DER CYBERTHREATS-REPORT

Juni 2024

Einblicke aus einem weltweiten Netzwerk von Experten, Sensoren, Telemetrie und Bedrohungsdaten

THEMEN:

Schnelle und tiefgreifende Veränderungen bei APT-Bedrohungen

LockBit mischt das Ransomware-Ökosystem auf

Wachsender Tool-Bestand der Angreifer

Präsentiert von

Trellix ADVANCED RESEARCH CENTER

Mithilfe eines Tools zur EDR-Umgehung gelang es Bedrohungsakteuren gerade erfolgreich, bei einem Unternehmen in unserer Branche die Endpoint Detection and Response-Funktionen auszuhebeln.

Es wird immer schwerer, den Missbrauch legitimer Sicherheits-Tools zu verhindern, um den Wettlauf mit den Angreifern zu gewinnen.

Als CISO müssen Sie flexibel, schnell, souverän und kontrolliert vorgehen. Ihr CEO und der Vorstand möchten mehr über Ihre Protokollierungs- und Warnungs-Tools wissen. Gleichzeitig muss Ihr Team Lücken identifizieren und einen Plan haben, um sie zu schließen.

Der Cyber-Sicherheitswettlauf ist ein Triathlon, bei dem Sie in den Disziplinen SecOps, Technologie und Analysedaten antreten. Der Wettlauf ist bereits im Gange, und Sie brauchen einen langen Atem.

> Nicht nur Schutzmechanismen werden immer raffinierter, sondern auch die Tools und Taktiken der staatlich unterstützten Angreifer und kriminellen Akteure.

DER CYBERTHREATS-REPORT

Dieser vom Trellix Advanced Research Center verfasste Bericht stellt Einblicke, Bedrohungsdaten und Empfehlungen vor, die aus verschiedenen Datenquellen für Cyber-Sicherheitsbedrohungen gewonnen wurden, und entwickelt daraus nützliche Experten-Interpretationen sowie empfohlene Vorgehensweisen für die Cyber-Abwehr. Diese Ausgabe konzentriert sich auf Daten und Erkenntnisse, die wir zwischen dem 1. Oktober 2023 und dem 31. März 2024 erfasst haben.

1. Schnelle und tiefgreifende Veränderungen bei APT-Bedrohungen
2. LockBit mischt das Ransomware-Ökosystem auf
3. EDR-Killer-Tools betreten die Bühne
4. Betrugsmaschen zur US-Präsidentschaftswahl
5. GenAI und der Cybercrime-Untergrund

VORWORT

Für CISOs waren operative Bedrohungsdaten und die Kontextualisierung von globalen Bedrohungen für Ihre Umgebung noch nie so wichtig.

Da wir mit weniger Mitteln mehr erreichen sollen, benötigen CISOs und ihre SecOps-Teams Bedrohungsdaten, mit denen sie Bedrohungen vorhersagen, die relevantesten Bedrohungen für Ihr Unternehmen identifizieren, Programme und Budgets an die wahrscheinlichsten Bedrohungen und Akteure anpassen sowie einen proaktiven statt reaktiven Ansatz wählen können.

Als „Kunde Null" für Trellix habe ich noch nie so viel Potenzial gesehen, dass Bedrohungsanalysen den Spielraum für Aktivitäten und Strategien von Sicherheitsverantwortlichen vergrößern.

Nutzen Sie die Inhalte dieses Berichts für Ihre strategische Planung, Budget-Begründung, zum Informieren des Vorstands sowie für operative Unterstützung. Ich hoffe, Sie finden diesen Bericht nützlich und informativ. Er soll als Ausgangspunkt dienen und Sie dabei unterstützen, Maßnahmen gegen APTs zu planen, sich auf APTs vorzubereiten und diese Bedrohungen abzuwehren.



Harold Rivas
CISO, TRELLIX

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

EINLEITUNG

Ebenso wie bei all unseren Berichten möchten wir mit diesem Bericht die Diskussion um Bedrohungsdaten unterstützen und unsere Beobachtungen in einen Kontext setzen.

Die Situation

Die letzten sechs Monate waren bisher einmalig – eine konstante Multi-Krise, die Aktivitäten von Cyber-Kriminellen und Bedrohungsakteuren weltweit befeuert hat. Wir erleben radikale Verhaltensänderungen, zum Beispiel:

- Bei Aktionen von Strafverfolgungsbehörden verhält sich das Ransomware-Ökosystem untypisch
- Autonome Gruppen verkaufen ihre Beute aus Penetrationstests und alternativen Angriffsmethoden an Ransomware-Gruppen
- Die Kriegshandlungen in Israel haben staatlich unterstützte Angriffe und Hacktivismus ausgelöst
- Bedrohungsakteure suchen nach immer neuen Methoden und profitieren von billigen und teils kostenlosen Tools für generative KI (GenAI), mit denen sie über Nacht zu Experten werden
- Tools zur EDR-Umgehung und Abschaltung werden für Bedrohungsakteure immer wichtiger

Katz-und-Maus-Spiel

Bei größeren Implementierungen von EDR-Lösungen (Endpoint Detection and Response) erleben wir ein Katz-und-Maus-Spiel, weil die Cyber-Sicherheit immer komplexer wird. Die Zunahme von Bedrohungsakteuren, die kriminelle Tools zum Unterlaufen von EDR nutzen, hat unser Interesse geweckt und ist ein scharfer Kurswechsel von der Nutzung klassischer Malware-Tools.

Das zwingt uns als Sicherheitsverantwortliche ebenfalls zu einem neuen Ansatz. EDR hat sich bei der Erkennung von Malware, Ransomware und APT-Aktivitäten als effektiv erwiesen, doch wenn die Lösung deaktiviert wird, beschneidet das die Möglichkeiten eines Unternehmens und seines CISOs erheblich. Sie benötigen Protokollierung, Warnmeldungen und operative Bedrohungsdaten, um einen Überblick über ungewöhnliches Verhalten in Ihrem System zu behalten. Es ist eine neue Ebene im Spiel.

Wir teilen unsere Bedrohungsdaten konsequent mit der Community – für uns ein zentraler Punkt, um Bedrohungsakteuren einen Schritt voraus zu bleiben. Außerdem behalten wir Kampagnen und Bedrohungsgruppen in großem Maßstab im Blick.

Die Situation ist dynamischer als je zuvor. Unser Ziel ist es, unsere Kunden und die gesamte Branche mit Bedrohungsdaten zu unterstützen, damit die Schutzmaßnahmen verbessert, Gegenmaßnahmen ergriffen und Lücken identifiziert werden können.

Bei diesem Katz-und-Maus-Spiel müssen wir vollen Einsatz zeigen.



John Fokker
HEAD OF THREAT INTELLIGENCE, TRELLIX

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

EINFÜHRUNG: DER CYBERTHREATS-REPORT, JUNI 2024

Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne

Für diesen Bericht hat das Trellix Advanced Research Center Aktivitäten aus dem Zeitraum vom 1. Oktober 2023 bis zum 31. März 2024 untersucht. Dabei zeigten sich Veränderungen bei Bedrohungsaktivitäten sowie eine deutliche Zunahme der geopolitisch motivierten Cyber-Bedrohungen. Hervorzuheben sind vor allem Aktivitäten im Zusammenhang mit regionalen und globalen Ereignissen wie Militärübungen, politischen oder wirtschaftlichen Versammlungen und Gipfeltreffen sowie Wahlen.

Trellix-Analysten sind sich relativ sicher, dass Bedrohungsakteure mit Fokus auf diese Ereignisse an relevanten Informationen über ihre Gegner interessiert sind, proaktiv in Netzwerken nach aktuellen Daten suchen oder sich strategisch in IT-Netzwerken festsetzen, um zu einem späteren Zeitpunkt Angriffe durchführen zu können.

- **Treffen der Präsidenten Biden und Xi in San Francisco:** Im November 2023 zeigten Trellix-Telemetriedaten nur wenige Tage vor dem Treffen zwischen US-Präsident Biden und Chinas Staatspräsidenten Xi in San Francisco im Rahmen des APEC-Gipfeltreffens (Asiatisch-Pazifische Wirtschaftsgemeinschaft) eine Zunahme an böswilligen Aktivitäten von APT-Gruppen, die mit China verbunden sind. Die Anzahl der Bedrohungsaktivitäten ging während und nach der Konferenz erheblich zurück.

  Nach Abschluss des Gipfeltreffens fielen die Bedrohungsaktivitäten auf das niedrigste Niveau seit November 2023. Dieses Muster bei den Bedrohungsaktivitäten deutet darauf hin, dass von China unterstützte Akteure stark durch geopolitische Ereignisse wie APEC beeinflusst werden. Es kann auch darauf hinweisen, dass der Rückzug chinesischer APT-Gruppen während eines großen politischen Ereignisses das öffentliche Image und die internationale Reputation Chinas schützen soll.
- **Der Krieg zwischen Israel und der Hamas:** Auch Bedrohungen mit dem Iran verbundener APT-Gruppen wurden von politischen Entwicklungen rund um den Israel-Hamas-Krieg beeinflusst. In den USA zeigen globale Trellix-Telemetriedaten in den letzten sechs Monaten regelmäßige Spitzen bei schädlichen Aktivitäten mit dem Iran verbundener APT-Gruppen (außer Ende November und Dezember 2023). Die Telemetriedaten demonstrieren insbesondere einen Rückgang bei Bedrohungsaktivitäten gegen US-Organisationen während der Freilassung israelischer Geiseln und des Waffenstillstands Ende November sowie im Dezember 2023. Dabei spielt der Umstand eine Rolle, dass die USA diesen humanitären Waffenstillstand aushandelten und der Iran ein offener Unterstützer der Hamas ist. Hinzu kommt, dass mit dem Iran verbundene APT-Gruppen laut der weltweiten Trellix-Telemetriedaten eine Vielzahl von TTPs wie Phishing, Infostealer, Backdoors, Downloader, schädliche Webshells und häufig ausgenutzte Schwachstellen verwenden, um im beobachteten Zeitraum Organisationen in Israel anzugreifen.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- **Militärübungen:** Parallel dazu können multinationale Militärübungen, mit denen die Einsatzbereitschaft gesteigert werden soll, eine Zunahme bei schädlichen Aktivitäten auslösen. Erst vor kurzem, im März 2024, zeigten die weltweiten Trellix-Telemetriedaten während der gemeinsam von den USA und Südkorea veranstalteten „Freedom Shield"-Militärübungen vom 4. bis 14. März 2024 wiederholte Spitzen bei Bedrohungsaktivitäten in Südkorea. Diese Übungen werden als Reaktion auf die wachsende nordkoreanische Nuklearbedrohung bezeichnet. Ganz konkret überschritt die Zahl der täglichen Bedrohungserkennungen in Südkorea am 7. März sowie am 13. März 2024 die Marke von 150.000 Erkennungen. Das ist mehr als sieben Mal mehr als die hier sonst üblichen 20.000 täglichen Erkennungen.
- **Russland-Ukraine-Krieg:** Der physische Krieg in der Region wird von großen und kleinen Cyber-Initiativen begleitet. Besonders hervorzuheben ist ein Vorfall, bei dem mit Russland verbundene Akteure bei einem Angriff auf den ukrainischen Telekommunikationsanbieter Kyivstar tausende virtuelle Server und PCs mithilfe einer neuen und hochentwickelten Wiper-Malware-Variante löschten. Die Attacke gegen Kyivstar war einer der schwerwiegendsten Cyber-Angriffe auf die Ukraine seit der russischen Invasion im Jahr 2022.

Highlights auf einen Blick

Auch wenn dieser Bericht eine Zusammenfassung verschiedenster Untersuchungen aus unserer Branche liefert, tauchen einige Themen immer wieder auf:

1. **Schnelle und tiefgreifende Veränderungen bei APT-Bedrohungen**
   a. **Mit Russland verbundenes Sandworm-Team eskaliert:** Mit zunehmenden geopolitischen Spannungen steigen die APT-Aktivitäten im gesamten Ökosystem. Auch wenn APT-Bedrohungen insgesamt zahlreicher werden, wurde das mit Russland in Verbindung stehende Sandworm-Team im vom Bericht abgedeckten Zeitraum 40 % häufiger entdeckt.
   b. **China bleibt umtriebig:** Mit China verbundene Bedrohungsgruppen bleiben die aktivsten APT-Player. Trellix registrierte mehr als 21 Millionen Erkennungen bei Aktivitäten dieser Bedrohungsakteure. Mehr als 23 % der weltweit erkannten böswilligen Aktivitäten richten sich gegen den staatlichen Sektor.
   c. **Rasanter Anstieg von Volt Typhoon-Aktivitäten:** Die relativ neue von China unterstützte APT-Gruppe Volt Typhoon nimmt aufgrund ihrer Verhaltensmuster und Angriffstaktiken eine Sonderstellung ein. Seit Mitte Januar 2024 wurden mithilfe von Trellix-Telemetriedaten mehr als 7.100 schädliche Aktivitäten im Zusammenhang mit Volt Typhoon entdeckt, wobei im Zeitraum zwischen Januar und März 2024 immer wieder Aktivitätsspitzen auftraten.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

2. **LockBit mischt das Ransomware-Ökosystem auf**
    a. **Betrüger beeinträchtigen Cybergang-Reputation:** Nach der weltweiten Strafverfolgungsaktion „Operation Cronos“ beobachtete Trellix, wie Betrüger sich als LockBit ausgaben, während die echte Gruppe hektisch alles daran setzte, ihr Gesicht zu wahren und das lukrative Geschäft zu retten.
    b. **USA weiterhin am häufigsten angegriffen:** Die USA bleiben das am häufigsten von Ransomware-Gruppen angegriffene Land, gefolgt von der Türkei, Hongkong, Indien und Brasilien.
    c. **Transportwesen und Versand am häufigsten betroffen:** Ransomware-Akteure hatten die Transport- und Versandbranche vom 4. Quartal 2023 bis zum 1. Quartal 2024 am häufigsten im Visier. Der Sektor generiert 53 % bzw. 45 % der weltweiten Ransomware-Erkennungen und liegt damit noch vor dem Finanzsektor.
    d. **Strafverfolgungsaktion führt zu Verurteilungen:** Kurz vor der Fertigstellung dieses Berichts deckten die weltweiten Strafverfolgungsbehörden die wahre Identität des Drahtziehers von LockBit auf. Weitere Aktionen gegen Ransomware-Kriminelle fanden am 1. Mai statt. Der REvil-Partner, der Kaseya und viele weitere Unternehmen angegriffen hatte, wurde zu 13 Jahren Haft sowie zu Schadenersatzzahlungen in Höhe von 16 Millionen US-Dollar verurteilt.
3. **EDR-Killer-Tools betreten die Bühne**
    a. **Ransomware-Gruppe D0nut tritt auf die Bühne:** Das Auftreten der Ransomware-Gruppe D0nut war besonders wegen der Verwendung eines innovativen EDR-Killer-Tools erwähnenswert. Es demonstriert eine raffinierte Taktik zur Umgehung der Endgeräteerkennung und Steigerung der Effektivität von Angriffen.
    b. **EDR-Umgehungs-Tool von Spyboy für Angriff auf Telekommunikationsanbieter:** Das EDR-Killer-Tool Terminator des Entwicklers Spyboy kam in einer neuen Kampagne im Januar 2024 zum Einsatz. Das Tool wird zur Umgehung von EDR-Lösungen verwendet, und 80 % der Erkennungen dieses Tools richteten sich gegen den Telekommunikationssektor.
4. **Betrugsmaschen zur US-Präsidentschaftswahl**
    a. **Phishing bleibt ein Problem:** Während die Welt dem Ergebnis der US-Präsidentschaftswahl im November entgegenblickt, werden Betrugsversuche beobachtet, die entsprechend gestaltet sind und um Spenden bitten.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

5. **GenAI und der Cybercrime-Untergrund**
    a. **Kostenlose KI-gestützte Tools:** Trellix beobachtete ein kostenloses ChatGPT 4.0-Jabber-Tool, das im Cybercrime-Untergrund erhältlich ist und Bedrohungsakteuren die Möglichkeit gibt, GenAI für ihre Aktivitäten zu nutzen. Zudem kann damit eine GenAI-Knowledge Base aufgebaut werden, um von anderen Cyber-Kriminellen zu lernen oder sogar deren Ideen und Tools zu stehlen.
    b. **Infostealer werden häufiger eingesetzt:** Trellix entdeckte zwei Infostealer (MetaStealer und LummaStealer), die GenAI-Funktionen zur Vermeidung der Erkennung nutzen und die Anwesenheit von Bots in Protokollen erkennen. Durch diese GenAI-Funktionen lassen sich kriminelle Taktiken noch schwerer finden und stoppen.

Methoden: So erfassen und analysieren wir Daten

Die Experten unseres Trellix Advanced Research Center-Teams erfassen die Statistiken, Trends und Einblicke, die in diesen Bericht einfließen, aus verschiedensten weltweiten – offenen sowie geschlossenen – Quellen. Die aggregierten Daten werden in unseren Plattformen Trellix Insights und Trellix ATLAS verarbeitet. Dabei setzt das Team auf intensive, integrierte und iterative Prozesse, die Machine Learning, Automatisierung und menschliche Intuition nutzen, um die Daten zu normalisieren, die Informationen zu analysieren und Einblicke zu gewinnen, die für Cyber-Sicherheitsverantwortliche und SecOps-Teams auf der ganzen Welt nützlich sind. Eine detaillierte Beschreibung unserer Methodik finden Sie am Ende dieses Berichts.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

ANALYSEN, EINBLICKE UND DATEN IN DIESEM BERICHT

Staatliche Akteure und Advanced Persistent Threats (APT)

Von Oktober 2023 bis März 2024 hat Trellix im Vergleich zu den sechs Monaten davor bei APT-bezogenen Erkennungen einen Anstieg von 17 % beobachtet. Das ist bemerkenswert, da wir schon in unserem letzten Bericht auf einen enormen Anstieg von 50 % bei diesen Erkennungen hingewiesen haben. Das APT-Ökosystem unterscheidet sich grundlegend von seinem Zustand vor einem Jahr – es ist aggressiver, raffinierter und aktiver geworden.

