DER CYBERTHREATS-REPORT

Juni 2023

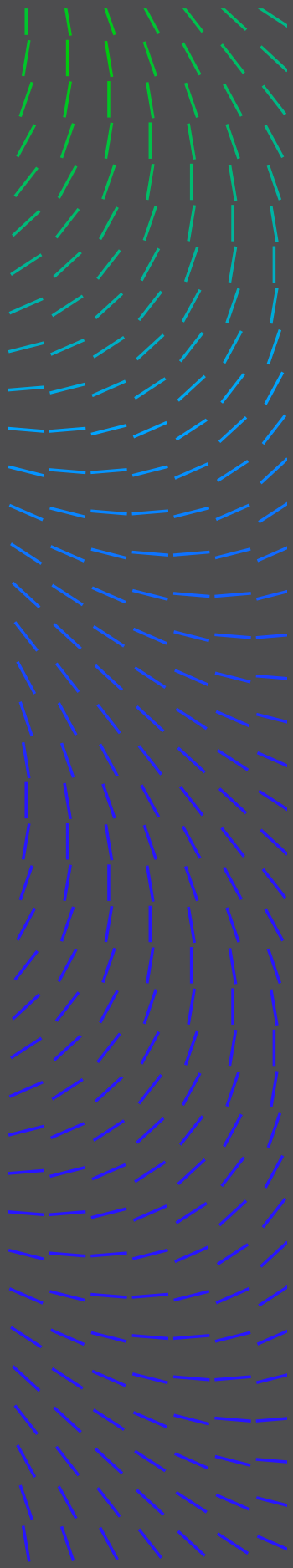
Einblicke aus einem weltweiten Netzwerk von Experten, Sensoren, Telemetrie und Bedrohungsdaten

Präsentiert von

Trellix ADVANCED RESEARCH CENTER

DER CYBERTHREATS-REPORT

Dieser vom Trellix Advanced Research Center verfasste Bericht (1) stellt Einblicke, Bedrohungsdaten und Empfehlungen vor, die aus verschiedenen Datenquellen für Cyber-Sicherheitsbedrohungen gewonnen wurden, und (2) 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. Januar 2023 und dem 31. März 2023 erfasst haben.



Cyber-Bedrohungen entwickeln und vermehren sich in ungebrochenem Tempo und Umfang.

SecOps-Teams haben alle Hände voll damit zu tun, Informationen, Ressourcen und Prozesse abzusichern. Gleichzeitig hat kein Team einen kompletten und vollständigen Überblick über die Bedrohungslandschaft.

Warum? Weil ein Überblick einen weiten Horizont erfordert. Mehrere Quellen. Datenströme. Rohdaten zu Bedrohungen. Enorme Mengen an Telemetriedaten.

Echte Einblicke erfordern einen strategischen unternehmens- und branchenübergreifenden Überblick, der auch geografische Regionen und Angriffsflächen berücksichtigt.

Willkommen beim Cyberthreats-Report vom Juni 2023.

EIN ÜBERBLICK ÜBER DIE RISIKEN, BEDROHUNGEN UND SCHWACHSTELLEN, DIE AKTIV VON ANGREIFERN GESUCHT UND ATTACKIERT WERDEN

Ich führe zahlreiche Gespräche mit Vorstandsmitgliedern, CEOs, CISOs, CIOs, CTOs und anderen Führungskräften, die für die Cyber-Abwehr von Staaten, Behörden und Unternehmen aus dem privaten Sektor und verschiedenen Branchen verantwortlich sind.

Wir sprechen dabei über verschiedenste Themen – von weltweiter Forschung, Innovationen und Bedrohungsdaten bis zu den neuesten Cyber-Abwehrmaßnahmen von SecOps-Teams. Und wir sprechen über ihre konkreten Herausforderungen. Trellix hat diese vor Kurzem im „The Mind of the CISO"-Bericht dokumentiert, wobei folgende Herausforderungen am häufigsten genannt wurden: zu viele unterschiedliche Informationsquellen (35 %), veränderte gesetzliche Anforderungen und Vorschriften (35 %), wachsende Angriffsflächen (34 %), Fachkräftemangel (34 %) sowie fehlende Beteiligung und Einbeziehung durch andere Unternehmensabteilungen (31 %).[1]

Fast jede dieser Interaktionen hat direkt oder indirekt mit der Beschaffenheit der Bedrohungslandschaft zu tun. Welche Arten von Angriffen finden statt? Welche Ransomware-Gruppen waren am erfolgreichsten? Welche Schwachstellen wurden angegriffen? Welche staatlichen Akteure sind am aktivsten? Welche Bedrohungstrends registrieren wir in der E-Mail- und Netzwerksicherheit?

