022 di renderne più difficile l'utilizzo da parte dei criminali informatici.



Attacchi sponsorizzati dagli Stati

- **I protagonisti:** i gruppi APT legati alla Cina, tra cui Mustang Panda e UNC4191, sono stati i più attivi nel prendere di mira gli Stati nel primo trimestre. Gli attori delle minacce affiliati alla Cina hanno dominato la scena globale, generando il 79,3% di tutta l'attività degli Stati, seguiti da quelli legati a Corea del Nord, Russia e Iran.
- **Gruppo APT più attivo:** Mustang Panda è rimasto per il terzo trimestre consecutivo il gruppo APT più attivo al mondo (72%), a indicare i continui e crescenti sforzi da parte della Cina a scopo di spionaggio e di generare disagi.

Vulnerabilità

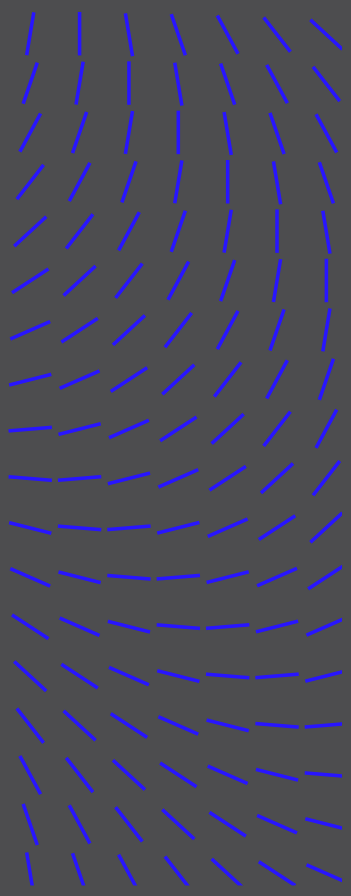
- **Mancata correzione delle vulnerabilità note:** la maggior parte delle vulnerabilità più critiche di questo trimestre è costituita da vulnerabilità note non ancora corrette.
- **Vecchie vulnerabilità:** il bug di una vulnerabilità Apple divulgata nel febbraio di quest'anno risaliva all'exploit FORCEDENTRY, utilizzato da NSO Group come parte del suo spyware Pegasus reso pubblico nel 2021.

Sicurezza dell'email

- **Nuovi vettori d'attacco:** sebbene Microsoft abbia iniziato a bloccare gli allegati macro per la piattaforma Office, i criminali informatici hanno rapidamente adottato altri vettori di infezione per continuare a prendere di mira i dispositivi Windows, come l'avvelenamento SEO, OneNote e gli allegati ZIP.
- **Marchi inaffidabili:** oltre alle email di phishing generiche, i malintenzionati sfruttano sempre di più marchi e servizi legittimi, come quelli di PayPal, Google, DWeb e IPFS, per truffare le vittime e rubare le loro credenziali di identificazione online.

Accesso non autorizzato al cloud

- **Evoluzione delle tattiche:** gli attacchi contro le infrastrutture cloud continuano ad aumentare man mano che sempre più aziende migrano da un'infrastruttura on premise alle opzioni più convenienti e scalabili di Amazon, Microsoft, Google e altri.
- **Account validi:** nonostante la diffusione degli attacchi più sofisticati con autenticazione a più fattori, proxy ed esecuzione di API, la tecnica di attacco dominante restano gli account validi, con una frequenza più che doppia rispetto al secondo vettore di attacco più utilizzato. Ciò sottolinea che il rischio di accesso non autorizzato è reale, poiché i criminali informatici accedono a credenziali di account o siti web legittime per infiltrarsi e lanciare attacchi.



SEGNALAZIONI, DATI E ANALISI

Incidenti di sicurezza

Gli incidenti di sicurezza trattati in questa sezione si basano su segnalazioni pubbliche. Nel primo trimestre del 2023 i file binari di Windows, gli strumenti di terze parti, il malware personalizzato e gli strumenti dei test di penetrazione hanno continuato a influire sulle attività delle aziende poiché i criminali informatici hanno sfruttato i vettori d'attacco più facili. PowerShell e Windows Command Shell continuano a essere sfruttate per generare attività che portano alla persistenza, alla distribuzione e all'estrazione.

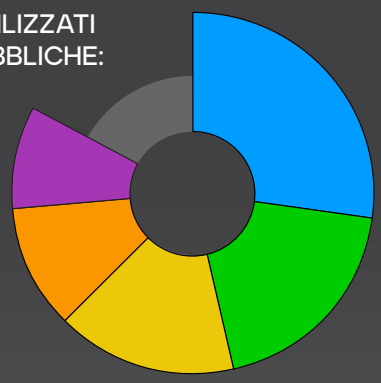
PRINCIPALI FILE BINARI DI WINDOWS UTILIZZATI: 1° TRIMESTRE 2023

1. PowerShell
2. Windows CMD
3. Attività pianificata
4. RunDLL32
5. WMIC

Le attività pianificate, l'inserimento di file DLL dannosi e l'esecuzione di comandi tramite l'infrastruttura di gestione di Windows (WMI) completano la top 5. Sia attraverso l'esecuzione di script o con l'immissione manuale da tastiera, i criminali informatici hanno continuato a utilizzare i file binari non protetti e non monitorati già a loro disposizione.

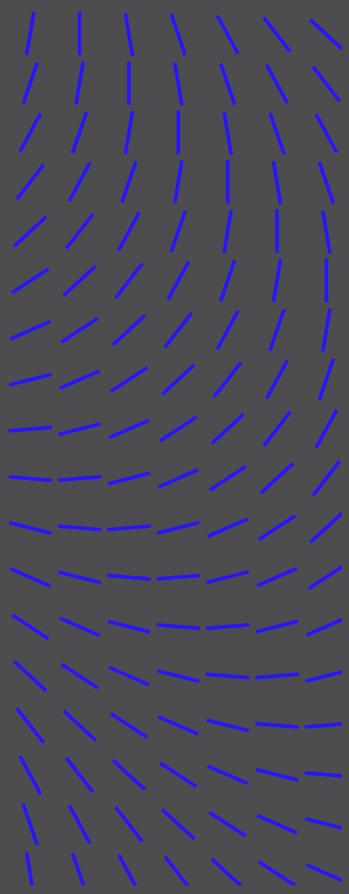
In molti casi gli strumenti di terze parti, il freeware e gli strumenti per i test di penetrazione svolgono un ruolo nel ciclo di vita di un attacco, aiutando i criminali informatici a stabilire la persistenza, eseguire gli script, identificare e raccogliere informazioni mirate e elevare i privilegi per accedere a risorse o dati altrimenti inaccessibili agli account con restrizioni. Inoltre, un criminale informatico può, al fine di elevare i privilegi, eseguire dei processi di installazione con privilegi elevati e accedere ad aree, risorse o dati altrimenti inaccessibili agli account con restrizioni.