In der sich schnell entwickelnden Cyber-Bedrohungslandschaft stellen APT-Gruppen (Advanced Persistent Threat) weiterhin eine große und komplexe Herausforderung für die weltweite Cyber-Sicherheit dar.

Wir werden die APT-Aktivitäten (Advanced Persistent Threats) vom 4. Quartal 2023 bis zum 1. Quartal 2024 gründlich analysieren, wobei wir uns auf die Herkunftsländer dieser Bedrohungen, ihre primären Ziele und die bei ihren Operationen eingesetzten Tools konzentrieren. Wir vergleichen unsere Erkenntnisse mit Daten aus dem 1. Halbjahr 2023 (2. bis 3. Quartal) und ziehen dazu zwei wichtige Messgrößen heran: die prozentuale Veränderung und die Veränderung des proportionalen Anteils.

- Prozentuale Veränderung: Diese Messgröße zeigt uns, ob die Aktivitäten einer speziellen APT-Gruppe, die gezielten Angriffe auf bestimmte Länder oder die Nutzung bestimmter Tools im Zeitverlauf zugenommen haben, abgenommen haben oder gleich geblieben sind. Mit diesen Informationen können wir verfolgen, wie sich das Verhalten dieser Bedrohungsakteure und die Cyber-Bedrohungen selbst insgesamt verändern.
- Veränderung des proportionalen Anteils: Diese Messgröße liefert Kontext, weil sie nicht einfach nur zeigt, dass sich die Aktivitäten verändert haben, sondern wie sich diese Veränderungen mit Blick auf alle Cyber-Sicherheitsbedrohungen darstellen. Wenn zum Beispiel die Erkennungen für einen bestimmten Akteur deutlich zugenommen haben, könnte es sich trotzdem nur um einen kleinen Teil aller Cyber-Bedrohungen handeln, wenn die Bedrohungsumgebung insgesamt viel aktiver geworden ist. Und wenn die Zahl der Erkennungen gesunken ist, der Rest der Bedrohungsumgebung aber noch stärker nachgelassen hat, könnte dieser Akteur an relativer Bedeutung gewinnen.

Mithilfe dieser Messgrößen möchten wir ein nuanciertes Bild von den Veränderungen bei den APT-Aktivitäten vermitteln und Einblicke in strategische Ziele, bevorzugte Methoden und damit einhergehende Herausforderungen für die Cyber-Sicherheit geben. Die folgenden Abschnitte befassen sich eingehend mit diesen Erkenntnissen. Dabei gehen wir auf die komplizierte Welt der APT-Gruppen sowie darauf ein, welche kontinuierlichen Maßnahmen zum Schutz vor komplexen Bedrohungen erforderlich sind.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

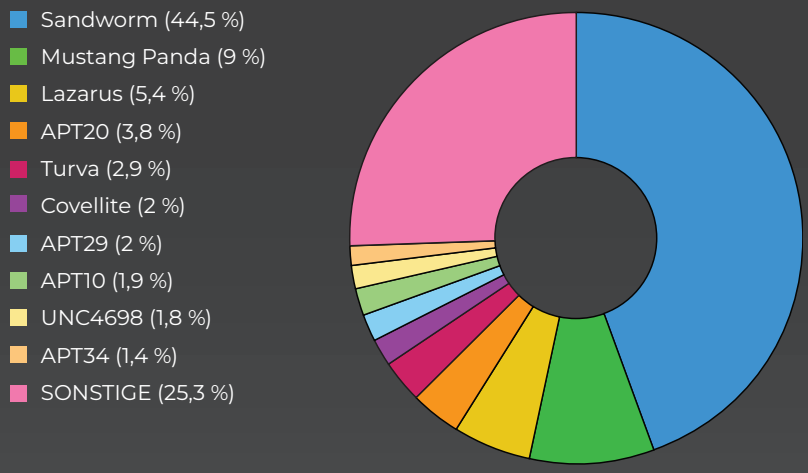
Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Aktive staatliche Akteure und APT-Gruppen

Im Zeitraum von Oktober 2023 bis März 2024 gab es bei den Aktivitäten der verschiedenen APT-Gruppen erhebliche Schwankungen. Dies unterstreicht die Dynamik bei Cyber-Bedrohungen und zeigt, wie sich der operative Schwerpunkt und die Techniken der Akteure verändern.

TOP 10 DER APT-GRUPPEN NACH ERKENNUNGEN, 4. QUARTAL 2023 BIS 1. QUARTAL 2024



VERÄNDERUNGEN BEI DEN AKTIVITÄTEN DER CYBER-BEDROHUNGSGRUPPEN: PROZENTUALE VERÄNDERUNG UND VERÄNDERUNG DES PROPORTIONALEN ANTEILS

Hochentwickelte hartnäckige Bedrohungen	Prozentuale Veränderung	Veränderung des proportionalen Anteils
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 %
Sonstige	-28,99 %	-33,33 %

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- **Taktikwechsel:** Bei dem in der Vergangenheit für seine disruptiven Cyber-Angriffe bekannten Sandworm-Team haben wir eine Zunahme der Erkennungen um sagenhafte 1.669 % mit einer Veränderung des proportionalen Anteils von 40 % verzeichnet. Diese enorme Zunahme lässt auf eine einzigartige Verstärkung der Cyber-Aktivitäten dieser mit Russland verbundenen Gruppe schließen.
- **Aggressive Ausweitung der Operationen:** APT29, eine Gruppe mit langer Geschichte in der Cyber-Spionage, hat ihre Aktivitäten deutlich verstärkt. Die Zahl der Erkennungen stieg um 124 %. Ähnlich starke Steigerungen gab es bei APT34 und Covellite mit 97 % bzw. 85 %, was auf ein schnelleres Tempo ihrer Operationen oder den Beginn neuer Kampagnen hindeutet.
- **Homöostase:** Im Gegensatz dazu verzeichneten Gruppen wie Mustang Panda, Turla und APT28 nur minimale Veränderungen ihrer Aktivitätsniveaus. Die Erkennungen von Mustang Panda zeigten einen Rückgang von 2 %, während die von Turla geringfügig um 3 % stiegen.
- **Neue Akteure:** Bemerkenswert ist die neue Gruppe UNC4698 mit einer Zunahme von 363 % bei den Erkennungen, was den Aufstieg eines potenziell wichtigen neuen APT-Players vermuten lässt.

WAS WISSEN WIR ÜBER UNC4698?

Über diese Gruppe ist nicht viel bekannt. Forscher konnten ihr Verhalten als Gruppenaktivität erkennen, ohne es jedoch bisher zuordnen zu können.

Davon abgesehen ist über UNC4698 bekannt, dass die Gruppe sich auf Industriespionage konzentriert und dabei sensible operative Daten sammelt, die für wirtschaftliche oder sicherheitspolitische Ziele genutzt werden könnten. Angesichts der Vorgehensweise und des regionalen Schwerpunkts der Angriffe steckt wahrscheinlich China dahinter.

Die üblichen Ziele der Gruppe sind Öl- und Gasunternehmen in Asien.

Die Gruppe ist auch dafür bekannt, eine spezielle Malware namens SNOWYDRIVE zu verwenden.

UNC4698 nutzt verschiedene Taktiken, Techniken und Prozeduren (TTPs) im Zusammenhang mit Malware, die über USB-Sticks verteilt wird. Die wichtigsten dieser TTPs sind:

- **Erstzugriff über infizierte USB-Geräte:** Zur Infizierung werden vor allem USB-Laufwerke mit böswilliger Software eingesetzt, die eine Backdoor zum Host-System öffnen soll.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

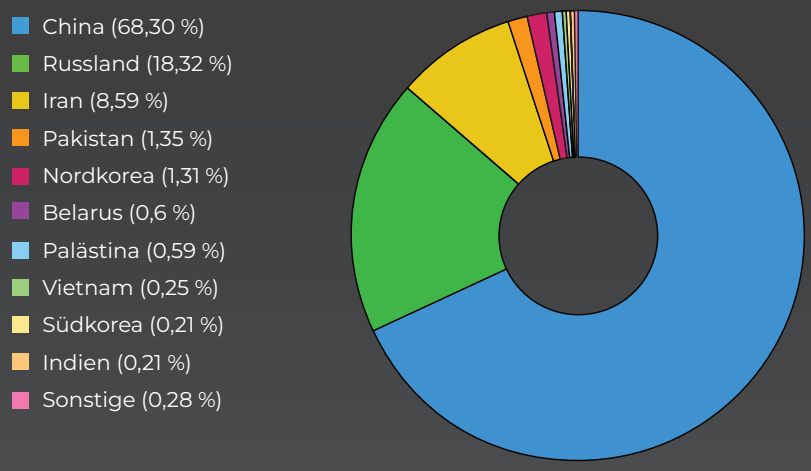
WAS WISSEN WIR ÜBER UNC4698? *(Forts.)*

- **Ausführung über böswillige Dateien:** Die Malware beinhaltet in der Regel einen Dropper, der böswillige ausführbare Dateien und DLLs auf die Festplatte schreibt, um mehr Kontrolle zu erlangen. Diese Dateien tarnen sich oft als legitime Software, sodass sie der Erkennung entgehen.
- **Persistenz und Änderung der Registrierung:** UNC4698 stellt Persistenz auf den infizierten Systemen sicher, indem die Windows-Registrierung dahingehend geändert wird, dass die Malware beim Hochfahren des Systems automatisch startet.
- **C&C-Kommunikation (Command and Control):** Die Malware konfiguriert eine Methode für die Remote-Kommunikation, damit die Angreifer Befehle übermitteln und die kompromittierten Systeme aus der Ferne steuern können.
- **Bewegung innerhalb des Netzwerks über Wechseldatenträger:** Die Malware kann sich selbst auf andere USB-Geräte kopieren, die mit dem infizierten Rechner verbunden sind, und die Infektion damit einfacher an andere Systeme weitergeben.

Bei weniger bekannten oder nicht identifizierten Gruppen beobachteten wir eine Zunahme von 62 % bei den Erkennungen, was auf eine diverse und wachsende Gruppe von Bedrohungen jenseits der gut dokumentierten APT-Gruppierungen hinweist. Der Anstieg des proportionalen Anteils um 8 % ist ein Beleg für die kontinuierliche Weiterentwicklung und Diversifizierung der Cyber-Bedrohungen.

APT-Gruppen und Herkunftsländer

TOP 10 DER MIT APT VERBUNDENEN LÄNDER NACH ERKENNUNGEN, 4. QUARTAL 2023 BIS 1. QUARTAL 2024



INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Bei staatlich unterstützten Cyber-Aktivitäten von Oktober 2023 bis März 2024 weisen die Trellix-Telemetriedaten auch in Bezug auf die Herkunftsländer auf starke Veränderungen hin.



Mit China verbundene Bedrohungsgruppen bleiben die aktivsten APT-Player

- **Erhebliche Eskalation bei den Operationen:** Geopolitische Motive und Cyber-Sicherheitsmaßnahmen entwickeln sich länderübergreifend weiter. Unsere Telemetriedaten machen Folgendes deutlich:
  a. Bei mit Russland verbundenen Bedrohungsgruppen gab es einen signifikanten Anstieg um 31 % bei den APT-Bedrohungen, wobei ihr proportionaler Anteil um 4 % zunahm. Dies deutet auf eine erhebliche Eskalation der Cyber-Angriffe hin und spiegelt möglicherweise strategische Ziele oder Reaktionen auf globale Cyber-Sicherheitsdynamiken wider.
  b. Mit dem Iran verbundene Gruppen haben ihre Cyber-Aktivitäten ebenfalls deutlich ausgebaut, wie die Anstiege um 8 % bei den Erkennungen und 3,89 % beim proportionalen Anteil zeigen. Die deutliche Verstärkung der Cyber-Angriffe passt zu den geopolitischen Zielen des Landes und seiner Beteiligung am Krieg zwischen der Hamas und Israel.
- **Stärkere Diversifizierung:** China bleibt der aktivste APT-Player mit einem leichten Anstieg um 1 % bei den Erkennungen. Sein proportionaler Anteil an der Gesamtzahl der Erkennungen verzeichnete jedoch einen leichten Rückgang um 1 %, was auf eine stärkere Diversifizierung der APT-Herkunftsländer in diesem Zeitraum hindeuten könnte. Im Februar dieses Jahres gab es zudem Berichte über signifikante Anstrengungen der von China unterstützen APT-Gruppe Volt Typhoon, kritische Infrastrukturen in den USA anzugreifen. Mehr dazu im folgenden Abschnitt.
- **Strategiewechsel:** Bei mit Nordkorea, Vietnam und Indien verbundenen Gruppen wurden erhebliche Rückgänge der APT-Aktivitäten verzeichnet (Nordkorea 82 %, Vietnam 80 %, Indien 82 %). Der signifikante Rückgang des proportionalen Anteils Nordkoreas (um 6 %) ist besonders bemerkenswert und deutet möglicherweise auf eine Verlagerung des Schwerpunkts, einen Strategiewechsel oder Veränderungen bei den Möglichkeiten hin.
- **Weitere Länder betreten die Bühne:** Bei mit Pakistan und Belarus verbundenen Gruppen haben wir beachtliche Zunahmen bei ihren APT-Aktivitäten verzeichnet. Ihre Erkennungen stiegen um 55 % bzw. enorme 2.019 %. Diese Zunahmen, insbesondere der exponentielle Anstieg bei Belarus-bezogenen Gruppen, deuten auf neue oder bisher nicht genügend beachtete APT-Akteure hin.

  In der Kategorie „Sonstige“ gab es eine Zunahme um 121 % bei den Erkennungen. Diese Diversität zeigt, dass sich die APT-Aktivitäten nicht auf die am häufigsten erwähnten Länder beschränken. Vielmehr sind Cyber-Bedrohungen ein weltweites Problem und machen eine breit angelegte und anpassungsfähige Cyber-Sicherheitsstrategie erforderlich.

Wir werden diese neuen Muster in den kommenden Monaten genau beobachten.

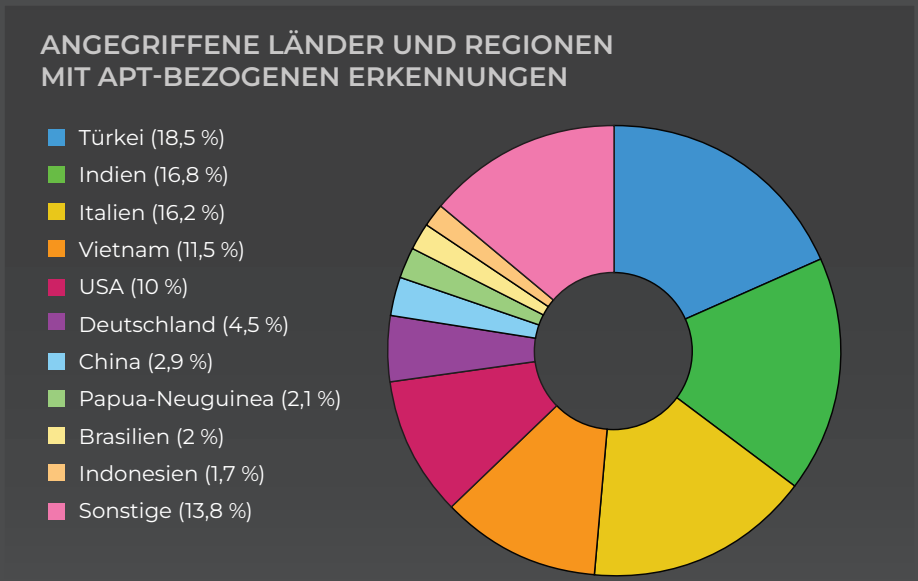
INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix



Angegriffene Länder und Regionen

Dieser Abschnitt konzentriert sich auf die Länder und Regionen, in denen Trellix vom 4. Quartal 2023 bis zum 1. Quartal 2024 APT-bezogene Aktivitäten erkannt hat, die signifikante Veränderungen beim Schwerpunkt und bei der Strategie von APT-Gruppen deutlich machen.

> Die Daten verdeutlichen, dass Cyber-Bedrohungen ein weltweites Problem sind und das Interesse von APT-Gruppen an Ländern sehr unterschiedlich ist.

Das Trellix Advanced Research Center ist sich relativ sicher, dass die erkannten Aktivitäten in bestimmten Ländern und Regionen von folgenden Faktoren beeinflusst wurden.



Die Türkei verzeichnete eine einzigartige Zunahme APT-bezogener Erkennungen.

Operative Ziele:
Die Zahl der Erkennungen bei den gegen die Türkei gerichteten Bedrohungen stieg um enorme 1.458 %, während sich der proportionale Anteil an der Gesamtzahl der Erkennungen um 16 % erhöhte. Dieser bemerkenswerte Anstieg deutet auf eine signifikante Verlagerung des Schwerpunkts bei den Cyber-Bedrohungen in Richtung Türkei hin und ist möglicherweise Ausdruck größerer geopolitischer Spannungen oder spezifischer operativer Ziele von APT-Gruppen.