„Das Wissen dieser Vorstandsmitglieder, CEOs, CISOs, CIOs, CTOs oder SecOps-Experten, das wir in diesem Bericht vorstellen und das in die umfangreichen Empfehlungen, Informationen und Ausblicke von Trellix einfließt, kann für den Erfolg Ihrer Arbeit entscheidend sein."

Wir bei Trellix haben viel zu berichten, weil wir jeden Tag an vorderster Front für Sie kämpfen. Wir verfügen über enorme Bedrohungsdaten, Einblicke und Informationen, die wir von mehr als einer Milliarde Sensoren auf der ganzen Welt erhalten. Das Wissen dieser Vorstandsmitglieder, CEOs, CISOs, CIOs, CTOs oder SecOps-Experten, das wir in diesem Bericht vorstellen und das in die umfangreichen Empfehlungen, Informationen und Ausblicke von Trellix einfließt, kann für den Erfolg Ihrer Arbeit entscheidend sein.

Mein Kollege John Fokker, der beim Advanced Research Center-Team von Trellix für Bedrohungsdaten verantwortlich ist, hat hier einen hervorragenden Bericht zusammengestellt. Mit diesen Einblicken können Sie den Fokus Ihres Teams ausrichten, Ihre Prozesse straffen und die richtigen XDR-Technologien implementieren. Ein Hinweis in eigener Sache: Wir freuen uns über Tipps dazu, auf welche Bereiche wir uns in zukünftigen Ausgaben konzentrieren sollen, damit Ihr Unternehmen sicher geschützt und erfolgreich ist.

Joseph (Yossi) Tal
SENIOR VICE PRESIDENT, HEAD OF TRELLIX ADVANCED RESEARCH CENTER

UNTERSTÜTZUNG DER CYBER-SICHERHEITSHELDEN AN VORDERSTER FRONT

Ich arbeite mit Helden zusammen. Dabei meine ich nicht mein Team, obwohl es aus Experten besteht, denen während ihrer Karriere im öffentlichen und privaten Sektor Superkräfte nachgesagt werden.

Damit meine ich Sie. Ich meine die Menschen und weltweiten Teams, die sich auf die erweiterten Forschungsmöglichkeiten von Trellix – unsere Systeme, Erkenntnisse und Daten – verlassen, um ihre Unternehmen und Organisationen vor Cyber-Angriffen zu schützen. Das betrifft CISOs, CTOs und CIOs ebenso wie unsere Kollegen bei Agenturen wie Europol, beim FBI und der NSA, der CISA (Cybersecurity and Infrastructure Security Agency), beim ACSC (Australia's Cyber Security Centre) und beim NCSC-UK (United Kingdom's National Cyber Security Centre). Ebenso – und sogar ganz besonders – meine ich jedes einzelne Mitglied Ihres SecOps-Teams.

„Wie Sie aus Ihrem beruflichen Alltag nur allzu gut wissen, entwickelt sich Cyber-Sicherheit mit unglaublicher Geschwindigkeit. Dazu gehören bahnbrechende Technologien und ein starker Wechsel zu XDR."

Was denken Sie, welche Faktoren besonders zum Erfolg Ihres SecOps-Teams beitragen? Laut dem Trellix-Bericht, den mein Kollege Joseph Tal bereits erwähnt hat, sind sich die Cyber-Sicherheitsverantwortlichen auf der ganzen Welt einig und nennen vor allem verbesserte Transparenz (44 %), stärkere Priorisierung auf Wesentliches (42 %), breiter aufgestellte Zusammenarbeit zur Abwehr von Multi-Vektor-Angriffen (40 %) sowie verbesserte Genauigkeit (37 %).[2]

Für jeden dieser Faktoren werden vor allem zuverlässige Erkenntnisse, Informationen und Daten benötigt. Die Inhalte in diesem Bericht sind ein Beispiel dafür.

Wie Sie aus Ihrem beruflichen Alltag nur allzu gut wissen, entwickelt sich Cyber-Sicherheit mit unglaublicher Geschwindigkeit. Dazu gehören bahnbrechende Technologien und ein starker Wechsel zu XDR, neue Tendenzen in der Gesetzgebung – von Gesetzen zu Haftungsansprüchen – sowie Veränderungen in der Bedrohungslandschaft. Bei den Ansätzen, mit denen SecOps-Teams der nächsten Generation von Cyber-Angriffen „einen Schritt voraus" bleiben können, vollzieht sich eine Revolution. Wenn Sie gewinnen wollen, benötigen Sie zunächst Einblicke und ein umfassendes Verständnis der aktuellen Situation.