PRINCIPALI STRUMENTI TERZI UTILIZZATI SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE 2023



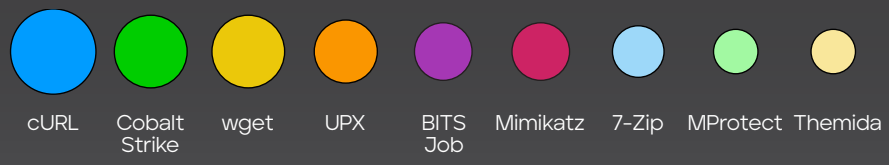
CATEGORIE DEGLI STRUMENTI

- Trasferimento di file
- Programmi di compressione del software
- Strumenti di post-sfruttamento
- Strumenti di accesso remoto
- Utilità di archiviazione



STRUMENTI TERZI UTILIZZATI SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE 2023

STRUMENTI SPECIFICI



Gli strumenti di terze parti più pericolosi come Cobalt Strike, Mimikatz e Sharphound vengono utilizzati sia legittimamente sia dai criminali informatici per raccogliere password, impostare dei beacon o aumentare i privilegi. Una volta che un malintenzionato ha compromesso un ambiente, può utilizzare strumenti di trasferimento dei file come cURL per accedere a payload remoti oppure Rclone per esfiltrare i dati verso un archivio nel cloud.

Nel primo trimestre del 2023 Magecart Group, APT29 e APT41 sono stati i tre collettivi più attivi nel prendere di mira gli utenti di aree geografiche e settori scelti, come metodi per guadagnare denaro, rubare segreti governativi o inibire l'uso delle infrastrutture. Siamo rimasti sorpresi nel constatare che Magecart Group sia in cima alla lista, in quanto raramente opera alla stessa scala degli altri principali gruppi APT affiliati agli Stati. Nei prossimi mesi monitoreremo l'attività del gruppo per valutare se i dati del periodo attuale indicano il suo riemergere sulla scena globale.

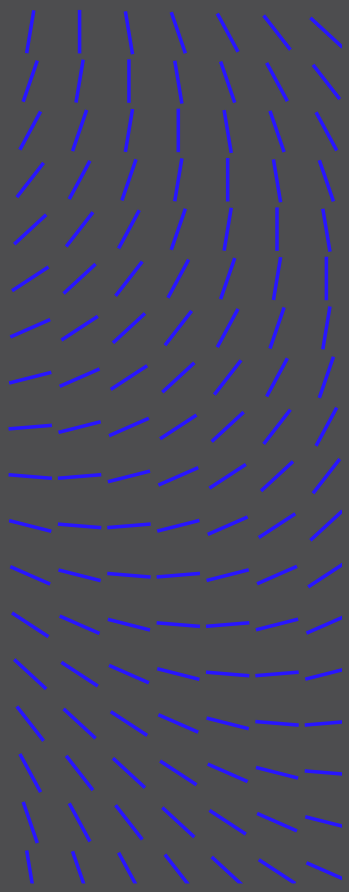
Nelle passate campagne globali, le meno sofisticate tecniche "spray-and-pray", concepite per invogliare gli utenti suscettibili a fare clic su un link dannoso o scaricare un file pericoloso hanno seminato caos in diversi settori. Gli attacchi mirati sono diventati più sofisticati, aumentando la propria persistenza nei settori manifatturiero, finanziario e sanitario. Sebbene gli altri due settori, telecomunicazioni ed energia, sembrino essere stati colpiti meno frequentemente negli eventi globali, sono ugualmente importanti e le aziende associate potrebbero non aver segnalato le violazioni o rilevato incidenti contro di loro.

PRINCIPALI GRUPPI DI CRIMINALI INFORMATICI SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE 2023

1.	Magecart Group	5%
2.	APT29	4%
3.	APT41	4%
4.	Blind Eagle	4%
5.	Gamaredon Group	4%
6.	Lazarus	4%
7.	Mustang Panda	4%
8.	Sandworm Team	4%

PRINCIPALI SETTORI COLPITI SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE

1.	Industria manifatturiera	8%
2.	Finanza	7%
3.	Sanità	6%
4.	Telecomunicazioni	5%
5.	Energia	5%



Gli eventi segnalati che sono stati analizzati e controllati dai nostri ricercatori, contengono una grande quantità di informazioni, correlazioni o attribuzioni a un singolo criminale informatico, un gruppo o collettivi APT più sofisticati. Gli strumenti, le tecniche e le procedure, oltre alle famiglie di malware, includono i malware di caricamento e downloader, gli strumenti di amministrazione a distanza (RAT), i ladri di informazioni e il ransomware. Sulla base degli eventi del primo trimestre 2023, analizzati e disponibili tramite Insights, l'Ucraina è risultata il Paese colpito più di frequente, seguita da vicino dagli Stati Uniti.

Nello stesso periodo le famiglie di ransomware più attive sono state Royal Ransom, Trigona e Maui. Trellix ha di recente pubblicato un'analisi dettagliata di Royal Ransom e del suo modus operandi con file eseguibili Windows e Linux. Sebbene le statistiche rappresentate siano emerse specificamente dalla nostra piattaforma Insights, molti altri eventi si sono verificati nell'infrastruttura connessa a livello globale, inclusi noti eventi segnalati o mantenuti riservati e gli eventi che devono ancora essere identificati e risolti.

PRINCIPALI PAESI COLPITI SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE

7% 

Sulla base degli eventi pubblici disponibili per l'analisi, abbiamo stabilito che l'Ucraina è il Paese più colpito dai criminali informatici, seguito a ruota dagli Stati Uniti.