- **Strategische Bedeutung:** Indien und Italien haben mit 614 % bzw. 308 % ebenfalls beträchtliche Steigerungen bei den Erkennungen verzeichnet. Der Aufstieg dieser Länder in der Liste der Ziele kann ein Zeichen für ihre wachsende strategische Bedeutung in der Cyber-Domäne sein, wobei die Faktoren ökonomischer, politischer oder technologischer Art sein können.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

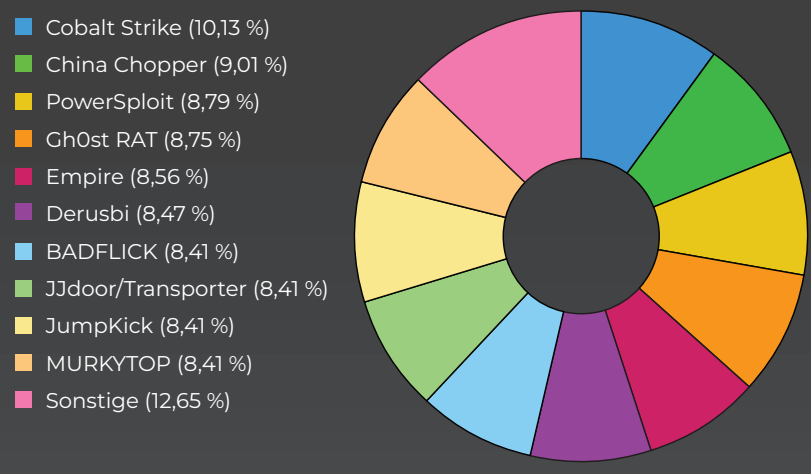
Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- **Der Kreis der angegriffenen Länder wird größer:** Interessanterweise zeigen Vietnam und die USA gegenläufige Trends, obwohl sie weiterhin viele APT-Erkennungen generieren. Während die Erkennungen für Vietnam um 9 % zunahmen, ging der proportionale Anteil um 9 % zurück, was darauf hindeutet, dass der Kreis der angegriffenen Länder größer wird. Bei den USA verzeichneten wir einen moderaten Anstieg um 15 % bei den Erkennungen und einen Rückgang um 7 % beim proportionalen Anteil, was auf eine Diversifizierung der Angriffsstrategien der APT-Gruppen schließen lässt.
- **Geopolitische Entwicklungen:** Deutschland, China, Papua-Neuguinea und Brasilien haben eine Zunahme bei den Erkennungen verzeichnet, wobei sich der proportionale Anteil von Deutschland und China deutlich veränderte. Diese Diversifizierung bei den Angriffszielen spiegelt die strategischen und opportunistischen Anpassungen wider, mit denen APT-Gruppen auf die globale Cyber-Sicherheitslage und geopolitische Entwicklungen reagieren.
- **Stärkung der nationalen Sicherheit:** Indonesien verzeichnete bei den Erkennungen einen deutlichen Rückgang um 48 % und beim proportionalen Anteil einen Rückgang um 4 %. Dies könnte auf eine vorübergehende Depriorisierung oder eine erfolgreiche Stärkung der nationalen Cyber-Sicherheitsmaßnahmen hindeuten.
- **Verstärkter Fokus:** Die in der Kategorie „Sonstige“ zusammengefassten Länder verzeichneten einen Rückgang der erkannten APT-bezogenen Aktivitäten um 23 %, der proportionale Anteil ging um 21 % zurück. Möglicherweise haben sich APT-Gruppen in diesem Zeitraum stärker auf konkrete Ziele von hohem Interesse konzentriert.

Wir rechnen damit, dass sich die Angriffsziele aufgrund geopolitischer Trends weiterhin schnell verändern werden.

Böswillige Tools

TOP 10 DER ERKANNTEN BÖSWILLIGEN TOOLS, 4. QUARTAL 2023 BIS 1. QUARTAL 2024



INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Die Analyse böswilliger Tools, die vom 4. Quartal 2023 bis zum 1. Quartal 2024 bei APT-Kampagnen eingesetzt wurden, zeigt bemerkenswerte Trends bei den Präferenzen und operativen Taktiken der Cyber-Bedrohungsakteure. Die Veränderungen bei den Erkennungsraten und ihren proportionalen Anteilen liefern Einblicke in die Cyber-Bedrohungslandschaft und von APT-Gruppen eingesetzte Tools.

Folgende Trends wurden beobachtet:

- **Offensive Tools werden stärker:** Cobalt Strike ist bei vielen Bedrohungsgruppen weiterhin das Tool der Wahl, auch wenn die Zahl der Erkennungen um 17 % gesunken ist. Der relativ geringe Rückgang beim proportionalen Anteil (1 %) zeigt, dass es weiterhin beliebt und effektiv ist und dass der Schutz vor vielseitigen und weitverbreiteten offensiven Tools eine enorme Herausforderung ist.
- **Angriffstechniken per Webshell, PowerShell und Remote-Zugriff weiterhin beliebt:** Bei China Chopper, PowerSploit und Gh0st RAT verzeichneten wir ebenfalls erhebliche Rückgänge bei den Erkennungen (um 23 %, 24 % bzw. 24 %). Die nur leichten Veränderungen beim proportionalen Anteil deuten darauf hin, dass sie weiterhin sehr häufig von Bedrohungsakteuren eingesetzt werden. Diese Tools sind bekannt für ihre Fähigkeiten im Rahmen von Webshell-Angriffen, PowerShell-Exploits und Remote-Zugriffen. Ihre Beliebtheit zeigt, dass sich Cyber-Kriminelle bei Cyber-Angriffen nach wie vor auf bewährte, vielseitige Tools verlassen.
- **Schwerer erkennbare Tools:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick und MURKYTOP verzeichneten mit einem Rückgang um 25 % bei den Erkennungen ähnliche Abwärtstrends. Dies könnte auf eine größere Verschiebung bei den bevorzugten Angriffs-Tools oder eine Anpassung an Gegenmaßnahmen und Erkennungstechniken zurückzuführen sein, die einen Wechsel zu neueren, schwerer erkennbaren Tools bewirken.
- **Ständige Innovation:** Die Kategorie der „sonstigen“ böswilligen Tools verzeichnete einen deutlichen Anstieg um bis zu 30 % bei den Erkennungen und einen spürbaren Anstieg beim proportionalen Anteil um 6 %. Dies unterstreicht, dass Bedrohungsakteure permanent ihre Techniken und Tools weiterentwickeln und anpassen, um der Erkennung zu entgehen und die eigenen Ziele zu erreichen.

Die sich verändernden Präferenzen bei den eingesetzten böswilligen Tools verdeutlichen, dass Cyber-Bedrohungsakteure sich an Entwicklungen in der Cyber-Sicherheit anpassen.

> Nicht nur die Abwehrmechanismen werden immer raffinierter, sondern auch die offensiven Tools und Taktiken der APT-Gruppen.

Die Zunahme der „sonstigen“ Erkennungen bedeutet einen Wechsel zu einer breiteren Palette von Tools und unterstreicht die Notwendigkeit kontinuierlicher Untersuchungen, Bedrohungsdatenanalysen sowie adaptiver Verteidigungsstrategien, mit denen die Risiken durch diese dynamischen Cyber-Bedrohungen reduziert werden können.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

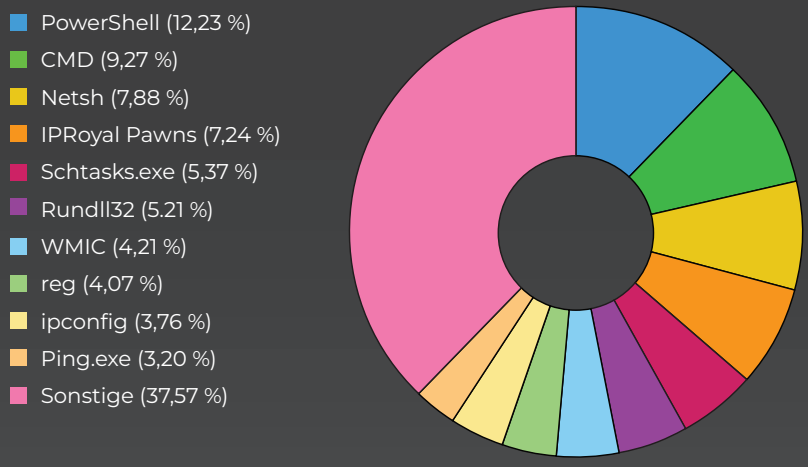
Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Nicht böswillige Tools

TOP 10 DER ERKANNTEN NICHT BÖSWILLIGEN TOOLS, 4. QUARTAL 2023 BIS 1. QUARTAL 2024



> Diese als „Living off the Land“ bekannte Taktik erschwert die Erkennung und unterstreicht die Raffinesse von Bedrohungsakteuren.

Der Einsatz nicht böswilliger Tools bei Cyber-Angriffen von APT-Gruppen vom 4. Quartal 2023 bis zum 1. Quartal 2024 weist auf einen wichtigen Aspekt aktueller Cyber-Bedrohungen hin: die Nutzung legitimer System-Tools für böswillige Zwecke. Diese als „Living off the Land“ bekannte Taktik erschwert die Erkennung und unterstreicht die Raffinesse von Bedrohungsakteuren. Die Statistiken zeigen deutliche Veränderungen bei der Nutzung dieser Tools und betonen deren strategische Bedeutung bei Cyber-Angriffen.

- **Vielseitigkeit:** PowerShell verzeichnete einen erheblichen Anstieg von 105 % bei den Erkennungen mit einer Veränderung des proportionalen Anteils um 1 %. Die wachsende Beliebtheit unterstreicht die Vielseitigkeit und das Potenzial des Tools, zahlreiche böswillige Aktivitäten zu automatisieren – von der Erkundung bis zur Übertragung von Schaddaten.
- **Fokus auf Netzwerkmanipulation:** Bei Netsh und IPRoyal Pawns wurden bei den Erkennungen jeweils erhebliche Zunahmen um 99 % bzw. 102 % verzeichnet. Da diese Tools häufig für Netzwerkkonfigurationen und Proxy-Datenverkehr genutzt werden, weist dies auf einen strategischen Fokus auf Netzwerkmanipulations- und Umgehungstechniken hin.
- **Skalierbare Automatisierung:** Bei Schtasks.exe haben wir mit 138 % die größte prozentuale Veränderung unter allen genannten Tools verzeichnet. Es werden also deutlich häufiger geplante Tasks genutzt, um Persistenz zu erreichen und böswillige Schaddaten auszuführen, ohne dass Benutzer eingreifen müssen.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- **Taktische Veränderungen:** Bei Rundll32 und WMIC haben wir eine zunehmende Nutzung, aber einen Rückgang beim proportionalen Anteil verzeichnet. Dies deutet auf eine Verschiebung der taktischen Präferenzen von APT-Gruppen hin. Die Tools werden jedoch weiter genutzt.
- **Tool-Diversifizierung:** Auch bei Cmd, der guten alten Eingabeaufforderung auf Windows-Systemen, stellten wir eine deutlich stärkere Nutzung fest (Steigerung um 65 %). Der parallele Rückgang des proportionalen Anteils um 2,5 % lässt auf eine stärkere Diversifizierung bei den von APT-Gruppen genutzten Tools schließen.

  Die in der Kategorie „Sonstige" zusammengefassten seltener genutzten oder stärker spezialisierten Tools verzeichneten eine Zunahme bei den Erkennungen um 42 %. Der proportionale Anteil ging deutlich zurück (um 21 %), was auf ein wachsendes Tool-Arsenal der Cyber-Bedrohungsakteure hindeutet.

Die Veränderungen bei den von APT-Gruppen genutzten nicht böswilligen Tools verdeutlichen, warum die Erkennung und Abwehr hochentwickelter Cyber-Bedrohungen so schwierig ist. Die strategische Auswahl und Nutzung dieser Tools offenbart ein genaues Verständnis der angegriffenen Umgebungen und erhebliche Bemühungen, unerkannt zu bleiben.

> **TIPP für CISOs:** Cyber-Sicherheitsmaßnahmen müssen über klassische Malware-Erkennung hinausgehen. Um den Missbrauch legitimer Tools für Cyber-Angriffe zu verhindern, müssen Sie in der Lage sein, Verhalten zu analysieren und Anomalien zu erkennen.

Mit Daten, die über die globalen Sensoren von Trellix ATLAS erfasst, mit strategischen Einblicken aus branchenverifizierten Berichten kombiniert und vom Trellix Advanced Research Center bereitgestellt werden, können unsere Kunden Bedrohungsakteure erkennen, die ihre Branche angreifen. Unsere Verhaltensanalysen bieten zudem die Möglichkeit, ungewöhnliche Verhaltensweisen in ihren Umgebungen aufzudecken.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Fazit

Unsere Analyse der APT-Aktivitäten (Advanced Persistent Threat) vom 4. Quartal 2023 bis zum 1. Quartal 2024 hat gezeigt, dass Cyber-Bedrohungen immer dynamischer und komplexer werden. Die Veränderungen bei den Herkunftsländern der APT-Gruppen, den angegriffenen Ländern sowie den eingesetzten böswilligen und nicht böswilligen Tools machen deutlich, dass die Cyber-Bedrohungsakteure ihre Strategien permanent anpassen.

APT-Gruppen zeigen weiterhin enorme Kompetenz in diesen Bereichen:

1. Anpassungsfähigkeit und Raffinesse
2. Nutzung verschiedener böswilliger Tools
3. Ausnutzung legitimer Systemdienstprogramme für Spionage, zur Störung von Abläufen und zum Stehlen sensibler Informationen

Die bei der Wahl ihrer Ziele und Taktiken beobachteten Veränderungen machen die strategischen Ziele dieser Gruppen deutlich und zeigen, wie sie auf die globalen Entwicklungen in der Cyber-Sicherheit und bei den Abwehrmaßnahmen reagieren.

Die erheblichen Verschiebungen bei den Angriffstaktiken, wobei einige Länder deutliche Steigerungen bei APT-bezogenen Aktivitäten verzeichneten, beleuchten die geopolitischen Motive hinter diesen Cyber-Angriffen. Gleichzeitig verdeutlichen die Veränderungen bei den genutzten Tools (einschließlich die bemerkenswerte Zunahme von „Living off the Land"-Taktiken), warum die Erkennung und Abwehr von APT-Bedrohungen so schwierig ist – zumal es bei legitimen Tools kaum noch möglich ist, legitime und böswillige Aktivitäten zu unterscheiden.

Hinzu kommt, dass die Diversifizierung der APT-Herkunftsländer und Angriffsstrategien darauf hindeutet, dass Cyber-Angriffstaktiken zunehmend weltweit verfügbar sind. Daher ist ein einheitlicher und kollaborativer Cyber-Sicherheitsansatz erforderlich.

> Natürlich ist kein Land oder Unternehmen gegen diese raffinierten Bedrohungsakteure vollständig immun.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Volt Typhoon: Eine von China unterstützte APT-Gruppe

Staatlich gestützte Bedrohungsgruppen stellten auch vom 4. Quartal 2023 bis zum 1. Quartal 2024 eine ernste Bedrohung für Unternehmen und Organisationen auf der ganzen Welt dar. Diese Angreifer haben oft beste technische Voraussetzungen und erhebliche Erfahrung mit raffinierten Cyber-Bedrohungen. Im Gegensatz zu Cyber-Kriminellen und Hacktivisten greifen sie Netzwerke über längere Zeiträume an und können dabei auf hervorragende Kompetenzen und umfangreiche Ressourcen zurückgreifen.

23 %

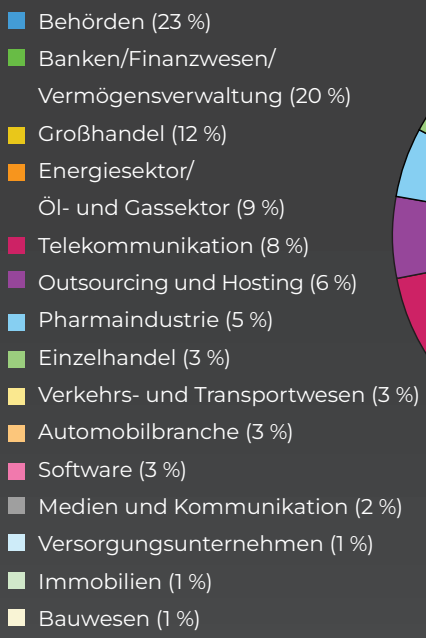
Mehr als 23 % aller weltweit erkannten böswilligen Aktivitäten richten sich gegen den staatlichen Sektor.



Es wurden über 21 Millionen Bedrohungsaktivitäten durch von China unterstützte APT-Gruppen erkannt.

Laut den Trellix-Telemetriedaten stellen von China unterstützte Bedrohungsgruppen weltweit eine wachsende Bedrohung für den staatlichen Sektor dar. Unsere Daten umfassen für den Zeitraum von Oktober 2023 bis März 2024 mehr als 21 Millionen Bedrohungsaktivitäten von APT-Gruppen, die von China unterstützt werden.