Wir ziehen alle an einem Strang. Trellix unterstützt Sie bei der Bewältigung der Herausforderungen. Dieser Bericht richtet sich an Sie.

John Fokker
HEAD OF THREAT INTELLIGENCE
AND PRINCIPAL ENGINEER
TRELLIX ADVANCED RESEARCH CENTER

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

EINFÜHRUNG

Strategischer Kontext: Eine Welt im Umbruch

Für das Interpretieren der Daten in diesem Bericht ist es notwendig, das große Ganze im globalen Maßstab zu verstehen, da Cyber-Bedrohungen für Unternehmen nicht in einem technischen Vakuum entstehen. Zu den wichtigsten Faktoren bei Cyber-Risiken gehören Kriege und Naturkatastrophen, erhebliche wirtschaftliche Umwälzungen sowie neue Schwachstellen aufgrund von Veränderungen bei Geschäftsmodellen, wichtigen Partnern, zentralen Prozessen, neuen Technologien und gesetzlichen Vorschriften. Die folgenden Faktoren sind in unsere Bedrohungsdaten für das 1. Quartal 2023 eingeflossen:

Russlands Invasion in die Ukraine und asymmetrische Kriegsführung gegen den Westen: Cyber-Aktivitäten für Spionage, Kriegsführung und Desinformation zu politischen, wirtschaftlichen und territorialen Zwecken von großen Staaten eskalieren weiterhin. Hacker setzen auf immer raffiniertere Cyber-Angriffe gegen westliche Unternehmen, staatliche Stellen und Infrastrukturen.

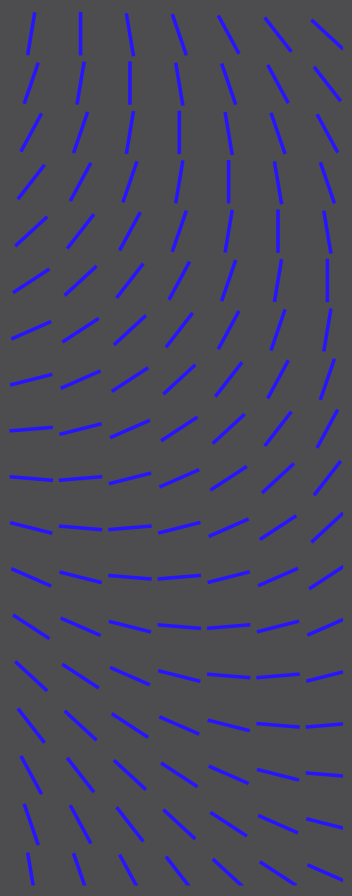
Xi Jinpings konsolidierte Kontrolle über China und geopolitische Ambitionen: Die nationalen Ziele Chinas, die selbstbewusste Außenpolitik sowie Wirtschaftsspionage sind treibende Cyber-Risikofaktoren, da mit China in Verbindung stehende APT-Gruppen (Advanced Persistent Threats, hochentwickelte hartnäckige Bedrohungen) die weltweite Bedrohungslandschaft dominieren.

Schwellenländer und schnelles Wachstum der Infrastruktur: Viele Schwellenregionen verzeichnen zunehmendes Wirtschaftswachstum und forcieren das Wachstum ihrer Infrastrukturen sowie Technologien. Dabei steht Cyber-Sicherheit nicht immer an erster Stelle, was zu entsprechenden Schwachstellen in kritischen Infrastrukturen führt.

Weltweite Inflation und deren wirtschaftliche sowie politische Auswirkungen: Dieses Quartal war geprägt durch Marktschwankungen, finanzielle und politische Krisen sowie vom Druck auf Ausgaben und Cyber-Sicherheitsbudgets.

Ständige Post-COVID-Lieferkettenunterbrechungen: Neue regionsübergreifende Markteinführungswege erforderten einen Wechsel von Partnern, Transportnetzwerken sowie Informationsweitergaben, was zur Vergrößerung der Cyber-Risiken führte. Da die Lieferketten ständig durch Cyber-Bedrohungen gefährdet sind, ist der Bedarf an Zero-Trust-Funktionen in allen Branchen groß.

Der Mythos von der überlegenen Apple-Sicherheitsumgebung: Dieser Mythos hält sich hartnäckig, obwohl macOS-Umgebungen nicht mehr als sicher gelten können, seitdem Bedrohungsakteure Golang-basierte Malware massenhaft einsetzen und mehr Angriffsvektoren für Attacken auf verschiedene Betriebssysteme nutzen.