1.	Ucraina	7%
2.	Stati Uniti	7%
3.	Germania	4%
4.	Corea del Sud	3%
5.	India	3%

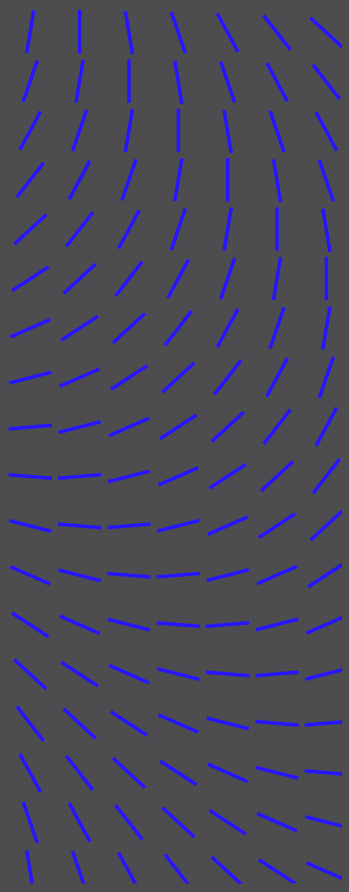
PRINCIPALI RANSOMWARE SECONDO LE SEGNALAZIONI PUBBLICHE: 1° TRIMESTRE

1.	Royal Ransom	7%
2.	Trigona	4%
3.	Maui	4%
4.	Magniber	3%
5.	LockBit	3%

Ransomware

Le statistiche visualizzate qui di seguito sono quelle delle campagne, non dei rilevamenti stessi. I nostri dati di telemetria globali mostrano indicatori di compromissione (IOC) che appartengono a diverse campagne lanciate da vari gruppi di criminali informatici.

All'inizio dell'anno, soprattutto a gennaio, è abbastanza comune assistere a un calo dell'attività dei criminali informatici. Questa tendenza potrebbe spiegare la notevole diminuzione delle attività associate ai ransomware Hive e Cuba. Anche l'interruzione delle attività di Hive da parte dell'FBI e dell'Europol alla fine di gennaio potrebbe aver interferito in modo significativo con le sue operazioni. LockBit continua a essere una famiglia di ransomware diffusa. Particolarmente aggressivo, ha apparentemente successo nello spingere le vittime a pagare i riscatti.



PRINCIPALI RANSOMWARE UTILIZZATI: 1° TRIMESTRE 2023

8%

Cuba è stato il gruppo di ransomware più attivo, seguito da Play e LockBit.

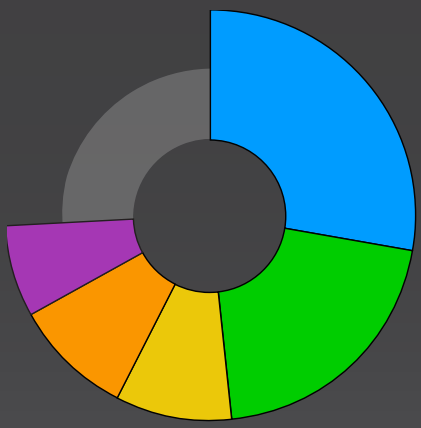
- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

STRUMENTI DI RANSOMWARE UTILIZZATI: 1° TRIMESTRE 2023

28%

CobaltStrike è stato usato in quasi un terzo degli attacchi di ransomware del trimestre. Il suo utilizzo è cresciuto nonostante i recenti aggiornamenti per renderne più difficile l'abuso da parte dei criminali informatici.

- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC

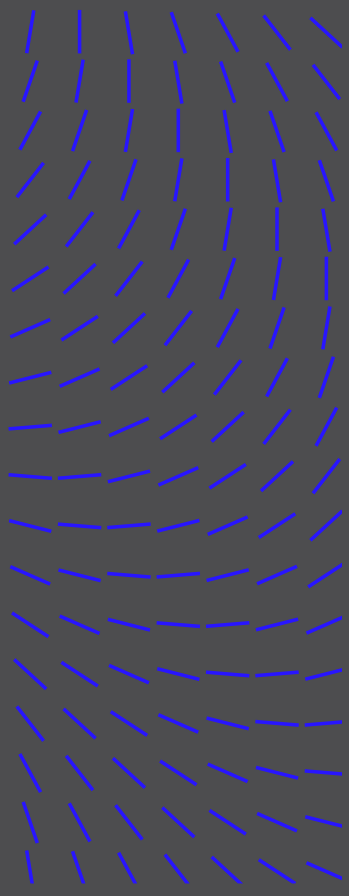


PAESI PIÙ COLPITI DAI GRUPPI DI RANSOMWARE: 1° TRIMESTRE 2023

15%

Questo trimestre, gli Stati Uniti restano il Paese più colpito dall'attività del ransomware, seguito a ruota dalla Turchia.

1.	Stati Uniti	15%
2.	Turchia	14%
3.	Portogallo	10%
4.	India	9%
5.	Canada	9%



SETTORI PIÙ COLPITI DAI GRUPPI RANSOMWARE: 1° TRIMESTRE 2023

1.	Assicurazioni	20%
2.	Servizi finanziari	17%
3.	Settore farmaceutico	7%
4.	Telecomunicazioni	4%
5.	Esternalizzazione e hosting	4%

I gruppi di ransomware estorcono soldi alle vittime pubblicandone le informazioni nei cosiddetti "siti di divulgazione" (leak site) per forzare le trattative oppure quando il pagamento del riscatto viene rifiutato. Gli esperti di Trellix utilizzano RansomLook, uno strumento open source, per raccogliere dati dai post e poi normalizzare e arricchire i risultati per fornire un'analisi anonima delle vittime.

È importante sottolineare che non tutte le vittime vengono segnalate sui rispettivi siti di divulgazione. Molte vittime pagano il riscatto e non vengono conteggiate. Queste metriche sono un indicatore delle vittime prese di mira dai gruppi ransomware a fini di estorsione o rappresaglia e non devono essere confuse con il numero totale delle vittime.