WELTWEITE ERKENNUNGEN VON APT-GRUPPEN, DIE MIT CHINA VERBUNDEN SIND



(Quelle: Trellix ATLAS)

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

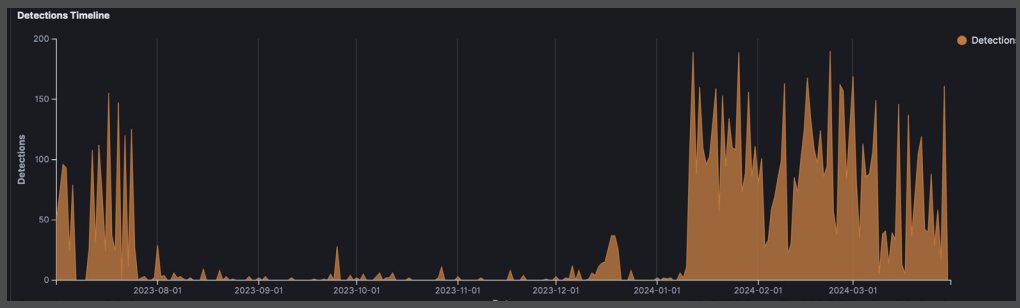
Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Überblick

Die relativ neue von China unterstützte APT-Gruppe Volt Typhoon nimmt aufgrund ihrer Verhaltensmuster und Angriffstaktiken eine Sonderstellung ein, denn diese unterscheiden sich von den konventionellen Cyber-Spionage- und Datenerfassungsaktivitäten anderer mit China verbundener APT-Gruppen. Laut früheren Open-Source-Berichten hat sich diese chinesische APT-Gruppe auf IT-Netzwerke für Industriesteuerungssysteme spezialisiert, um im Falle einer geopolitischen Krise oder eines Krieges laterale Bewegungen zu erleichtern und damit OT-Assets (operative Technologie) sowie Funktionen zu stören. Die Trellix-Telemetriedaten zeigen, dass Volt Typhoon seit den ersten Aktivitäten im Januar 2024 weltweit wiederholt staatliche Einrichtungen (z. B. in den USA) mit „Living off the Land"-Techniken angegriffen hat.

Zeitleiste der Aktivitäten

Laut den globalen Trellix-Telemetriedaten wurde Volt Typhoon Mitte 2021 zum ersten Mal erkannt. Die Gruppe tauchte jedoch von August 2023 bis Januar 2024 bis auf wenige Ausnahmen fast komplett unter. Für diese Pause könnte eine sehr intensive Phase von Ermittlungen in den Monaten nach dem ersten Anbieterbericht zu Volt Typhoon im Mai 2023 verantwortlich sein, der weltweit Aufmerksamkeit erregte. Es könnte aber auch sein, dass Volt Typhoon seine Angriffsinfrastruktur in diesem Zeitraum so veränderte, dass nur wenige Bedrohungsaktivitäten erkannt wurden.



Zeitleiste der erkannten Volt Typhoon-Aktivitäten, Juli 2023 bis März 2024 (Quelle: Trellix ATLAS)

Laut den Trellix-Telemetriedaten wurde Volt Typhoon Mitte Januar 2024 wieder aktiv. Seitdem wurden mithilfe von Trellix-Telemetriedaten mehr als 7.100 schädliche Aktivitäten im Zusammenhang mit Volt Typhoon entdeckt, wobei im Zeitraum zwischen Januar und März 2024 immer wieder Aktivitätsspitzen auftraten.



Details zu den erkannten Volt Typhoon-Aktivitäten, Januar bis März 2024

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Taktiken, Techniken und Prozeduren (TTPs)

Unsere Erkennungsdaten lassen vermuten, dass Volt Typhoon seit der Wiederaufnahme der Aktivitäten Mitte Januar 2024 eine Reihe nativer Windows-Tools und -Funktionen genutzt hat, um Befehle für böswillige Zwecke auszuführen. Bei diesen auch als LOTL (Living off the Land) bezeichneten Tools handelt es sich um Tools mit doppelter Nutzung, die als legitime Software und Funktionen im System verfügbar sind und bei von China unterstützten Akteuren wie Volt Typhoon immer beliebter werden. Eines dieser Tools ist Netsh.exe. Es kann für verschiedene böswillige Zwecke eingesetzt werden, z. B. zum Deaktivieren von Firewall-Einstellungen und Einrichten eines Proxy-Tunnels, über den der Remote-Zugriff auf einen infizierten Host ermöglicht wird. Ein weiteres von den Volt Typhoon-Bedrohungsakteuren genutztes Tool ist Ldifde, mit dem Informationen erfasst werden können.

Nachdem sich Angreifer Zugang zu einem Domänen-Controller verschafft haben, können sie mit Ldifde sensible Daten exportieren oder autorisierte Verzeichnisänderungen vornehmen. Analog können die Volt Typhoon-Bedrohungsakteure auch Ntdsutil für böswillige Aktivitäten nutzen. Dieses legitime Tool wird von Administratoren zum Warten von Datenbanken verwendet, ermöglicht aber auch das Erstellen eines Dumps vom Active Directory, um Anmeldeinformationen zu sammeln und sensible Daten zu exfiltrieren.

Die Volt Typhoon-Bedrohungsakteure haben bei ihren Aktivitäten weiterhin Open-Source-Tools wie FRP, Impacket und Mimikatz eingesetzt. Die Trellix-Telemetriedaten zeigen zudem, dass Volt Typhoon im Februar und März 2023 die folgenden LOTL-Tools und -Befehle verwendet hat:

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

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Volt Typhoon hat laut unseren Telemetriedaten die folgenden wichtigen MITRE ATT&CK-Tools genutzt:

- Erstzugriff – T1190: Ausnutzung von öffentlicher Anwendung
- Ausführung – T1106: Native API
- Persistenz – T1546: Von Ereignis ausgelöste Ausführung
- Erlangen höherer Berechtigungen – T1546: Von Ereignis ausgelöste Ausführung
- Umgehung der Schutzmaßnahmen – T1070.001: Löschung von Windows-Ereignisprotokollen
- Umgehung der Schutzmaßnahmen – T1070: Dateilöschung
- Umgehung der Schutzmaßnahmen – T1027: Verschleierte Dateien oder Informationen
- Zugriff auf Anmeldeinformationen – T1003.003: NTDS
- Zugriff auf Anmeldeinformationen – T1003: Herunterladen von Betriebssystem-Anmeldeinformationen
- Zugriff auf Anmeldeinformationen – T1110: Brute-Force-Angriff
- Zugriff auf Anmeldeinformationen – T1555: Anmeldeinformationen aus Kennwortspeichern
- Erkennung – T1069.002: Domänengruppe
- Erkennung – T1069.001: Lokale Gruppen
- Erkennung – T1083: Erkennung von Dateien und Verzeichnissen
- Erkennung – T1057: Prozesserkennung
- Erkennung – T1010: Erkennung von Anwendungsfenstern
- Erfassung – T1560: Gesammelte Archivdaten
- Erfassung – T1560.001: Archivierung über Dienstprogramm
- Command and Control – T1090.002: Externer Proxy
- Command and Control – T1105: Eintrittstool-Übertragung
- Command and Control – T1132: Datencodierung

Entwicklung der Ransomware-Bedrohungslandschaft

Ransomware-Angriffe haben im 4. Quartal 2023 zugenommen, wobei neue Familien des Jahrgangs vermehrt in den Vordergrund traten.

- **EDR-Killer-Tools:** Die neue Ransomware-Gruppe D0nut war wegen der Verwendung eines innovativen EDR-Killer-Tools besonders erwähnenswert. Es demonstriert eine raffinierte Taktik zur Umgehung der Endgeräteerkennung und Steigerung der Effektivität von Angriffen. Weitere Informationen dazu finden Sie im folgenden Abschnitt.
- **Ausnutzung von Schwachstellen:** In diesem Zeitraum setzte sich der Trend fort, zur vereinfachten Ransomware-Verbreitung kritische Schwachstellen auszunutzen. Insbesondere CVE-2023-4966 (auch als Citrix Bleed bekannt) wurde von LockBit 3.0-Partnern ausgenutzt. Dies belegt, dass kritische Infrastrukturen weiterhin für komplexe Cyber-Angriffe anfällig sind. Darüber hinaus hat die Ausnutzung von CVE-2023-22518 in Confluence Data Center und Confluence Server gezeigt, dass die Angreifer gängige Unternehmensplattformen hauptsächlich infiltrieren, um Ransomware einzuschleusen. Die Ransomware-Kampagne Cactus griff Qlik Sense-Installationen an, indem sie neu

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

entdeckte Schwachstellen ausnutzte. Dies zeigte erneut die Agilität der Angreifer bei der Anpassung an bestehende Sicherheitsmaßnahmen und Ausnutzung neuer Schwachstellen. Insgesamt war das 4. Quartal 2023 für Ransomware-Gruppen ein sehr aktives Quartal.

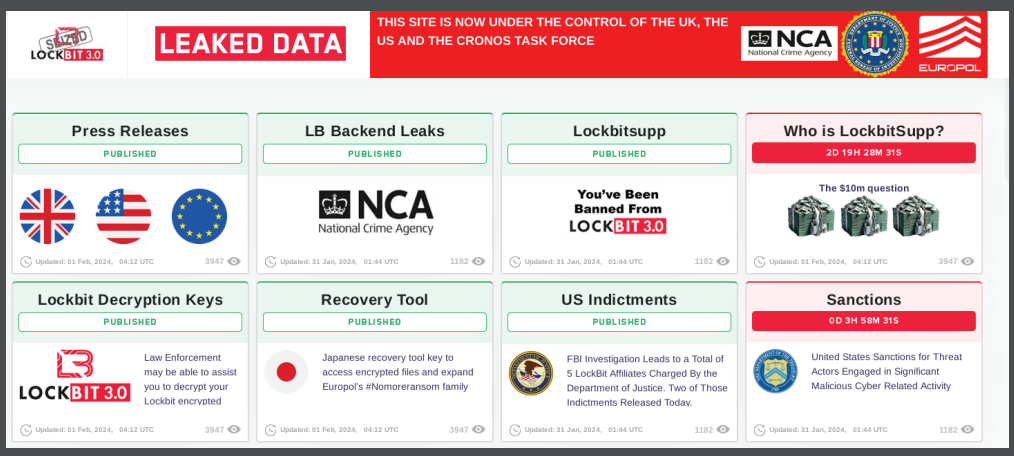
Der Status Quo wurde jedoch im 1. Quartal 2024 durch eine bemerkenswerte Maßnahme der Strafverfolgungsbehörden erschüttert.

Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor

Am 19. Februar 2024 begann die Operation Cronos – eine konzertierte Aktion internationaler Strafverfolgungsbehörden. Sie brachte die Geschäfte der berüchtigten LockBit-Gruppe zum Erliegen und ließ die langlebige kriminelle Gruppierung auch einmal erfahren, wie sich das anfühlt. Neben den Erfolgsmeldungen konnten die Strafverfolgungsbehörden am Ende auch die vollständige Kontrolle über die Leak-Website der kriminellen Gruppe übernehmen und dort selbst einige Leaks präsentieren, um die kriminelle Gruppe so vor der ganzen Welt bloßzustellen. Es wurden verschiedene Anklagen präsentiert, und aktive Partner erhielten bei der Anmeldung beim LockBit-Backend eine freundliche Begrüßungsnachricht, die unmissverständlich zeigte, dass ihre Identitäten bekannt waren.

Diese Aktionen sollten nicht nur den Betrieb von LockBit beenden, sondern auch den Ruf der Gruppe schädigen und das Vertrauen innerhalb der Gruppierung zerstören.

Gegen Ende der Arbeiten für diesen Bericht gab es in der „Operation Cronos“ eine weitere Entwicklung. Die weltweiten Strafverfolgungs-behörden starteten Runde 2, indem sie die wahre Identität des Drahtziehers von LockBit aufdeckten. Dies war jedoch nicht der einzige Sieg der Behörden. Am 1. Mai wurde der REvil-Partner, der Kaseya und viele andere Unternehmen angegriffen hatte, zu 13 Jahren Haft und Schadenersatzzahlungen in Höhe von 16 Millionen US-Dollar verurteilt. Weitere Informationen über die Mitwirkung des Trellix Advanced Research Center im REvil-Fall können Sie hier lesen.



INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Letztes Jahr wurde LockBit in unserem Bericht vom Februar als aggressivste Gruppierung bei Lösegeldforderungen genannt. Diese Cyber-Kriminellen führen ihre Kampagnen mit verschiedenen Techniken durch, zum Beispiel durch Ausnutzen von Schwachstellen, die bereits 2018 entdeckt wurden. LockBit war 2023 im gesamten Jahresverlauf die aktivste Ransomware-Gruppe, die die meisten Opfer auf ihrer Leak-Website postete. Dabei griffen sie vor allem nordamerikanische und europäische Unternehmen aus verschiedenen Branchen an, wobei der Bereich Industriegüter und -dienstleistungen am stärksten betroffen war. LockBit entwickelte sich 2023 kontinuierlich weiter und nahm neue Tools und Methoden in sein Ransomware-Arsenal auf. Zu den bemerkenswerten Ereignissen gehörten die Arbeit an einem LockBit Green-Verschlüsseler auf der Basis des geleakten Codes der Ransomware Conti sowie LockBit-Varianten für Angriffe auf macOS. Darüber hinaus haben wir 2023 ein LockBit-RaaS-Angebot gesehen, das Partnern anderer RaaS-Programme wie ALPHV und NoEscape, die zerschlagen wurden, eine neue Heimat versprach.

Im Nachgang der Maßnahmen der Strafverfolgungsbehörden beobachten wir, dass LockBit hektisch alles daran setzte, ihr Gesicht zu wahren und das lukrative Geschäft zu retten. Angesichts der Publicity zu den kriminellen Aktivitäten von LockBit war dies zu erwarten. Doch im Cybercrime-Untergrund lässt sich ein Server schneller wiederherstellen als über Jahre hinweg aufgebautes Vertrauen. Es bleibt abzuwarten, wie viele Informationen zum Betrieb, zur Rolle und zu den Partnern von LockBit von den Strafverfolgungsbehörden zusammengetragen werden konnten.

> Diese Unsicherheit führt zu einem enormen Risiko für Cyber-Kriminelle, die mit LockBit und deren (früherem) Team zusammenarbeiten wollen.

Die bisher bekannt gewordenen Informationen haben klar gezeigt, dass in der Welt der Kriminellen jeder gegen jeden kämpft. Das Trellix Advanced Research Center hat weitere Akteure beobachtet, die die geleakte LockBit Black-Version nutzen, um die bekannte Marke zu ihrem eigenen Vorteil zu nutzen.

Nachahmer oder nicht, die Opfer waren definitiv real, und die Ereignisse der letzten beiden Quartale haben definitiv das Potenzial für einen guten Film.

Ransomware weltweit

Für unsere Recherchen zu den Ransomware-Aktivitäten im 1. Quartal 2024 haben wir mehrere Quellen untersucht: Leak-Websites, Telemetriedaten und öffentliche Berichte. Ein paar Worte zu jeder der Kategorien.

- **Leak-Websites:** Diese Websites präsentieren Beweise für erpresste Opfer, die das geforderte Lösegeld nicht gezahlt haben, und gewähren damit Einblick in die Aktivitäten der kriminellen Gruppe. Allerdings muss darauf hingewiesen werden, dass die Leak-Websites die Situation nicht zwangsläufig akkurat abbilden. Angesichts der Tatsache, dass sie von Kriminellen betrieben werden, ist klar, dass nicht alle Angaben wahr oder korrekt sind. Sofern die Gruppen Wort halten, werden nur Opfer gelistet, die das Lösegeld nicht gezahlt haben. Somit bleibt das Bild in jedem Fall unvollständig. Die in diesem Bericht verwendeten Daten beziehen sich zwar auf die Gesamttrends bei Leak-Websites, zeichnen aber trotzdem ein aussagekräftiges Bild.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

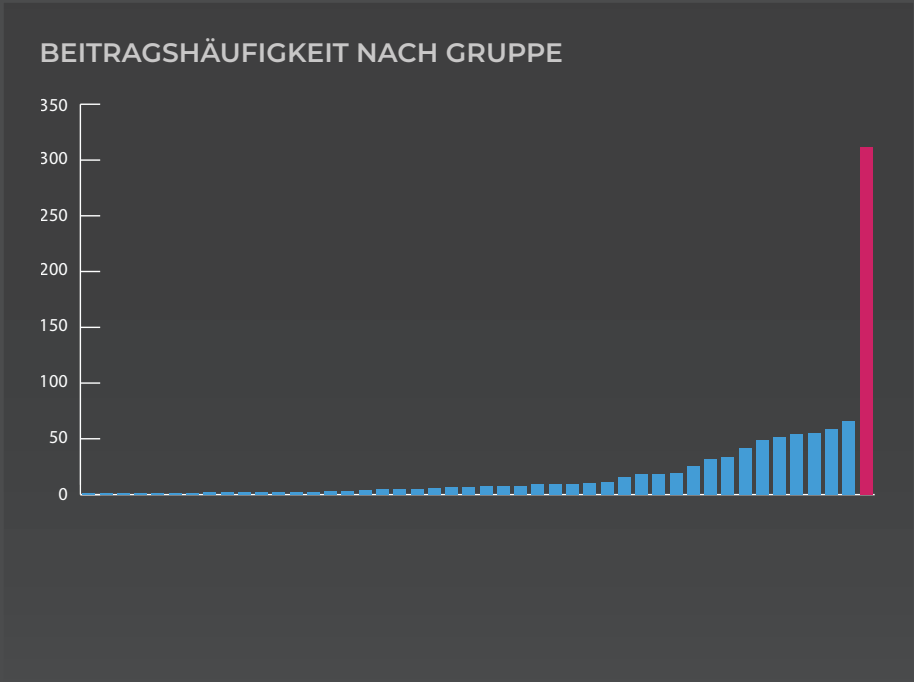
Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- **Telemetriedaten:** Telemetriedaten werden vom Trellix-Sensorökosystem abgeleitet. Eine Erkennung liegt vor, wenn eines unserer Produkte eine Datei, URL, IP-Adresse oder einen anderen Indikator erkennt und dies an uns meldet. Dabei muss es sich nicht bei jeder Erkennung um eine Infektion handeln. Wenn Kunden die Erkennung bestimmter Dateien testen, um ihre internen Regeln zu optimieren, tauchen auch diese Erkennungen in der aggregierten Protokollierung auf. Bei der Betrachtung des Gesamtbildes behalten diese Daten ihre Aussagekraft, da Trends trotzdem deutlich werden.
- **Öffentliche Berichte:** Berichte von Anbietern und Einzelpersonen werden von unserem Advanced Research Center verarbeitet, um Merkmale zu analysieren und Trends herauszuarbeiten. Jeder Bericht beinhaltet eine gewisse Verzerrung, z. B. kann ein Anbieter in einer geografischen Region stärker präsent sein als ein anderer Anbieter, sodass diese beiden Anbieter über unterschiedliche Ereignisse berichten. Aufgrund der verschiedenen Verzerrungen in den analysierten Berichten wenden wir keinen speziellen Filter an.

Aktive Ransomware-Gruppen

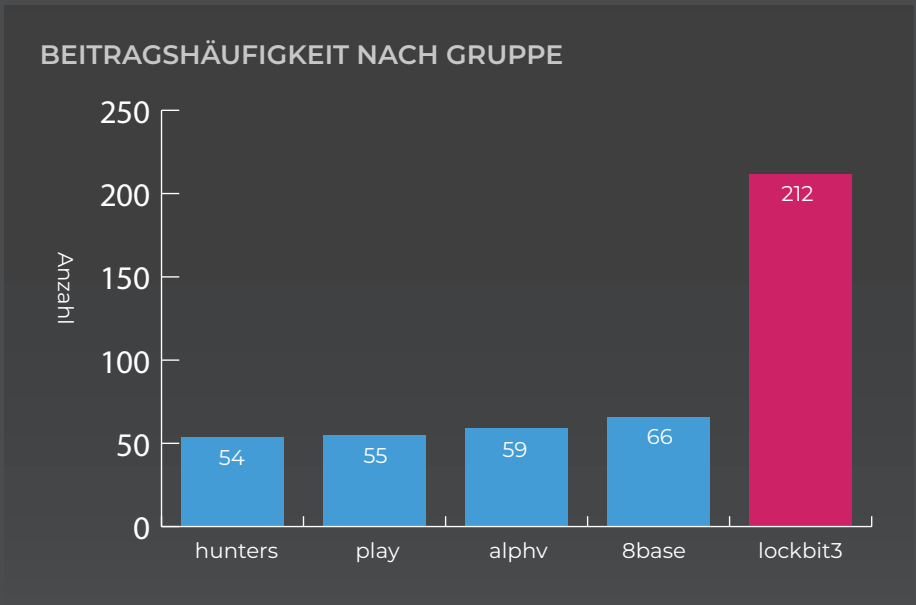
Viele der aggregierten Leak-Website-Posts vom 1. Quartal 2024 sind sehr aktiv. Gelegentlich sehen wir Leak-Websites, auf denen allgemeine Bekanntmachungen gepostet werden. In den meisten Fällen werden jedoch „Beweise“ für Erpressungen präsentiert oder Opferdaten geleakt. Zudem werden Opfer oft mehrfach gepostet. Damit werden die Zahlen aufgeblasen, weil ein Opfer in den Daten mehrfach gezählt wird.



INHALT

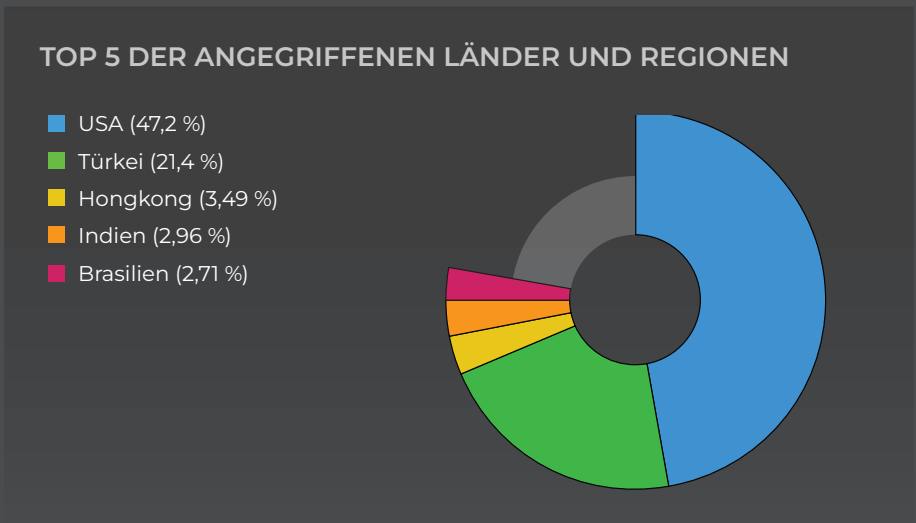
Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
Highlights auf einen Blick
Methoden: So erfassen und analysieren wir Daten
Analysen, Einblicke und Daten in diesem Bericht
Staatliche Akteure und Advanced Persistent Threats (APT)
Aktive staatliche Akteure und APT-Gruppen
APT-Gruppen und Herkunftsländer
Angegriffene Länder und Regionen
Böswillige Tools
Nicht böswillige Tools
Fazit
Volt Typhoon: Eine von China unterstützte APT-Gruppe
Überblick
Zeitleiste der Aktivitäten
Taktiken, Techniken und Prozeduren (TTPs)
Entwicklung der Ransomware-Bedrohungslandschaft
Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
Ransomware weltweit
Die neuen EDR-Killer- und EDR-Umgehungs-Tools
Januar-Kampagne mit EDR-Tool Terminator von Spyboy
Weitere EDR-Killer-Tools beobachtet
E-Mails bleiben eine gefundenes Fressen für Angreifer
Wahlspendenbetrug
Steuer-Phishing
Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
„ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
Nutzung generativer KI bei Infostealern
Bot-Projekt „Telegram Pro Poster“
Nachwort
Methoden
Anwendung: Verwendung dieser Informationen
Erläuterungen zur Analyse in diesem Bericht
Ressourcen
Über das Trellix Advanced Research Center
Über Trellix

Bei der Betrachtung der Häufigkeit von Posts auf den Leak-Websites der fünf aktivsten Lösegeldgruppen stellt LockBit alle anderen in den Schatten. Die Gruppenaktivitäten liegen (außer bei LockBit) bei über 50 Posts pro Quartal, d. h. zwischen den Postings zweier Opfer vergehen im Durchschnitt weniger als zwei Tage. Wie bereits erwähnt, betreffen diese Zahlen Opfer, die nicht gezahlt haben. Das bedeutet, dass die tatsächliche Zahl der Opfer wahrscheinlich höher ist – auch wenn es keine Möglichkeit gibt, ihre genaue Zahl festzustellen.



Angegriffene Länder und Regionen

Anhand der fortlaufenden Aktivitäten der Ransomware-Gruppen können wir Ransomware-Erkennungen innerhalb der Trellix-Telemetriedaten sehen. Die USA generieren die meisten Erkennungen gefolgt von der Türkei, Hongkong, Indien und Brasilien.



INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

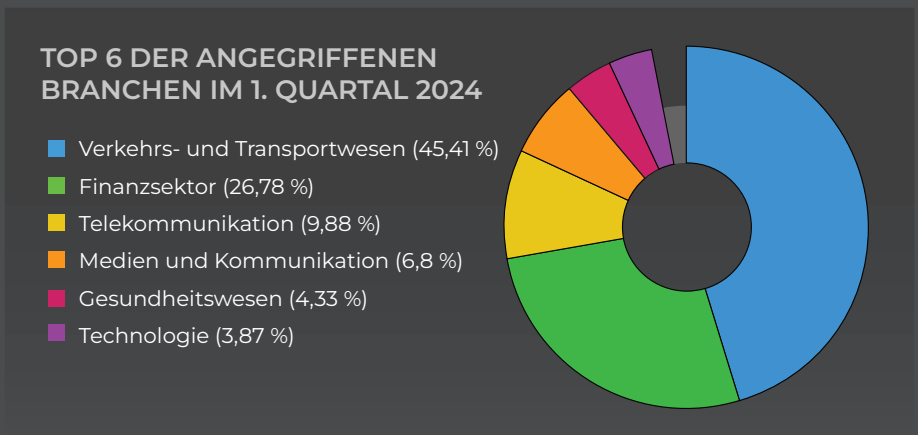
Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Wenn man bedenkt, dass Ransomware eine Bedrohung für alle Branchen in fast jeder Region ist, ergeben die Erkennungsmetriken in Bezug auf die Anzahl der Kunden durchaus Sinn.

Im vorgehenden Quartal sahen die Telemetriedaten relativ ähnlich aus, abgesehen von der Zunahme der Erkennungen in Indien und China. Wir haben keine Hinweise darauf, dass es eine spezielle Kampagne gegen diese Regionen gab, und vermuten, dass Malware-Tests durchgeführt wurden und dort zu einer höheren Zahl von Erkennungen führten.

Angegriffene Branchen

Die Aggregation der globalen Telemetriedaten nach Branche zeigt, dass die Hälfte der Erkennungen aus dem Bereich Transportwesen und Versand und etwas mehr als ein Viertel aus dem Finanzsektor kommen. Diese beiden Branchen machen mehr als 72 % aller Erkennungen aus. Das ist nur logisch, denn die Verfügbarkeit ihrer Dienstleistungen ist von entscheidender Bedeutung. Wenn ein Transportunternehmen aufgrund eines Ransomware-Angriffs keine Güter transportieren kann, muss es seine geschäftlichen Abläufe stoppen, was zu enormen finanziellen Belastungen führt. Analog basiert der Finanzsektor auf Vertrauenswürdigkeit. Kompromittierungen sensibler Daten bzw. Ausfallzeiten aufgrund eines Ransomware-Angriffs treffen Finanzdienstleister ins Mark.



Im 4. Quartal 2023 unterschieden sich die am häufigsten angegriffenen Branchen geringfügig – an der Spitze blieb allerdings alles gleich. Sie vereinten sogar einen noch größeren Anteil auf sich und kamen in diesem Zeitraum zusammen auf insgesamt 78 % aller Erkennungen. Der Technologiesektor und das Gesundheitswesen verzeichneten im 1. Quartal 2024 im Vergleich zum vorhergehenden Quartal einen Rückgang, wobei die Differenz nicht mit konkreten Ereignissen erklärt werden kann.

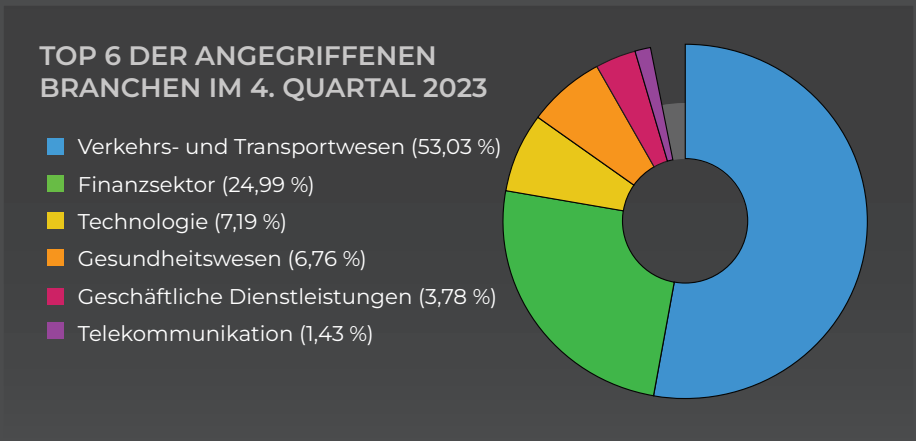
INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix



Tools und Techniken

Die letzte der drei erwähnten Quellen sind öffentliche Berichte. Aus den gesammelten Berichten können MITRE-Techniken, die zugehörigen Tools und Befehlszeilen extrahiert werden.

> **TIPP für CISOs:** Diese Informationen können Blue Teams in Unternehmen für Erkennungszwecke nutzen. Wenn sie sich auf die am häufigsten eingesetzten Techniken und Tools konzentrieren, können sie mehrere Angriffsarten verschiedener Akteure abwehren und dabei mit dem effektivsten Angriff beginnen. Darüber hinaus können sich Red Team- und Purple Team-Übungen auf diese Techniken konzentrieren, um zu testen, welche Erkennungsmaßnahmen bereits wirken.

Die folgende Tabelle listet die häufigsten Techniken in absteigender Reihenfolge auf.

MITRE ATT&CK-Techniken	Individuelle Kampagnen
Datenverschlüsselung für mehr Auswirkung	31
Erkennung von Dateien und Verzeichnissen	23
PowerShell	23
Eintrittstool-Übertragung	21
Erkennung von Systeminformationen	21
Verschleierte Dateien oder Informationen	19
Änderung der Registrierung	18
Windows Command Shell	17
Entschleierung/Dekodierung von Dateien oder Informationen	16
Dienstbeendigung	16

Angesichts der Ziele von Ransomware stehen wenig überraschend Techniken zur Datenverschlüsselung sowie zur Erkennung von Dateien und Verzeichnissen ganz oben auf der Liste. Beim Vergleich dieser Techniken mit den dominanten Techniken des 4. Quartals 2023 lässt sich feststellen, dass überwiegend die gleichen Techniken gelistet werden, lediglich die Platzierung variiert möglicherweise.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

MITRE ATT&CK-Techniken	Individuelle Kampagnen
Datenverschlüsselung für mehr Auswirkung	45
PowerShell	29
Verschleierte Dateien oder Informationen	25
Erkennung von Dateien und Verzeichnissen	24
Windows Command Shell	24
Verhinderung der Systemwiederherstellung	23
Ausnutzung von öffentlicher Anwendung	21
Eintrittstool-Übertragung	21
Prozesserkennung	21
Dienstbeendigung	21

Ebenso wie bei den APTs nutzen Ransomware-Angreifer weiterhin legitime Tools für kriminelle Zwecke. Die verwendeten Tools beeinflussen die beobachteten Techniken, weil ein Tool ein Mittel zum Zweck und damit in diesem Fall eine Technik ist. PowerShell und die Windows Command Shell werden zum Beispiel oft genutzt, um zusätzliche Befehle im System auszuführen, z. B. zum Entfernen von Schattenkopien – ein wichtiger Schritt im Rahmen der Technik „Verhinderung der Systemwiederherstellung". Deshalb sind dies auch die am häufigsten genutzten Tools, wie die folgende Abbildung zeigt.

Name des Befehlszeilen-Tools (laut Attribution)	Eindeutige Kampagnen
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
Reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Die Nutzung von VSSAdmin, BCDEdit und wevtutil deutet darauf hin, dass die Ransomware verhindern soll, dass Systeme von Opfern wieder in einen normalen Zustand wie vor dem Angriff zurückversetzt werden können. Die Nutzung von reg deutet auf Änderungen an der Registrierung hin, die aus verschiedenen Gründen vorgenommen werden können. Malware nutzt oft die Registrierung, um Persistenz zu erzielen. Ransomware legt jedoch keinen Wert auf Persistenz, da sie nach der Verschlüsselung keinen Sinn mehr hat. Stattdessen kann sie andere Einstellungen ändern, um bestimmte Aktionen zu erlauben, die normalerweise nicht möglich wären. Rundll32 wird oft genutzt, um eine DLL (Dynamic Link Library) zu laden und auszuführen, hat aber oft auch eine Prozessinjektion zum Ziel.

Ähnlich wie im vorhergehenden Quartal stehen PowerShell und die Eingabeaufforderung (Cmd) aus genau diesem Grund ganz oben auf der Liste. VSSAdmin und BCDEdit sind ebenfalls vertreten, während das Windows Event Util (wevtutil) nicht in der Liste der häufigsten Tools auftaucht. Angesichts der geringen Zahlen aller erwähnten Tools (der höchste Wert in beiden Quartalen liegt bei 13) überrascht es nicht, dass nicht alle Kampagnen dieselben Tools nutzen. Schon eine kleine Abweichung kann zum Ausschluss eines Tools aus dieser Liste führen.

Name des Befehlszeilen-Tools (laut Attribution)	Eindeutige Kampagnen
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

Ransomware stellt nach wie vor eine Bedrohung dar.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

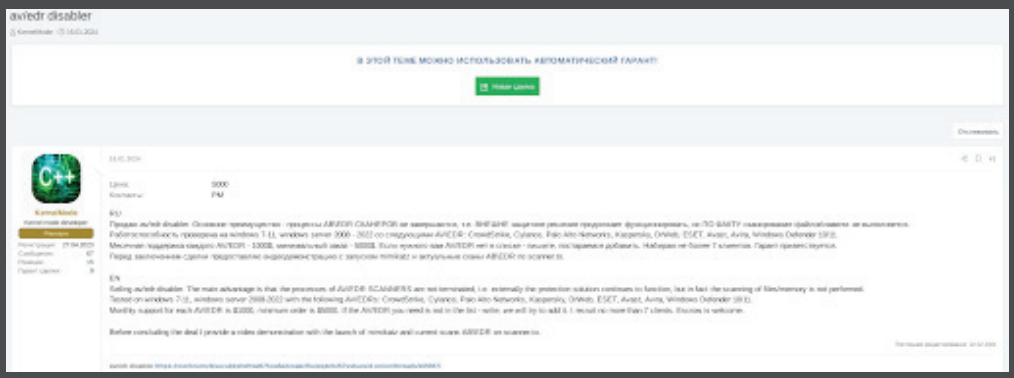
Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Die neuen EDR-Killer- und EDR-Umgehungs-Tools

Durch die weltweite Einführung von EDR-Lösungen in vielen Unternehmen können komplexere Angriffe besser erkannt, verstanden und abgewehrt werden. Bedrohungsakteure nutzen heutzutage oft „Living off the Land"-Binärdateien (LOLBins) und komplexe Angriffsmethoden, können aber durch die EDR-Technologie nicht mehr so einfach unerkannt bleiben.