GRUPPI DI RANSOMWARE CON IL MAGGIOR NUMERO DI VITTIME IN BASE AI LORO SITI DI DIVULGAZIONE: 1° TRIMESTRE 2023

1.	LockBit	30%
2.	Hive	22%
3.	Clop	12%
4.	Royal Ransom	7%
5.	ALPHV	5%

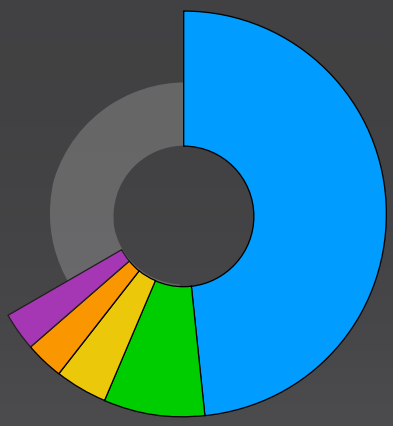
SETTORI PIÙ COLPITI DAI GRUPPI DI RANSOMWARE IN BASE AI LORO SITI DI DIVULGAZIONE: 1° TRIMESTRE 2023

1.	Beni e servizi industriali	25%
2.	Vendita al dettaglio	14%
3.	Tecnologia	11%
4.	Sanità	8%
5.	Servizi finanziari	6%

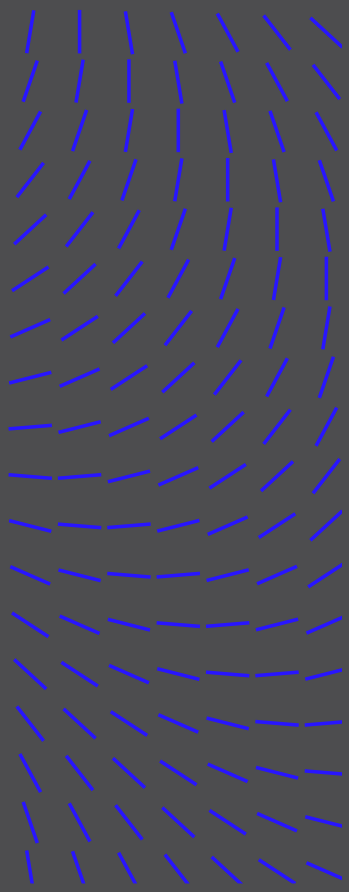
PRINCIPALI PAESI DELLE AZIENDE ELENCATE SUI SITI DI DIVULGAZIONE: 1° TRIMESTRE 2023

48%

delle aziende vittime elencate nei siti di divulgazione dei gruppi di ransomware erano basate negli Stati Uniti.



- Stati Uniti
- Regno Unito
- Germania
- Canada
- India



DIMENSIONI DELLE AZIENDE ELENCATE NEI SITI DI DIVULGAZIONE: 1° TRIMESTRE 2023

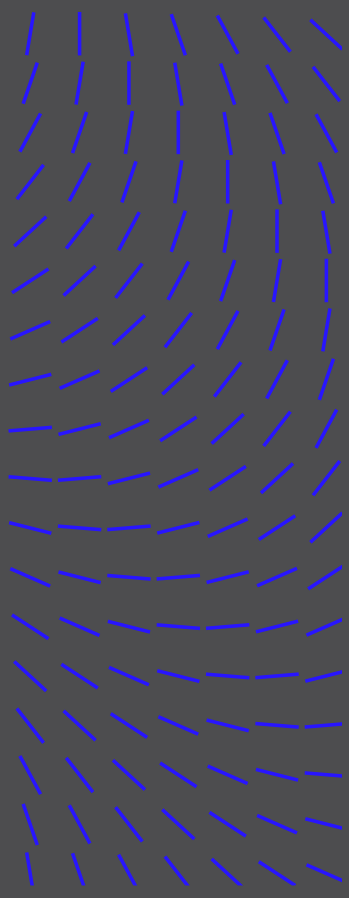
NUMERO DI COLLABORATORI		FATTURATO ANNUO	
1.	51-200 32%	1.	10-50mln $ 38%
2.	1.001-5.000 22%	2.	1-10mld $ 23%
3.	11-50 15%	3.	1-10mln $ 21%
4.	201-500 15%	4.	100-250mln $ 11%
5.	501-1.000 15%	5.	500-1mld $ 7%

Attività degli Stati-Nazione

Le informazioni sugli attacchi sponsorizzati dagli Stati provengono da più fonti il che ci permette di delineare un quadro più completo del panorama delle minacce e ridurre gli errori di osservazione. In primo luogo, utilizziamo le statistiche estratte dalla correlazione tra i gruppi sponsorizzati dagli Stati, gli indicatori di compromissione (IOC) e i dati di telemetria dei clienti di Trellix. In secondo luogo, forniamo informazioni tratte da vari rapporti pubblicati dal settore della sicurezza, vagliati e convalidati dal gruppo di Intelligence sulle minacce.

Come sopra detto, queste statistiche sono quelle delle campagne, non dei rilevamenti stessi. A causa dell'aggregazione di vari registri, dell'uso da parte dei nostri clienti di framework di simulazione delle minacce e di correlazioni di alto livello con la base di conoscenza di intelligence sulle minacce, i dati vengono filtrati manualmente per soddisfare i nostri obiettivi d'analisi.

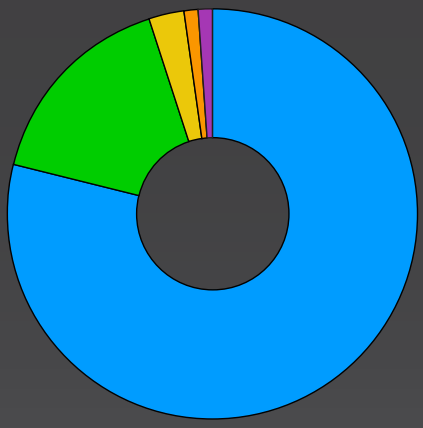
Il panorama globale continua a essere dominato dai collettivi affiliati alla Cina. Mustang Panda è stato all'origine di una significativa maggioranza di rilevamenti nel primo trimestre del 2023. Dato l'uso massiccio del trasferimento locale diretto (sideloading) e di altre tecniche furtive, è possibile che i gruppi APT affiliati alla Cina cambino gli strumenti malware con minore frequenza rispetto ad altri criminali informatici. In questo caso, questa pratica potrebbe portare a "distorsioni delle proiezioni" o a una stima gonfiata dei rilevamenti degli hash affiliati alla Cina.



PAESI D'ORIGINE PIÙ PREVALENTI DEI CRIMINALI INFORMATICI COINVOLTI IN ATTACCHI SPONSORIZZATI DAGLI STATI: 1° TRIMESTRE 2023

79%

La Cina è all'origine di una gran maggioranza di attacchi sponsorizzati dagli Stati nel 1° trimestre 2023.