Die Sicherheit bleibt ein Katz-und-Maus-Spiel – und Angreifer suchen nach Möglichkeiten, EDR-Lösungen zu umgehen oder auszuschalten. Diese Entwicklung hat eine ganze Generation neuer Tools und Techniken zum Ausschalten und Umgehen von EDR-Lösungen hervorgebracht, von denen einige in Cybercrime-Untergrundforen angeboten werden. Wir haben zum Beispiel bereits gesehen, dass die Ransomware-Gruppe D0nut mit ihrem eigenen EDR-Killer-Tool bereits eine gewisse Berühmtheit erlangen konnte.



Werbung für EDR-Killer-Tools im XSS-Untergrundforum

Januar-Kampagne mit EDR-Tool Terminator von Spyboy

Eine gängige Technik, bei der anfällige Treiber ausgenutzt werden, um eine privilegierte Code-Ausführung zu erreichen, wird als BYOVD-Angriff (Bring Your Own Vulnerable Driver) bezeichnet.

Ein Beispiel für diese Methode ist das EDR-Tool Terminator, das von einem Bedrohungsakteur namens Spyboy angeboten wurde. Terminator nutzt einen legitimen, aber anfälligen Windows-Treiber (der zum Malware-Schutz-Tool Zemana gehört), um beliebigen Code aus dem Windows-Kernel heraus auszuführen, mit dem wahrscheinlich CVE-2021-31728 ausgenutzt wird. Terminator tauchte Mitte 2023 erstmals auf. Trellix hat einen detaillierten Knowledge Base-Artikel zur Produktabdeckung veröffentlicht, den Sie hier finden können.

Vom 11. bis zum 17. Januar 2024 verzeichnete das Trellix Advanced Research Center ungewöhnliche Spyboy Terminator-Erkennungen in den Trellix-Telemetriedaten – eine neue Kampagne. Diese Terminator-Kampagne lief an drei Tagen des sechstägigen Zeitraums auf Hochtouren und wurde mehrfach bei einer staatlichen Einrichtung, einem nationalen Versorgungsunternehmen und einem Satelliten-kommunikationsunternehmen erkannt. Angesichts der Ziele dieser Kampagne ist sich Trellix ziemlich sicher, dass der Angriff mit dem Russland-Ukraine-Konflikt im Zusammenhang stand.

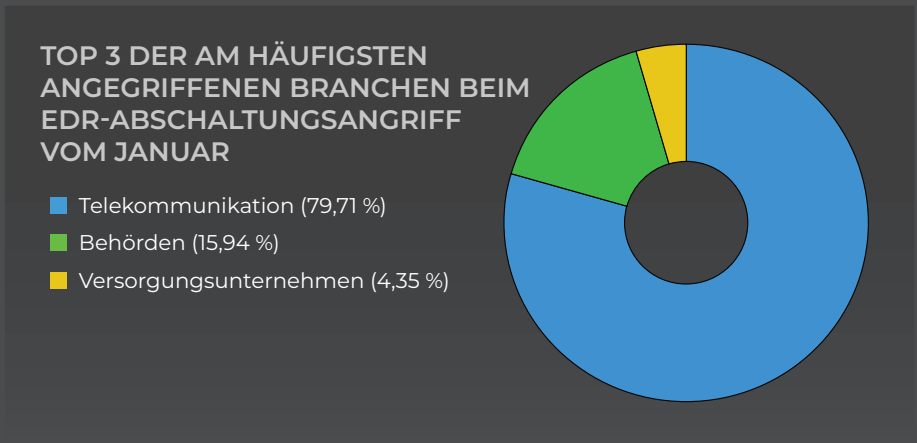
INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

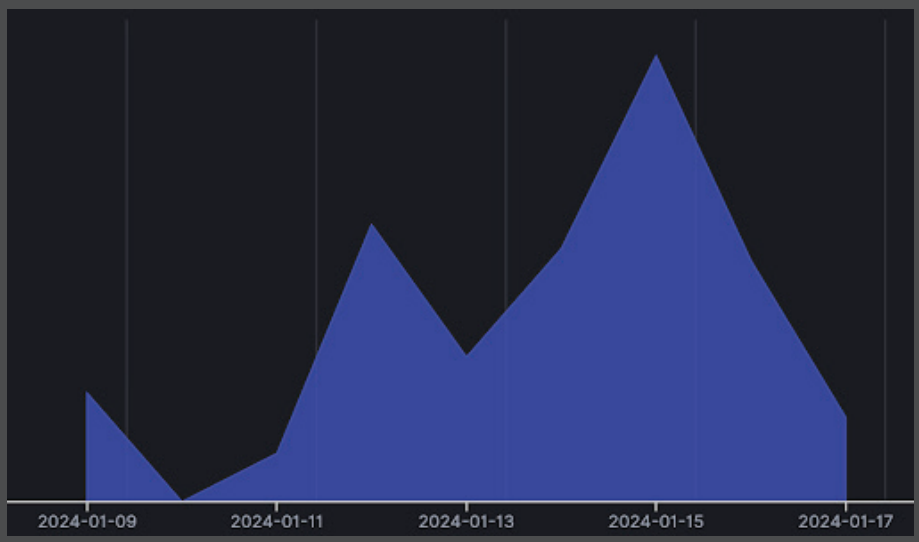




Trellix ATLAS-Erkennungen der EDR-Terminator-Kampagne gegen die Ukraine im Januar

Weitere EDR-Killer-Tools beobachtet

Sophos hatte Anfang 2023 bereits über ein Tool mit ähnlichem Zweck berichtet: AuKill. Dieses Tools nutzte ebenfalls einen eigenen anfälligen Treiber (BYOVD). Terminator und AuKill nutzten zwar verschiedene, aber jeweils legitime Treiber. Allerdings wurden bei einigen Kampagnen 2022 noch eigene böswillige Treiber von den Tools geladen.



INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Der Missbrauch legitimer Treiber für böswillige Zwecke erschwert die Erkennung der Angriffe und fällt mit der zuvor erwähnten LOLBin-Nutzung zusammen. Binärdateien und Treiber unterscheiden sich zwar technisch, Absicht und Motiv sind jedoch ähnlich, wenn nicht sogar identisch. Die Nutzung eines legitimen Treibers erinnert auch an HermeticWiper von 2022. Hier wurde der Treiber genutzt, um alle Daten auf dem Rechner komplett zu löschen, statt den Virenschutz zu deaktivieren. Eine weitere Überschneidung mit der Nutzung des zuvor erwähnten EDR Terminator-Tools und der Attribution von HermeticWiper ist die Nutzung durch einen prorussischen Akteur.

Wir haben auch ein Beispiel gesehen, bei dem Malware über das Discord CDN an einen unserer LATAM-Kunden verteilt wurde. Unser Team hat beobachtet, dass Discord weiterhin für Malware-Angriffe nach diesem Schema genutzt wird.

> **TIPP für CISOs:** Es ist äußerst wichtig, dass jedes SOC seine EDR-Lösung genau überwacht. Warnungen und Protokollierung müssen so eingerichtet sein, dass das SOC sofort informiert wird und geeignete Maßnahmen ergreifen kann, sobald EDR-Tools deaktiviert werden. Deaktivierte EDR-Tools können ein Anzeichen für Manipulation sein. Dann muss schnell gehandelt werden, um den Zugang der Angreifer zu Ihrem Netzwerk zu begrenzen. Zudem muss unbedingt eine gestaffelte Verteidigungsstrategie implementiert werden, die anderen Tools, wie der Plattform für Erkennungs- und Reaktionsmöglichkeiten für Netzwerke (NDR), die Erkennung potenzieller Vorfälle ermöglicht.

INHALT

- Vorwort
- Einleitung
- Einführung: Der Cyberthreats-Report: Juni 2024
  - Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
  - Highlights auf einen Blick
  - Methoden: So erfassen und analysieren wir Daten
- Analysen, Einblicke und Daten in diesem Bericht
  - Staatliche Akteure und Advanced Persistent Threats (APT)
    - Aktive staatliche Akteure und APT-Gruppen
    - APT-Gruppen und Herkunftsländer
    - Angegriffene Länder und Regionen
    - Böswillige Tools
    - Nicht böswillige Tools
    - Fazit
  - Volt Typhoon: Eine von China unterstützte APT-Gruppe
    - Überblick
    - Zeitleiste der Aktivitäten
    - Taktiken, Techniken und Prozeduren (TTPs)
  - Entwicklung der Ransomware-Bedrohungslandschaft
    - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
    - Ransomware weltweit
  - Die neuen EDR-Killer- und EDR-Umgehungs-Tools
    - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
    - Weitere EDR-Killer-Tools beobachtet
  - E-Mails bleiben eine gefundenes Fressen für Angreifer
    - Wahlspendenbetrug
    - Steuer-Phishing
  - Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
    - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
    - Nutzung generativer KI bei Infostealern
    - Bot-Projekt „Telegram Pro Poster“
- Nachwort
- Methoden
  - Anwendung: Verwendung dieser Informationen
  - Erläuterungen zur Analyse in diesem Bericht
- Ressourcen
  - Über das Trellix Advanced Research Center
  - Über Trellix

E-Mails bleiben ein gefundenes Fressen für Angreifer

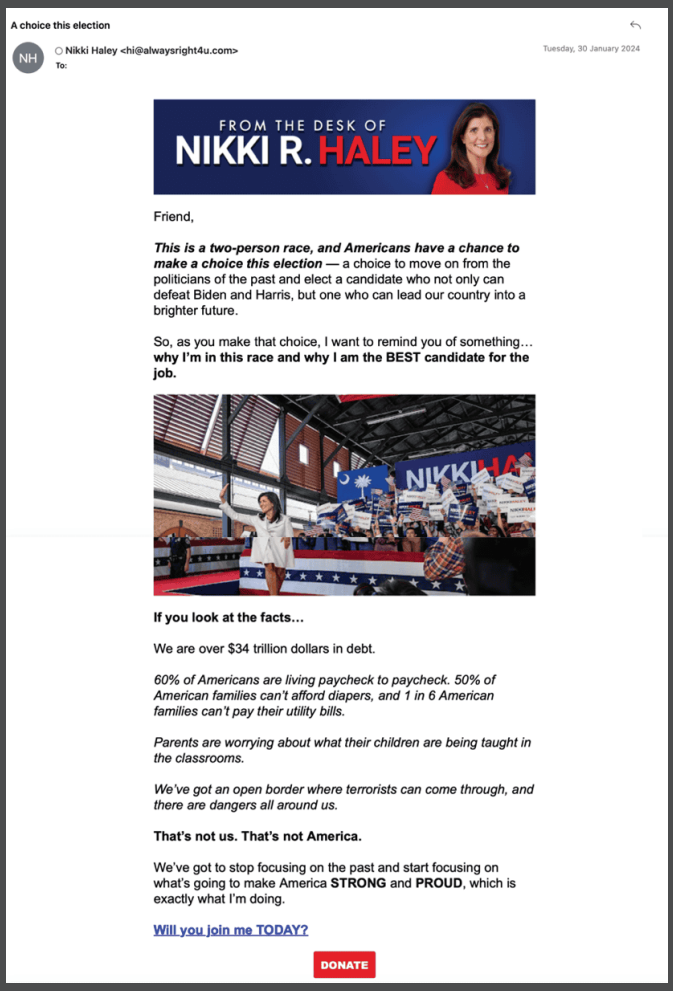
Trellix analysiert pro Tag zwei Milliarden E-Mails und 93 Millionen Anhänge. Dies bedeutet immense Datenmengen und viele Möglichkeiten, neue Techniken zu beobachten, die Akteure bei ihren Angriffen auf Opfer per E-Mail nutzen.

Wahlspendenbetrug

Bei Phishing-Betrug mit Wahlspenden wird der gute Wille von Personen und die Unterstützung für politische Kandidaten ausgenutzt, indem im Namen berühmter politischer Kandidaten patriotische Gefühle angesprochen werden. Im 1. Quartal 2024 haben unsere Forscher Cyber-Kriminelle beobachtet, die mithilfe legitimer Marketing-Services überzeugende Spendenseiten mit Bildern von Kandidaten neben amerikanischen Flaggen erstellen, um die Empfänger zu Spenden zu bewegen.

Bei diesen Betrugsversuchen werden URLs authentischer Marketing-Services genutzt, um Empfängern legitime E-Mails vorzugaukeln. Die E-Mails sollen jedoch die Großzügigkeit der Leute ausnutzen. Links in den E-Mails führen die Benutzer zu Spendenseiten, auf denen sie aufgefordert werden, ihre finanziellen Informationen einzugeben oder Geldbeträge an die Konten oder Wallet-Adressen der Absender zu überweisen.

Unsere E-Mail-Forscher haben die folgenden böswilligen E-Mails für Wahlspenden gefunden.



A choice this election

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

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

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix





Steuer-Phishing

Im steuerlichen Umfeld sind Phishing-Angriffe besonders besorgniserregend. Betrüger geben sich als staatliche Stellen, Steuerbehörden oder namhafte Steuerberater aus, um Personen zur Preisgabe persönlicher Informationen zu bewegen. Sie behaupten zum Beispiel, dass eine Steuernachzahlung fällig ist, Umsätze nicht gemeldet wurden oder eine Steuerrückzahlung ansteht. Ihr eigentliches Ziel sind dabei die Steuer- oder Sozialversicherungsnummern, Bankkontodaten oder andere wertvolle Informationen ihrer Opfer. Die E-Mails enthalten Links, die scheinbar zu offiziellen Webseiten von Behörden oder Finanzämtern gehören, tatsächlich aber zu Betrugswebseiten führen, auf denen die Daten gestohlen werden.

Trellix hat im 1. Quartal 2024 eine Zunahme von E-Mails beobachtet, die angeblich von der australischen Steuerbehörde kamen.

INHALT

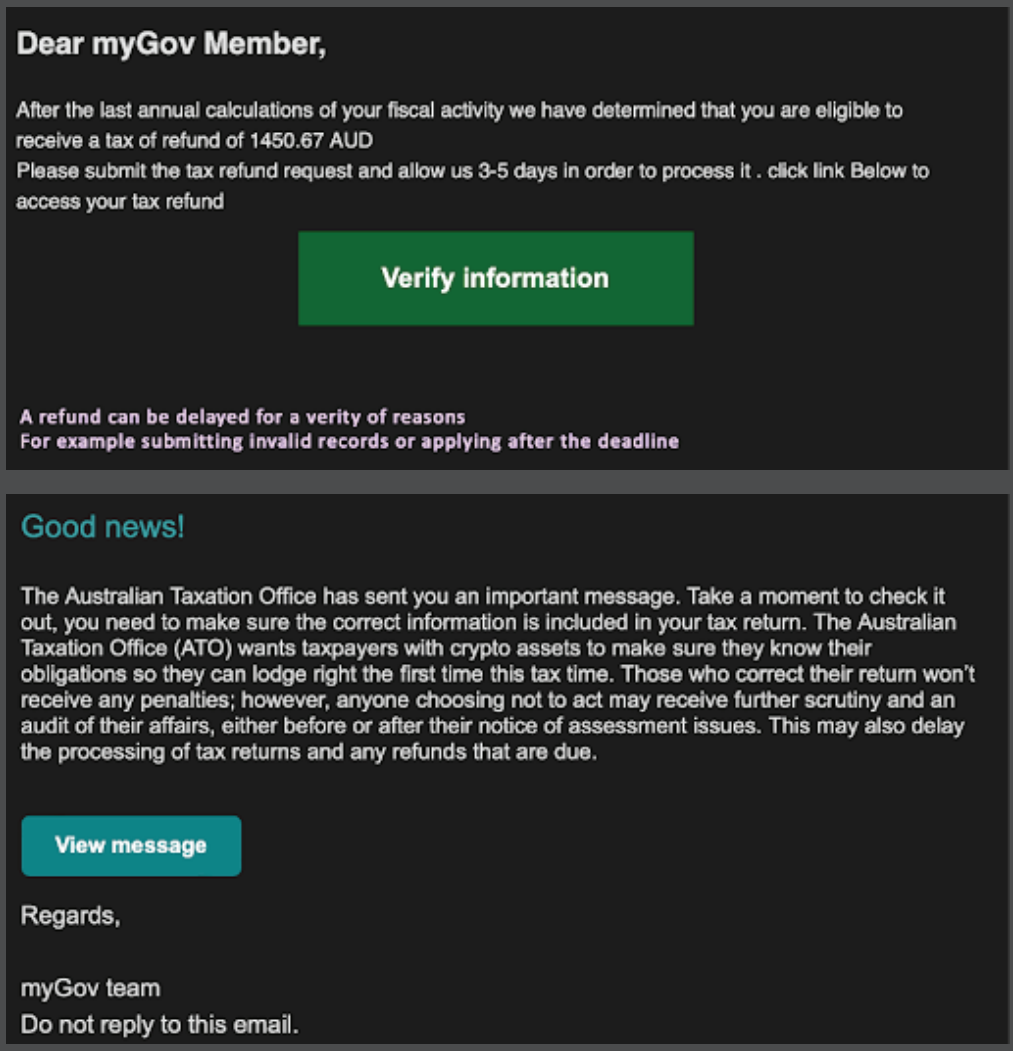
Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

Unten sehen Sie ein Beispiel aus der betreffenden Kampagne. Daraus geht klar hervor, dass Angreifer Dringlichkeit suggerieren, damit der Empfänger auf den Link für die Steuererstattung klickt.



Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund

KI und Machine Learning stehen nicht mehr nur zahlungskräftigen Unternehmen zur Verfügung. ChatGPT und andere Tools können von jedem, auch von Kriminellen, genutzt werden und so ist bei der KI längst ein Wettstreit zwischen den guten und bösen Akteuren entbrannt.
KI ist mächtig und sollte verantwortungsvoll eingesetzt werden, um Unternehmensziele zu erreichen. Unternehmen dürfen aber auf keinen Fall zulassen, dass sich Angreifer damit Vorteile verschaffen. Wir müssen die neuen Möglichkeiten zur Abwehr von Cyber-Kriminellen nutzen – zumal deren Taktiken und Waffen immer raffinierter werden.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

TIPP für CISOs: Die Rolle der CISOs ist noch wichtiger geworden, weil sie den Weg durch diese neue Bedrohungslandschaft weisen sollen. Da die Zahl der Cyber-Angriffe, der Druck durch KI und die Verantwortung steigen, stehen wenig überraschend 90 % der CISOs unter erhöhtem Druck. Es ist wichtig, mit KI und generativer KI Schritt zu halten. Dabei sind sich fast alle CISOs darin einig, dass ihre Unternehmen mehr tun könnten. Mehr dazu lesen Sie im neuesten Trellix-Bericht The Mind of the CISO: Decoding the GenAI Impact (Die Sicht der CISOs: Die Auswirkungen generativer KI).

Bedrohungsakteure werden von generativer KI angezogen, weil sie schnell und günstig ist. Vor allem bietet sie Expertise: Böswillige Akteure können Spearphishing-E-Mails in jeder Sprache mit perfekter Grammatik, Logos und Anmeldeinformationen verfassen. Sie können Exploits zehnmal schneller finden, schreiben und testen, ohne selbst über Expertenwissen verfügen zu müssen.

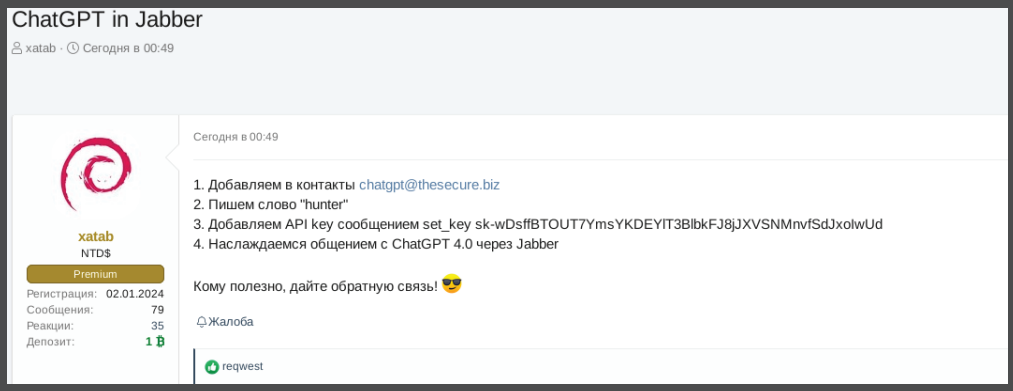
Unser Advanced Research Center-Team durchsucht regelmäßig den Cybercrime-Untergrund, um den Trends zu folgen. Generative KI wird bei Cyber-Kriminellen immer beliebter, und sie berichten über ihre Erfolge und verkaufen ihre Tools. Seit unserem letzten Bericht haben wir Folgendes seit Anfang 2024 beobachtet.

„ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt

Im Januar haben wir beobachtet, dass die Gruppe **xatab** in einem XSS-Untergrundforum nach einem Entwickler suchte, um „ChatGPT 4.0 in Jabber" zusammen mit einer API und einer Benutzeranleitung zu erstellen.

Neben der Vereinnahmung von LLM-Integrationen durch Cyber-Kriminelle ist es auch möglich, dass die Absicht/Motivation von **xatab** hinter dem „ChatGPT in Jabber"-Projekt darin besteht, die Korrespondenz von Bedrohungsakteuren abzufangen und ihre Anfragen zu belauschen, um Informationen und Kenntnisse darüber zu erlangen, woran Cyber-Kriminelle interessiert sind und was ihre Hauptthemen und -bereiche bei den illegalen Aktivitäten sind, die sie mit generativer KI optimieren wollen.

Wir haben Folgendes beobachtet:



xatab postete im XSS-Forum Anweisungen und den API-Schlüssel für „ChatGPT in Jabber"

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über 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!
```

Am 31. Januar 2024 hat **xatab** 2.000 US-Dollar für sein „ChatGPT in Jabber"-Projekt im XSS-Forum geboten. Nach einer kürzlichen XSS-Beschwerde eines Akteurs namens **germans**, der den gewünschten Bot erstellt hat und von **xatab** zunächst ignoriert wurde, hat **germans** scheinbar eingewilligt, für 1.500 US-Dollar einen ChatGPT-Bot in Jabber zu entwickeln. Der Bot wurde für die Jabber-Server des Exploit-Forums (@exploit[.]im) sowie des XSS-Forums (@thesecure[.]biz) erstellt. **xatab** hat ihn im Exploit- sowie im XSS-Forum im Darknet gepostet, wahrscheinlich, um ihn zu testen und Feedback von den Forumsmitgliedern zu erhalten. Der Bot basiert möglicherweise auf dem xmppgpt-Projekt.

xatab gab sich in mehreren Posts im Exploit- und im XSS-Forum als Vertreter eines APT-Teams aus (das in bestimmten Kreisen als erfahrener Pentester bekannt ist) und wies darauf hin, dass er einen Broker für den Zugang zu Unternehmensnetzwerken in den USA, Großbritannien, Kanada und Australien sucht. Er bot 20 % Umsatzbeteiligung für jeden Zugang und zahlte ein BTC an das Exploit- und das XSS-Forum, um seine Absichten bzw. die Ernsthaftigkeit seines Angebots zu unterstreichen.

Durch die Bereitstellung eines kostenlosen ChatGPT 4.0-Schlüssels für die Cybercrime-Community hat **xatab** zwei Dinge erreicht:

1. Die Gruppe unterstützt Bedrohungsakteure und hilft ihnen, generative KI zur Verbesserung und Durchführung ihrer Operationen einzusetzen.
2. Die Gruppe versucht, eine Knowledge Base bzw. einen Pool für generative KI zu erstellen, um von anderen Cyber-Kriminellen zu lernen oder deren innovative Ideen und Tools sogar zu stehlen.

Trellix hat das „ChatGPT in Jabber"-Projekt entsprechend den bereitgestellten Anweisungen getestet, und es scheint wie vom Bedrohungsakteur beschrieben zu funktionieren.

Nutzung generativer KI bei Infostealern

Am 21. Februar 2024 haben unsere Forscher einen Bedrohungsakteur namens MetaStealer beobachtet, der eine neue, verbesserte Version von **MetaStealer** im XSS-Forum bewarb. MetaStealer ist ein Infostealer, der 2021 erstmals in Erscheinung trat und wahrscheinlich ein Ableger des bekannten Infostealers Redline ist. Es wurden schon verschiedene Versionen von **MetaStealer** beobachtet, die neueste von Trellix gefundene Version beinhaltet jedoch eine GenAI-basierte Funktion, die die Erkennung erschwert.

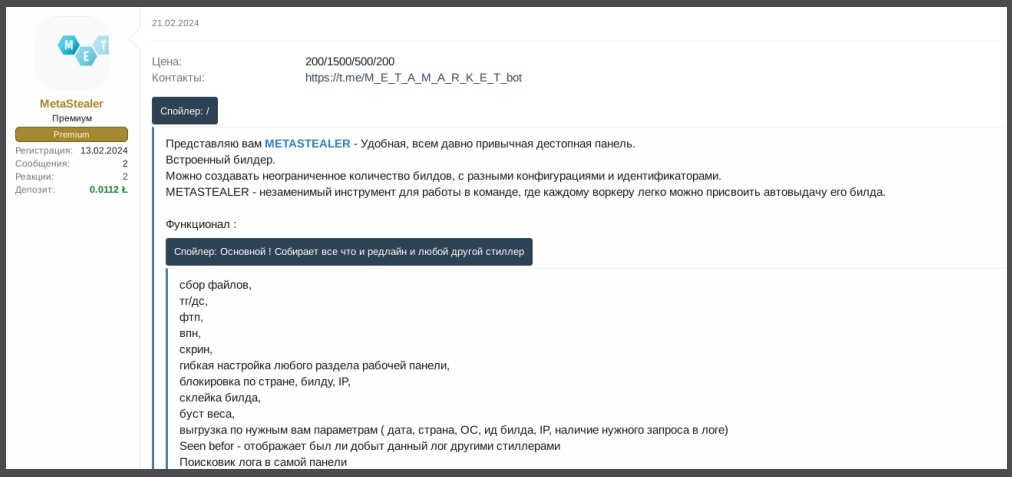
INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

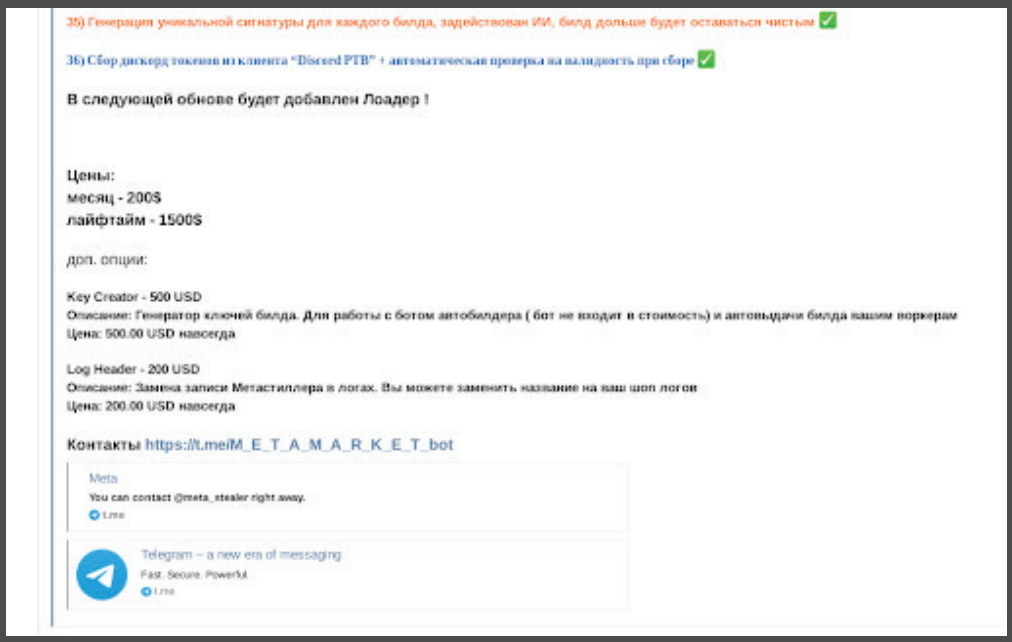
Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix



MetaStealer postete im XSS-Forum eine überarbeitete Version von MetaStealer

Der orange Text im Screenshot unter 35) bedeutet übersetzt „Generierung von individuellen Signaturen für jeden Build, KI wird hier verwendet, der Build bleibt länger sauber (oder unerkannt)“. Dies lässt vermuten, dass die MetaStealer-Entwickler eine neue GenAI-basierte Funktion in ihren Infostealer integriert haben, die individuelle MetaStealer-Builds erstellt, um der Erkennung zu entgehen und länger als bisher von Virenschutz- und EDR-Systemen unerkannt zu bleiben.



Überarbeitete Version von MetaStealer mit integrierter GenAI-Funktion zur Umgehung von Schutzmaßnahmen

Ein weiteres Beispiel ist der bekannte Infostealer LummaStealer. Seit August 2023 haben wir beobachtet, dass das LummaStealer-Team eine KI-basierte Funktion testet, mit der die Infostealer-Benutzer Bots in der Liste der Protokolle erkennen können. Das in LummaStealer eingebettete KI-gestützte System ist potenziell ein benutzerdefiniertes neuronales Netz, das zur Erkennung von Bots in verdächtigen Benutzerprotokollen trainiert wurde.

INHALT

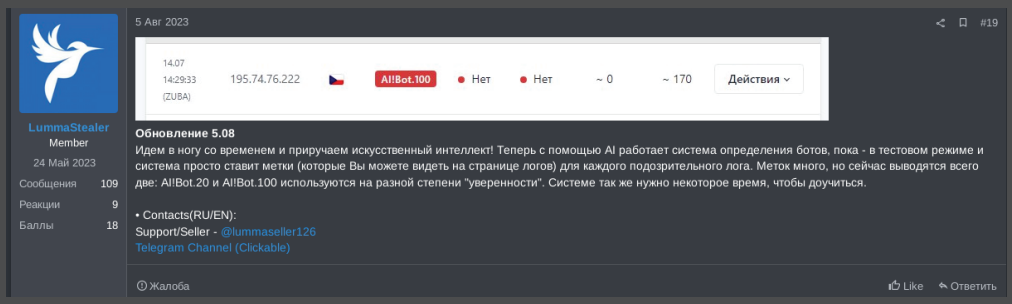
Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

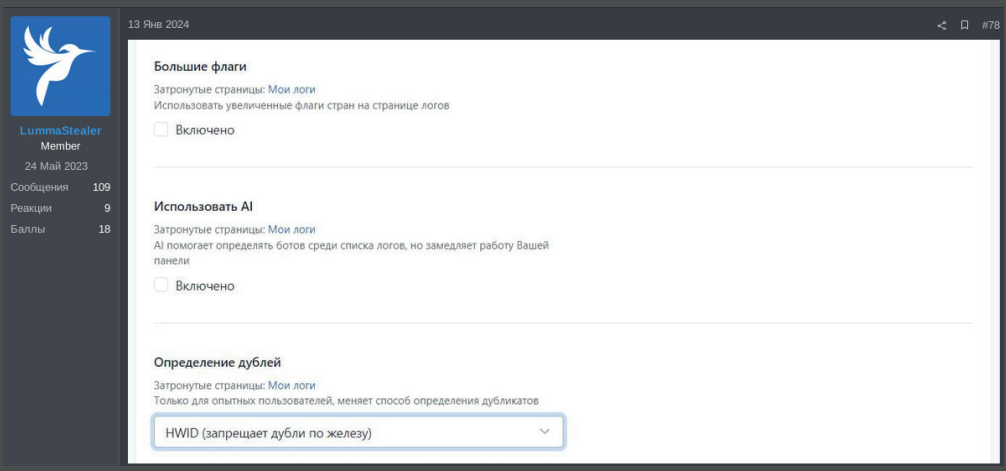
Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

LummaStealer nutzt das Label **AI!Bot.<Nummer>**, um das erkannte Protokoll als Bot zu kategorisieren, wobei <Nummer> scheinbar ein Wert von 0 bis 100 ist, der die Zuverlässigkeit der Bot-Erkennung repräsentiert:



Post von LummaStealer im RAMP-Forum mit Informationen darüber, dass sein Infostealer eine KI-basierte Funktion zur Erkennung von Bots in der Liste von Stealer-Protokollen verwendet

LummaStealer weist seine Benutzer darauf hin, dass das neuronale Netz noch trainiert wird und es noch einige Zeit braucht, um die Erkennungsgenauigkeit zu verbessern. Darüber hinaus hat **LummaStealer** im Januar 2024 mitgeteilt, dass die GenAI-basierte Funktion standardmäßig deaktiviert ist, weil sie die Funktion der LummaStealer-Konsole verlangsamt.



Post von LummaStealer im RAMP-Forum mit Informationen darüber, dass die KI-gestützte Bot-Erkennung standardmäßig deaktiviert ist

Bot-Projekt „Telegram Pro Poster“

Anfang März 2024 hat Trellix einen Bedrohungsakteur namens pepe beobachtet, der sein Projekt „Telegram Pro Poster“ im XSS-Forum als Teil eines Untergrundwettbewerbs für böswillige Tools/Software gepostet hat. Telegram Pro Poster ist ein Bot für die „tiefe Automatisierung von Telegram-Posts.“ Mit diesem Python-basierten Bot können Benutzer eine unbegrenzte Zahl von Telegram-Kanälen autonom verwalten, indem sie die Posts automatisch von den Telegram-Kanälen der „Spender“ in die Zielkanäle kopieren. Neben zahlreichen Funktionen für das Filtern von Posts hat dieser Bot zwei eingebettete GenAI-Funktionen für das Übersetzen von Telegram-Nachrichten und Paraphrasieren von Posts mit ChatGPT.

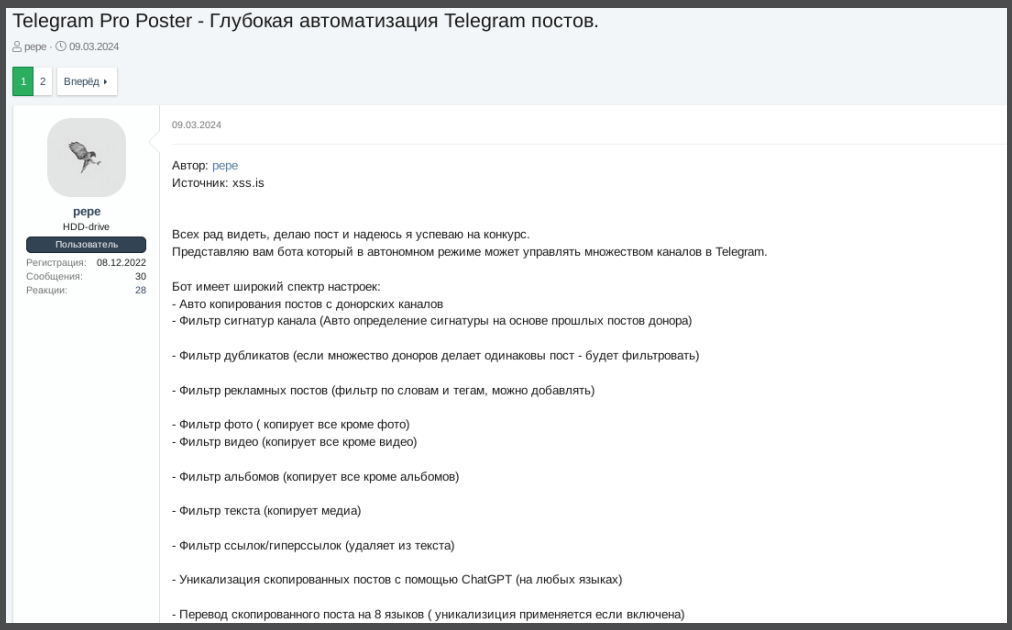
INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

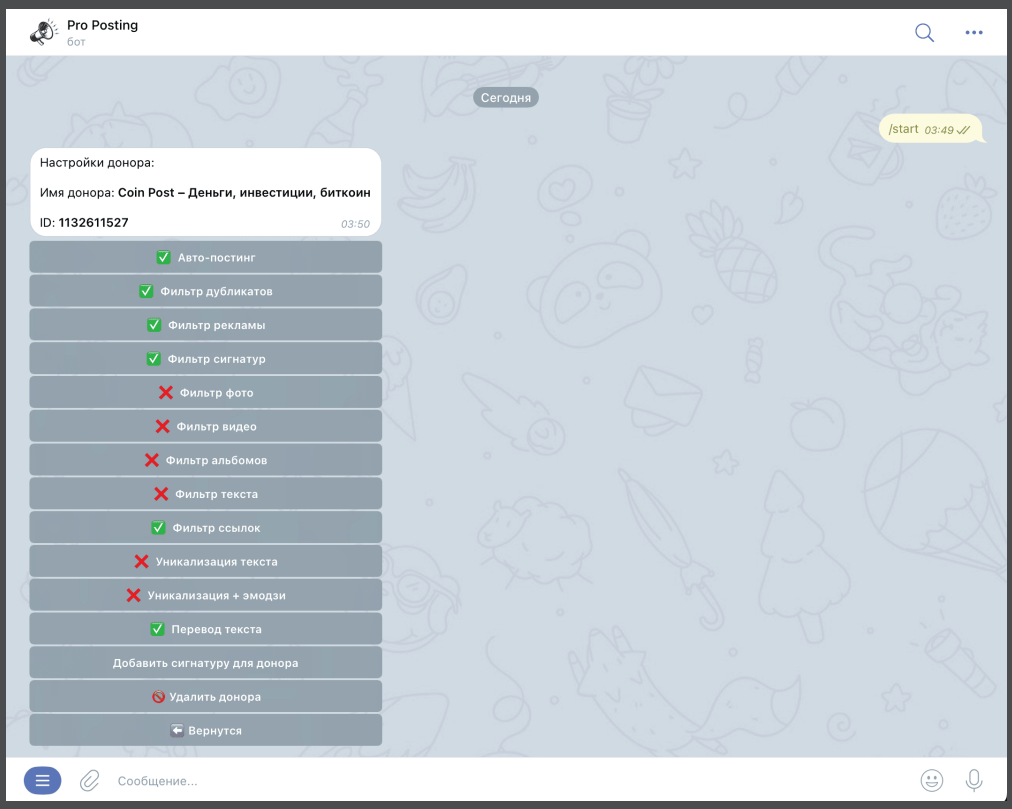
Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix



XSS-Forum-Beitrag zu Telegram Pro Poster für einen GenAI-basierten Bot



Filterfunktion von Telegram Pro Poster besitzt „Einzigartigmachung-Funktion“, die standardmäßig deaktiviert ist

Trellix ist an den Quellcode von Telegram Pro Poster gelangt und konnte die Code-Teile identifizieren, die kopierte Posts von den Spenderkanälen über die ChatGPT-API in acht Sprachen übersetzen, bevor sie an die Telegram-Zielkanäle gesendet werden (siehe Screenshot).

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über 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
```