- Cina
- Corea del Nord
- Russia
- Iran
- Pakistan

GRUPPI DI CRIMINALI INFORMATICI PIÙ DIFFUSI: 1° TRIMESTRE 2023

1.	Mustang Panda	72%
2.	Lazarus	17%
3.	UNC4191	1%
4.	Common Raven	1%
5.	APT34	1%

TECNICHE MITRE ATT&CK PIÙ DIFFUSE UTILIZZATE NEGLI ATTACCHI SPONSORIZZATI DAGLI STATI: 1° TRIMESTRE 2023

1.	Sideloading LDLL	14%
2.	Deoffuscamento/Decodifica di file o informazioni	11%
3.	Trasferimento di strumenti all'ingresso	10%
4.	Dati estratti dal sistema locale	10%
5.	Rilevamento di file e directory	10%

STRUMENTI DANNOSI PIÙ DIFFUSI UTILIZZATI NEGLI ATTACCHI SPONSORIZZATI DAGLI STATI: 1° TRIMESTRE 2023

38%

PlugX rappresenta il 38% degli attacchi sponsorizzati dagli Stati nel 1° trimestre 2023.

1.	PlugX	38%
2.	Cobalt Strike	35%
3.	Raspberry Robin	14%
4.	BLUEHAZE/DARKDEW MISTCLOAK	3%
5.	Mimikatz	3%

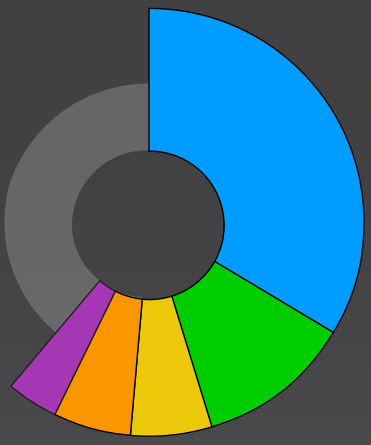
L'India è uno dei paesi leader in Asia e regioni limitrofe con programmi di sicurezza informatica efficaci. Alcuni gruppi, prevalentemente legati alla Cina, hanno dimostrato grande interesse per gli sviluppi tecnologici, militari e politici dell'India. Un numero considerevoli di rilevamenti in India può essere infatti attribuito a Mustang Panda.

PAESI CON PIÙ RILEVAMENTI DI ATTIVITÀ SPONSORIZZATE DAGLI STATI: 1° TRIMESTRE 2023

34%

Le Filippine guidano la classifica dei paesi con il maggior numero di rilevamenti di attività sponsorizzati dagli Stati: 1° trimestre 2023.

- Filippine
- India
- Myanmar
- Camerun
- Stati Uniti



PAESI CON PIÙ RILEVAMENTI DI ATTIVITÀ SPONSORIZZATE DAGLI STATI: 1° TRIMESTRE 2023

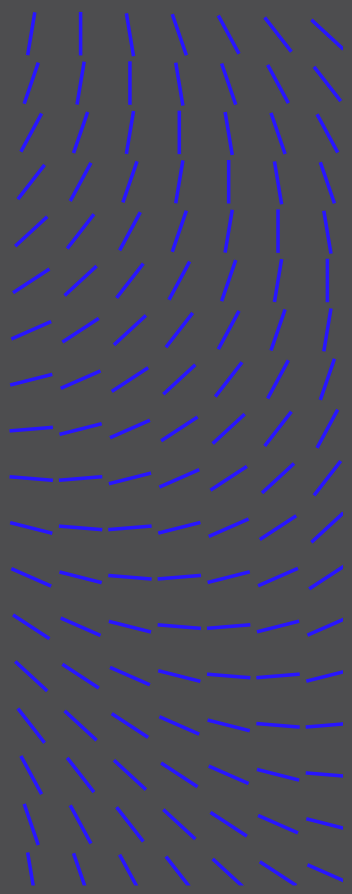
Energia/ Petrolio e gas | Esternalizzazione e hosting | Vendita all'ingrosso | Finanza | Istruzione

Vulnerabilità

Gli esperti di reverse engineering e in analisi delle vulnerabilità del Trellix Advanced Research Center monitorano continuamente le ultime vulnerabilità al fine di fornire indicazioni ai clienti su come i criminali informatici le sfruttano e su come ridurre la probabilità e l'impatto di questi attacchi.

Uno dei nostri risultati più importanti, ma non sorprendenti, del primo trimestre 2023 è che molte delle vulnerabilità più critiche di questo periodo corrispondono all'elusione di patch per CVE precedenti, bug della supply chain derivanti dall'utilizzo di librerie obsolete o vulnerabilità da tempo corrette che sono sopravvissute al loro momento di gloria.

Consideriamo per esempio CVE-2022-47966, una vulnerabilità critica (9,8) identificata nei prodotti ManageEngine di Zoho che è circolata a gennaio. ManageEngine è utilizzato da migliaia di aziende nel mondo, perciò non siamo rimasti sorpresi che lo sfruttamento di tale vulnerabilità sia stato rilevato nell'ambiente reale. Quello che ci ha stupito è stata la causa alla radice: l'utilizzo di Apache Santuario 1.4.1, una versione molto vecchia che conteneva un problema noto che consente l'iniezione XML. Zoho ha corretto questa vulnerabilità nella propria suite di prodotti a ottobre. Poco meno di tre mesi dopo la CISA ha segnalato un avviso di sicurezza dello sfruttamento nell'ambiente reale, chiedendo ai produttori di applicare una patch.



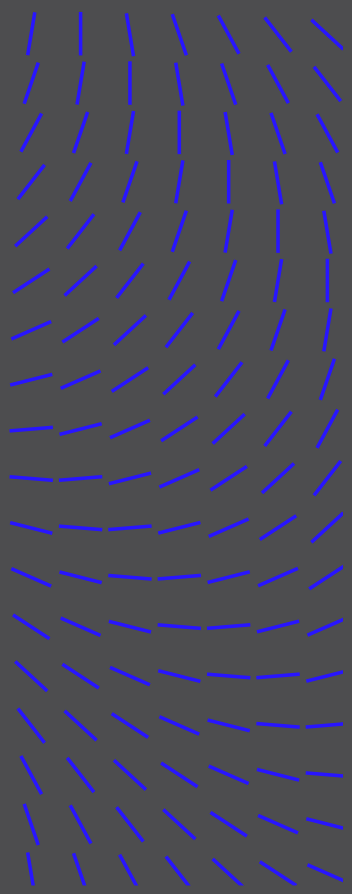
Un altro esempio è CVE-2022-44877, una vulnerabilità critica in Control Web Panel (CWP). Benché non direttamente correlata, questa vulnerabilità presenta molte caratteristiche in comune con l'esempio precedente: si tratta di una RCE 9.8 oggetto di un ampio e attivo sfruttamento a gennaio, nonostante la patch fosse stata applicata a ottobre. La causa alla radice non era degna di una conferenza Black Hat, in quanto si trattava di un'immissione di comandi che utilizzava l'espansione di una variabile shell standard in un parametro URL.

Un terzo esempio è CVE-2021-21974, vulnerabilità identificata nel servizio OpenSLP di VMware ESXi, corretta nel febbraio 2021, quasi due anni prima del suo improvviso riemergere con uno sfruttamento nell'ambiente reale. Quando segnalammo tale vulnerabilità nel Report dei bug di febbraio, evidenziammo che, secondo Shodan, circa 48.000 server accessibili da Internet stavano ancora eseguendo versioni vulnerabili di ESXi. Oggi tale numero è ancora superiore a 38.000, un calo inferiore al 22%.

Data	Numero di server ESXi vulnerabili secondo Shodan
Fine febbraio 2023	48.471
Fine aprile 2023	38.047

Studiando i dispositivi Apple all'inizio di quest'anno abbiamo trovato altri esempi: CVE-2023-23530 e CVE-2023-23531. Queste due vulnerabilità differiscono dalle precedenti nel senso che il loro impatto è limitato all'elevazione locale dei privilegi, non all'esecuzione di codice remoto. Non è tuttavia un buon motivo per trascurarne l'importanza, poiché una vulnerabilità molto simile è stata sfruttata da FORCEDENTRY, utilizzato da NSO Group per distribuire il suo spyware Pegasus nel 2021. In effetti, le due vulnerabilità da noi scoperte utilizzano la stessa tecnica primitiva alla base dell'exploit FORCEDENTRY: un'innocua classe detta NSPredicate. Purtroppo l'approccio di Apple alla prevenzione di FORCEDENTRY ha implicato l'utilizzo di una lunga lista di blocco per neutralizzare lo sfruttamento di NSPredicate: una mitigazione che non è riuscita a risolvere il problema alla radice e che ci ha permesso di eluderla.

È forte la tentazione di puntare il dito a tendenze come queste per concludere che i produttori non prendono sul serio la sicurezza oppure biasimare criminali informatici e ricercatori per i rigurgiti di vecchi exploit, ma non è questo il comportamento corretto. I ricercatori delle vulnerabilità più efficienti analizzano le varianti, perché un bravo ricercatore che emula le priorità dei veri criminali informatici e la scoperta di un meccanismo di elusione della prevenzione o di un vecchio CVE in un prodotto raramente sottoposto a patch produce un maggiore ritorno che il ripartire da zero. Le aziende che sono consapevoli di tale tendenza dovrebbero trarre la seguente conclusione: benché le tecnologie di rilevamento delle minacce siano insostituibili nel moderno panorama delle minacce, si possono ottenere molti risultati nei fondamentali, come i processi di applicazione delle patch e le verifiche della supply chain.



Sicurezza dell'email

Queste statistiche si basano sui dati di telemetria generati dalle diverse appliance di sicurezza dell'email implementate nelle reti dei nostri clienti in tutto il mondo.

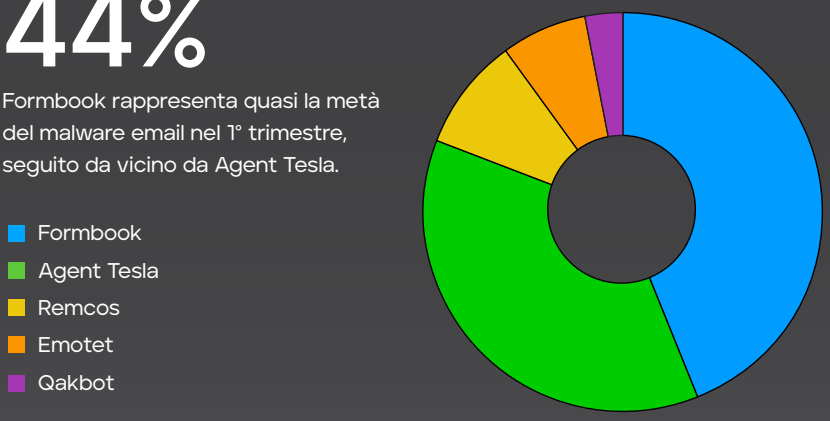
Gli attacchi di phishing che sfruttano i marchi legittimi per frodare gli utenti e rubarne le credenziali sono in aumento. DWeb, IPFS e Google Translate sono ampiamente utilizzati negli attacchi via email. I criminali informatici hanno anche abusato dell'email gratuita e di altri servizi simili, come le applicazioni PayPal Invoicing e Google Forms, per sferrare attacchi di vishing ed evitare il rilevamento. Analogamente sono stati presi di mira in questo periodo nuovi marchi come Scribd, LesMills e i buoni regalo di Google Play.

Inoltre, per quanto riguarda il malware specifico usato per questi attacchi, Formbook e Agent Tesla hanno entrambi registrato un notevole aumento nel primo trimestre 2023, rispetto alla fine dell'anno scorso. Ciò può essere dovuto al fatto che entrambi i malware sono più facili da acquisire e distribuire rispetto a Remcos, Emotet e Qakbot.

MALWARE EMAIL PIÙ DIFFUSI: 1° TRIMESTRE 2023

44%

Formbook rappresenta quasi la metà del malware email nel 1° trimestre, seguito da vicino da Agent Tesla.



PAESI PIÙ COLPITI DALLE EMAIL DI PHISHING: 1° TRIMESTRE 2023

30%

Stati Uniti e Corea sono stati i paesi più colpiti dai tentativi di phishing tramite email del 1° trimestre. Hanno infatti ricevuto quasi due terzi dei tentativi di phishing a livello globale.