Die zweite Funktion namens „Unikalisierung“ ist standardmäßig deaktiviert. Wenn sie aktiviert ist, fordert sie ChatGPT mit OPEN_AI_KEY auf, den vorhandenen Text in einer gewünschten Sprache zu paraphrasieren und optional ein Emoji hinzuzufügen.

```
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
```

INHALT

Vorwort

Einleitung

Einführung: Der Cyberthreats-Report: Juni 2024

- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht

- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort

Methoden

- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen

- Über das Trellix Advanced Research Center
- Über Trellix

Die XSS-Community der Cyber-Kriminellen gibt bereits positives Feedback zum Telegram Pro Poster-Projekt. Darin heißt es, dass das Projekt interessant ist und in kompetenten Händen sicherlich sehr nützlich sein wird. Ein weiterer Bedrohungsakteur im XSS-Form-Thread wies darauf hin, dass dieser Bot bereits von verschiedenen Telegram-Kanälen genutzt wird.

NACHWORT

Der Wettlauf ist im Gange

Operative Bedrohungsdaten liefern Erkenntnisse zu Art, Absicht und Zeitablauf bestimmter Cyber-Bedrohungen. Sie sind detaillierter und kontextbasierter als taktische Bedrohungsdaten und liefern Informationen über die Taktiken, Techniken und Prozeduren (TTPs) von Bedrohungsakteuren.

Mithilfe operativer Bedrohungsdaten verstehen Unternehmen den umfassenden Kontext von Cyber-Attacken, z. B. die Motivation der Angreifer oder die verwendeten Methoden. Dadurch können Sicherheitsteams die unterschiedlichen Angriffsarten vorhersehen und sich darauf vorbereiten.

Aus meiner Arbeit mit Kunden weiß ich, dass für jeden CISO das wichtigste Ziel darin besteht, das Risiko für sein Unternehmen zu minimieren. Operative Bedrohungsdaten sind dabei sehr nützlich, weil CISOs und ihre SecOps-Teams damit vorausblicken und eine sichere Basis etablieren können. So lassen sich Lücken in den Sicherheitsmaßnahmen der gesamten Unternehmensumgebung schließen. Diese Daten sind aber auch deshalb wichtig, weil sie einen Blick in die Köpfe der Angreifer erlauben – und damit eine Möglichkeit bieten, ihnen den Weg zu versperren.

Wir teilen unsere Erkenntnisse zu Bedrohungen, um Ihnen eine solide faktenbasierte Plattform bereitstellen zu können, die einige Ihrer wichtigsten Entscheidungen unterstützt. Dadurch können wir Ihre Cyber-Abwehr stärken und Ihnen helfen, den Angreifern im Wettlauf stets einen Schritt voraus zu bleiben.

Auf geht's!



Ashok Banerjee,
CHIEF TECHNOLOGIST, TRELLIX

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort

Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

METHODEN

Erfassung: Trellix und die erstklassigen Advanced Research Center-Experten erfassen die Statistiken, Trends und Einblicke, die in diesen Bericht einfließen, aus verschiedensten weltweiten Quellen.

- **Geschlossene Quellen:** In einigen Fällen werden die Telemetriedaten von Trellix-Sicherheitslösungen in kundeneigenen Cyber-Sicherheits-netzwerken und Schutz-Frameworks öffentlicher und privater Sektoren auf der ganzen Welt generiert. Besonders zu nennen wären hier Technologieanbieter, Infrastrukturbetreiber oder Datendienstleister. Diese Millionen Systeme generieren Daten aus einer Milliarde Sensoren.
- **Offene Quellen:** In anderen Fällen nutzt Trellix eine Kombination aus patentierten, proprietären und Open-Source-Tools, um Websites, Protokolle und Daten-Repositorys im Internet nach Informationen abzugrasen. Wir suchen auch im Darknet nach so genannten Leak-Websites, auf denen Bedrohungsakteure Daten ihrer Ransomware-Opfer veröffentlichen.

Normalisierung: Die aggregierten Daten werden in unseren Plattformen Trellix Insights und Trellix ATLAS verarbeitet. Dabei setzt das Team auf intensive, integrierte und iterative Prozesse, die Machine Learning, Automatisierung und menschliche Intuition nutzen, um die Daten zu normalisieren, die Ergebnisse anzureichern, persönliche Informationen zu entfernen und Korrelationen zu finden, wobei verschiedene Angriffs-methoden, Agenten, Sektoren, Regionen, Strategien und Ereignisse berücksichtigt werden.

Analyse: Als Nächstes analysiert Trellix dieses gewaltige Informationsreservoir anhand (1) der eigenen umfassenden Bedrohungsdaten-Knowledge Base, (2) Cyber-Sicherheitsberichten angesehener und anerkannter Branchenquellen sowie (3) den Erfahrungen und Erkenntnissen von Trellix-Cyber-Sicherheitsanalysten, Ermittlern, Reverse-Engineering-Spezialisten, Forensikern und Schwachstellenexperten.

Interpretation: Daraus gewinnt, überprüft und validiert das Trellix-Team wichtige Erkenntnisse, mit denen Cyber-Sicherheitsverantwortliche und ihre SecOps-Teams (1) die neuesten Trends bei Cyber-Bedrohungen verstehen und (2) mit diesen Einblicken zukünftige Cyber-Angriffe auf ihr Unternehmen vorhersehen, verhindern und abwehren können.

Anwendung: Verwendung dieser Informationen

Alle professionellen Analyseteams und Prozesse müssen die Effekte von Verzerrungen verstehen, erkennen und – sofern möglich – beseitigen. Als Verzerrung (engl. bias) wird die natürliche, tief sitzende oder unsichtbare Neigung bezeichnet, Fakten und ihre Bedeutung zu akzeptieren, abzulehnen oder zu manipulieren. Diese Grundeigenschaft betrifft alle Konsumenten von Inhalten.

Im Gegensatz zu stark strukturierten und kontrollierten mathematischen Tests oder Experimenten basiert dieser Bericht auf einer willkürlichen Stichprobe. Diese Ermessensgrundlage findet sich häufig in medizinischen, gesundheitsbezogenen, psychologischen und soziologischen Tests, die verfügbare und nutzbare Daten nutzen.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

- Kurz gesagt: Unsere Erkenntnisse basieren auf unseren Beobachtungen und umfassen explizit keine Nachweise für Bedrohungen, Angriffe oder Taktiken, die der Erkennung, Protokollierung und Erfassung entgehen konnten.
- Obwohl weder vollständige Informationen noch perfekte Transparenz zur Verfügung stehen, ist diese Art von Untersuchung hervorragend für den Zweck dieses Berichts geeignet: die Identifizierung wichtiger Datenquellen zu Cyber-Sicherheitsbedrohungen und die Entwicklung rationaler, fachkundiger und ethischer Interpretationen dieser Daten, die in empfohlene Vorgehensweisen für die Cyber-Abwehr einfließen.

Erläuterungen zur Analyse in diesem Bericht

Machen Sie mit den folgenden Grundsätzen vertraut, um die Einblicke und Daten in diesem Bericht zu verstehen:

- **Eine Momentaufnahme:** Niemand hat Zugang zu allen Protokollen aller mit dem Internet verbundenen Systeme, nicht alle Sicherheitszwischenfälle werden gemeldet und nicht alle Opfer werden erpresst oder auf Leak-Websites gelistet. Die möglichst umfangreiche Beobachtung kann jedoch das Verständnis der zahlreichen Bedrohungen verbessern und gleichzeitig blinde Flecken bei der Analyse und Untersuchung minimieren.
- **False-Positives und False-Negatives:** Zu den hochleistungsfähigen Trellix-Funktionen zur Überwachung und Telemetrieerfassung gehören Mechanismen, Filter und Taktiken, mit denen sich False-Positives und False-Negatives erheblich reduzieren oder sogar vollständig vermeiden lassen. Dadurch werden die Analyse und die Qualität der Ergebnisse deutlich verbessert.
- **Erkennungen, nicht Infektionen:** Bei Telemetrie geht es um Erkennungen, nicht um Infektionen. Eine Erkennung wird erfasst, wenn eines unserer Produkte eine Datei, URL, IP-Adresse oder einen anderen Indikator erkennt und dies an uns meldet.
- **Uneinheitliche Datenerfassung:** Einige Datensätze müssen sorgfältig interpretiert werden. So enthalten Telekommunikationsdaten zum Beispiel Telemetriedaten von ISP-Kunden, die in zahlreichen anderen Branchen und Sektoren tätig sind.
- **Attribution staatlicher Akteure:** Die Zuordnung staatlicher Verantwortlichkeiten bei verschiedenen Cyber-Angriffen und Bedrohungen kann ebenfalls sehr schwierig sein, da staatlich unterstützte Hacker und Cyber-Kriminelle häufig ihre Identität fälschen oder sich als vertrauenswürdige Quelle tarnen.

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber“-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster“

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix

RESSOURCEN

Threats-Report-Archive

The Mind of the CISO

TRELLIX ARC AUF X FOLGEN

Trellix ARC

Threats-Report-Archive ansehen

Trellix Advanced Research Center

INHALT

Vorwort

Einleitung

Einführung: Der Cyberthreats-Report: Juni 2024

- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht

- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort

Methoden

- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen

- Über das Trellix Advanced Research Center
- Über Trellix

ÜBER DAS TRELLIX ADVANCED RESEARCH CENTER

Das Trellix Advanced Research Center ist Vorreiter bei Untersuchungen zu neuen Methoden, Trends und Tools, die Cyber-Bedrohungsakteure in der weltweiten Cyber-Bedrohungslandschaft nutzen. Unser erfahrenes Forscherteam hilft CISOs, leitenden Sicherheitsverantwortlichen und deren Sicherheitsteams in aller Welt als zuverlässiger Partner. Das Trellix Advanced Research Center stellt Sicherheitsanalysten mit aktuellsten Inhalten operative und strategische Bedrohungsdaten bereit, betreibt unsere branchenführende KI-gestützte XDR-Plattform und bietet Datenprodukte und -dienstleistungen für Kunden weltweit an. Mehr unter https://www.trellix.com/de-de/advanced-research-center.html.

ÜBER TRELLIX

Trellix ist ein globales Unternehmen, das die Zukunft der Cyber-Sicherheit und verantwortungsvolle Arbeit neu definiert. Seine offene und native eXtended Detection and Response-Plattform (XDR) hilft Unternehmen, die mit den raffiniertesten Bedrohungen von heute konfrontiert werden, das Vertrauen in den Schutz und die Resilienz ihrer Abläufe zu stärken. Zusammen mit einem umfassenden Partnerökosystem fördert Trellix die technologische Innovationsfähigkeit durch künstliche Intelligenz, Automatisierung und Analysen, um über 40.000 Geschäfts- und Behördenkunden durch Living Security zu stärken. Mehr unter https://trellix.com/de-de.

Die in diesem Dokument enthaltenen Informationen beschreiben die Forschungsergebnisse zum Thema Computersicherheit. Sie werden Trellix-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Trellix führt die Untersuchungen entsprechend der Trellix-Richtlinie für die verantwortungsvolle Offenlegung von Schwachstellen durch. Jeglicher Versuch, die hierin beschriebenen Aktivitäten teilweise oder vollständig nachzuvollziehen, erfolgt ausschließlich auf Risiko des Benutzers, und weder Trellix noch die Tochterunternehmen können dafür verantwortlich oder haftbar gemacht werden.

Trellix ist eine eingetragene Marke von Musarubra US LLC oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

Trellix

Copyright © 2024 Musarubra US LLC

INHALT

Vorwort
Einleitung
Einführung: Der Cyberthreats-Report: Juni 2024
- Auswirkungen geopolitischer Ereignisse auf die Cyber-Domäne
- Highlights auf einen Blick
- Methoden: So erfassen und analysieren wir Daten

Analysen, Einblicke und Daten in diesem Bericht
- Staatliche Akteure und Advanced Persistent Threats (APT)
  - Aktive staatliche Akteure und APT-Gruppen
  - APT-Gruppen und Herkunftsländer
  - Angegriffene Länder und Regionen
  - Böswillige Tools
  - Nicht böswillige Tools
  - Fazit
- Volt Typhoon: Eine von China unterstützte APT-Gruppe
  - Überblick
  - Zeitleiste der Aktivitäten
  - Taktiken, Techniken und Prozeduren (TTPs)
- Entwicklung der Ransomware-Bedrohungslandschaft
  - Operation Cronos: Strafverfolgungsbehörden gehen gegen LockBit vor
  - Ransomware weltweit
- Die neuen EDR-Killer- und EDR-Umgehungs-Tools
  - Januar-Kampagne mit EDR-Tool Terminator von Spyboy
  - Weitere EDR-Killer-Tools beobachtet
- E-Mails bleiben eine gefundenes Fressen für Angreifer
  - Wahlspendenbetrug
  - Steuer-Phishing
- Das GenAI-Wettrüsten: Erkenntnisse aus dem Cybercrime-Untergrund
  - „ChatGPT in Jabber"-Projekt möglicherweise von krimineller APT-Gruppe aus Russland genutzt
  - Nutzung generativer KI bei Infostealern
  - Bot-Projekt „Telegram Pro Poster"

Nachwort
Methoden
- Anwendung: Verwendung dieser Informationen
- Erläuterungen zur Analyse in diesem Bericht

Ressourcen
- Über das Trellix Advanced Research Center
- Über Trellix