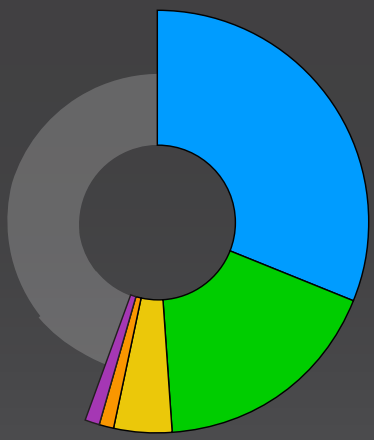
1.	Stati Uniti	30%
2.	Corea del Sud	29%
3.	Taiwan	10%
4.	Brasile	8%
5.	Giappone	7%

PRODOTTI E MARCHI PIÙ COLPITI DALLE EMAIL DI PHISHING: 1° TRIMESTRE 2023

38%

Benché siano stati colpiti centinaia di marchi, nel 1° trimestre 2023 i prodotti Microsoft sono stati di gran lunga i più sfruttati.

- Microsoft
- Google Captcha
- Outlook
- GCash
- USPS



SETTORI PIÙ COLPITI DA EMAIL DANNOSE: 1° TRIMESTRE 2023

1.	Enti pubblici	11%
2.	Servizi finanziari	8%
3.	Industria manifatturiera	6%
4.	Tecnologia	6%
5.	Intrattenimento	5%

FORNITORI DI SERVIZI WEB IN HOSTING ALTAMENTE ABUSATI: 1° TRIMESTRE 2023

1.	IPFS	41%
2.	Google Translate	33%
3.	Dweb	16%
4.	AmazonAWS Appforest	3%
5.	Firebase OWA	3%

TECNICHE DI ELUSIONE PIÙ UTILIZZATE NEGLI ATTACCHI DI PHISHING - 1° TRIMESTRE 2023

79% Gli attacchi di elusione basati su un reindirizzamento 302 sono stati la tecnica di elusione più diffusa usata negli attacchi di phishing nel 1° trimestre 2023.

46% Gli attacchi basati sui CAPTCHA sono aumentati notevolmente nel 1° trimestre 2023 rispetto al 4° trimestre del 2022.

Sicurezza della rete

Oltre a rilevare e bloccare gli attacchi basati sulla rete che minacciano i nostri clienti, i ricercatori del Trellix Advanced Research Center ispezionano diverse aree della catena di attacco (ricognizione, violazione iniziale, comunicazioni con il server C&C e tecniche, tattiche e procedure di spostamento laterale).

PRINCIPALI TENDENZE DEL MALWARE: 1° TRIMESTRE 2023

L'attività del ransomware STOP è diminuita del **94%**

La distribuzione del ransomware LockBit da parte di Amadey è aumentata del **25%**

L'attività del malware Android è aumentata del **12,5%**

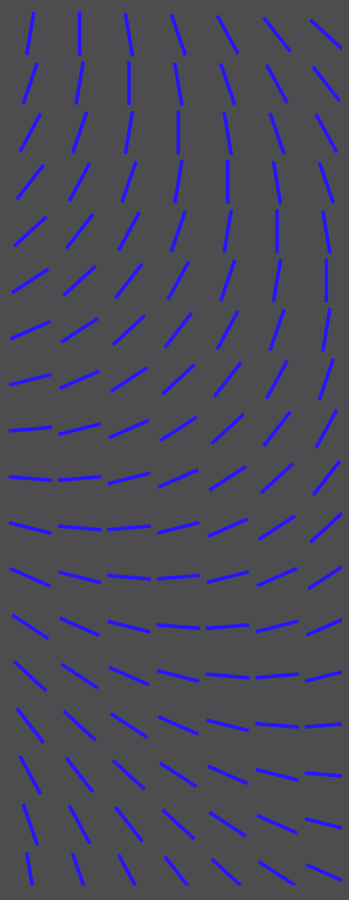
L'attività di Ursnif è aumentata del **10%**

L'attività di Smoke Loader è aumentata di **7 VOLTE**

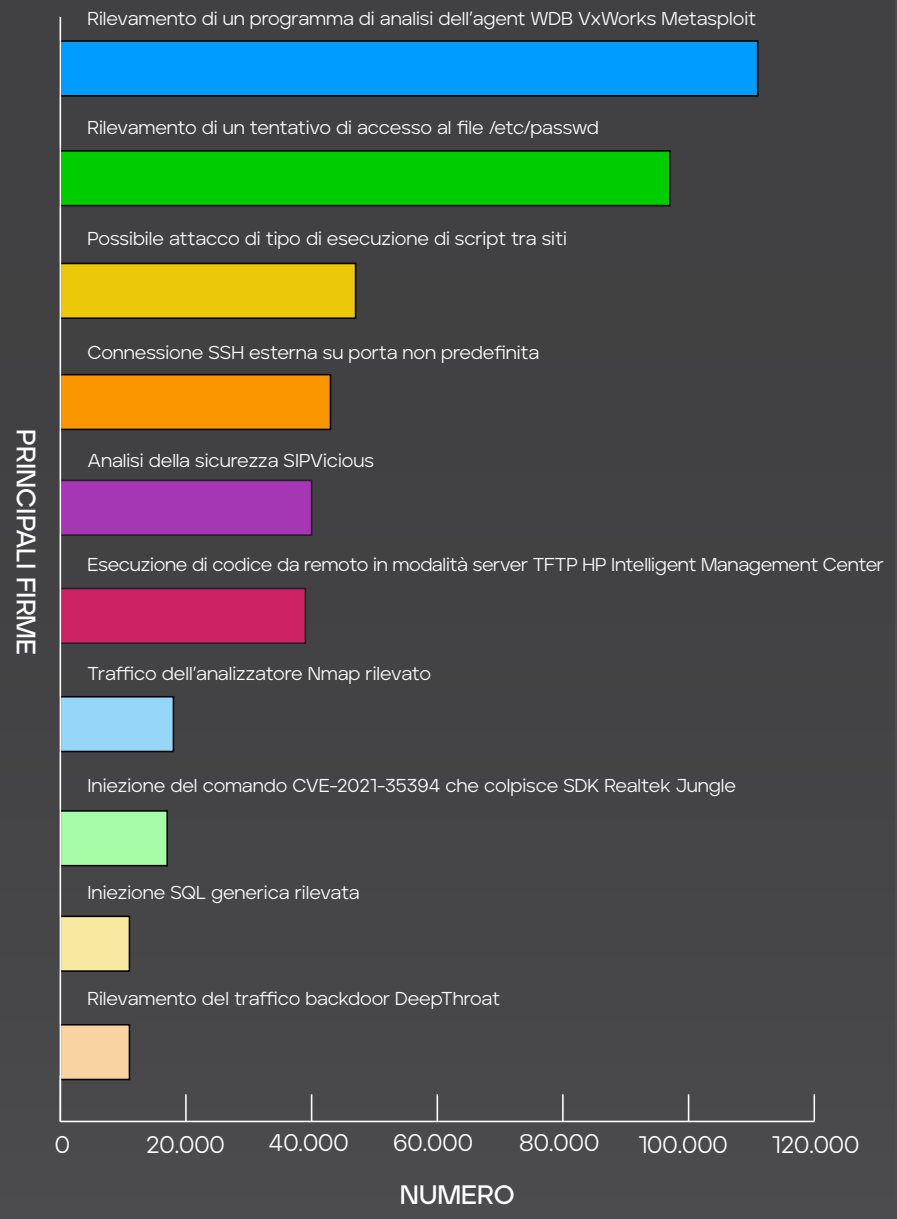
L'attività di Amadey è aumentata di **4 VOLTE**

L'attività di Cobalt Strike è aumentata di **3 VOLTE**

L'attività di Emotet è aumentata di **2 VOLTE**



ATTACCHI CON IL MAGGIOR IMPATTO SUI SERVIZI ACCESSIBILI DALL'ESTERNO: 1° TRIMESTRE 2023



Incidenti cloud

Gli attacchi contro l'infrastruttura cloud, i servizi sviluppati ed erogati da Amazon, Microsoft, Google e altri, continuano ad aumentare. La tabella seguente mostra i dati di telemetria degli attacchi cloud, ripartiti per cliente e per fornitore di servizi cloud.

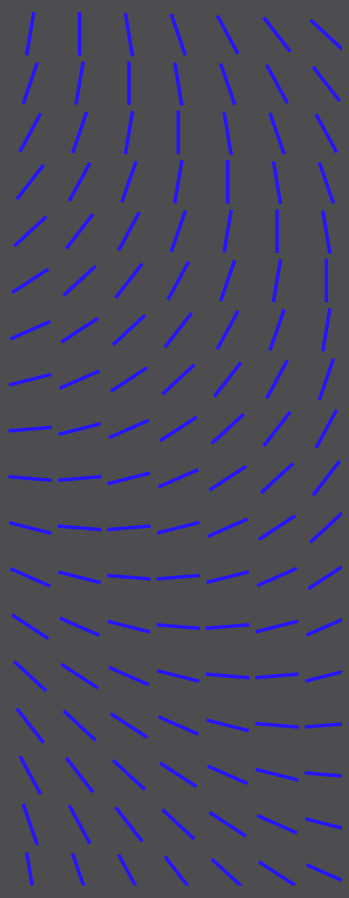
RILEVAMENTI DA PARTE DELLE TECNICHE MITRE ATT&CK: 1° TRIMESTRE 2023

	AWS	Microsoft Azure	GCP
Account validi	3437	4312	997
Modifica dell'infrastruttura di servizio di elaborazione dell'account cloud	4268	0	17
Porta non standard	115	0	17
Autenticazione a più fattori	190	1534	22
Rilevamento dei servizi di rete	141	93	0
Attacco di forza bruta	25	1869	22
Proxy	299	2744	135
Rilevamento degli account	264	68	787
Regola di inoltro dell'email	25	0	22
Esecuzione tramite API	1143	0	252

METODOLOGIA

Acquisizione: Trellix e gli esperti dell'avanzato 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 intelligence sulle minacce, (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 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.

RISORSE

Archivi dei report sulle minacce

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

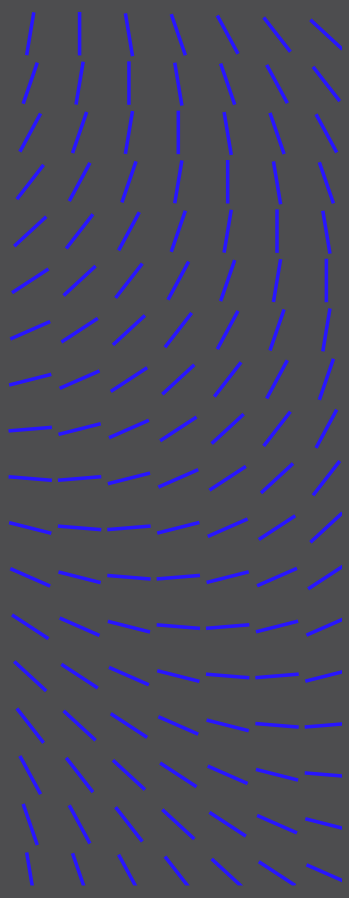
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

Consulta l'archivio dei report sulle minacce informatiche

Trellix Advanced Research Center

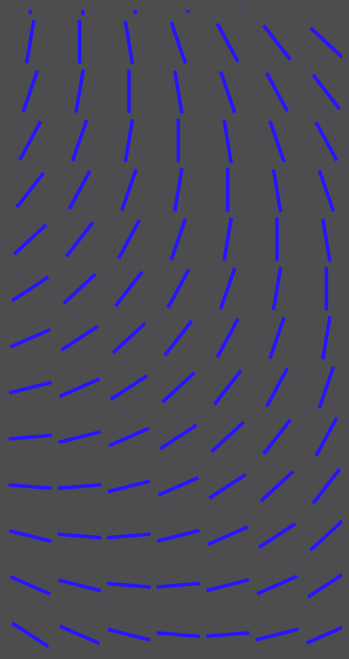


INFORMAZIONI SU TRELLIX ADVANCED RESEARCH CENTER

Trellix Advanced Research Center dispone dello statuto più esaustivo nel settore della sicurezza informatica ed è all'avanguardia nello studio di metodi, tendenze e gruppi di criminali informatici emergenti nel panorama delle minacce. Partner fondamentale dei team responsabili delle operazioni di sicurezza in tutto il mondo, il Trellix Advanced Research Center fornisce intelligence sulle minacce agli analisti di sicurezza e contenuti di prim'ordine, alimentando al contempo vita la nostra avanzata piattaforma XDR. Inoltre, il GruppoThreat Intelligence di Trellix Advanced Research Center offre prodotti e servizi di Threat Intelligence ai clienti di tutto il mondo.

INFORMAZIONI SU 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, hanno accelerato l'innovazione tecnologica attraverso la data science e l'automazione per supportare oltre 40.000 clienti in ambito privato e pubblico.



Per saperne di più, visita il sito Trellix.com.

Trellix

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 la data science e l'automazione per supportare oltre 40.000 clienti in ambito privato e pubblico.

072022-05