Künstliche Intelligenz hat ihre Auftritt und verspricht tiefgreifende Veränderungen: Cyber-Abwehrmaßnahmen werden von verbesserten Machine Learning, Sprachverarbeitung und anderen Fortschritten gleichermaßen unterstützt und untergraben. Weltweit entwickeln sich Cyber-Bedrohungen so schnell und in einem so großen Ausmaß, sodass menschliche Teams nicht mithalten können. Deshalb sind Lösungen mit künstlicher Intelligenz für die Cyber-Abwehr von Unternehmen unverzichtbar.

Cyber-Sicherheit: Herausforderungen für CISOs und die SecOps-Revolution

Welche Herausforderung ist eine der größten für Cyber-Sicherheitsverantwortliche und SecOps-Teams? Die Erfassung der eingehenden Bedrohungsdaten – mit einem enormen Tempo und Umfang – und die sofortige Weiterleitung verwertbarer Erkenntnisse an die Teams, die im Unternehmen für die Bedrohungssuche und die Gewährleistung der Sicherheit verantwortlich sind.

Trellix hat sich das Ziel gesetzt, diesen Prozess zu vereinfachen.

Dazu stellen wir Automatisierung bereit, damit Ihre Teams die Antworten erhalten, die Sie zur Priorisierung benötigen. Außerdem bieten unsere Produkte für XDR, Host-, Netzwerk- und E-Mail-Schutz herausragende integrierte Funktionen zur Bedrohungsdatenanalyse, Bedrohungssuche und Sicherheitskontrolle.

Die Bedrohungen des 1. Quartals dieses Jahres wurden auch durch unternehmensinterne Faktoren bestimmt, die in vielen Fällen mit den kontinuierlichen Problemen der Cyber-Sicherheitsverantwortlichen und Frontline-Teams zusammenhängen.

Veraltete Technologien: Viele Unternehmen setzen weiterhin auf veraltete Technologien wie SOAR und SIEM. Dabei sind 96 % der CISOs der Meinung, dass sie bessere Lösungen benötigen, um ihre Umgebung vor Cyber-Bedrohungen zu schützen.[3]

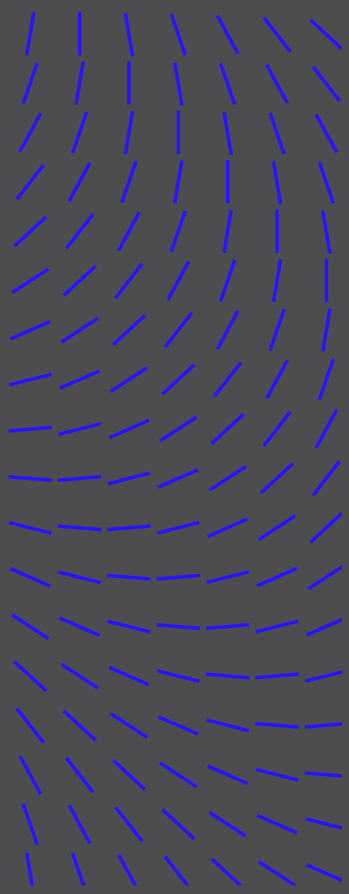
Zu viele Sicherheits-Tools: SecOps-Teams werden mit massenhaften Warnungen überhäuft und verfügen nicht über die notwendigen Hilfsmittel, um die richtigen Prioritäten zu setzen. Im Durchschnitt werden in Unternehmen 25 Sicherheitslösungen und Tools genutzt, was es erschwert, die Übersicht zu behalten.[4]

Überlastung durch zu viele Warnungen: Durch die Unmengen an Meldungen haben SecOps-Teams mit Schwierigkeiten durch falsche Prioritäten, False-Positives und übersehene Warnungen zu kämpfen. Laut IDC ignorieren 35 % der Sicherheitsverantwortlichen Warnungen – was zumindest zum Teil daran liegen könnte, dass es sich bei 45 % davon um False-Positives handelt.[5]

Unzureichende Ressourcen: Angesichts begrenzter SecOps-Ressourcen und fehlendem Know-how wird die Abwehr von Bedrohungen zu einem schwierigen Unterfangen. Die Berufserfahrung des durchschnittlichen SOC-Analysten ist eher begrenzt und beträgt etwa zwei Jahre.[6]

Methoden: So erfassen und analysieren wir Daten

Die erstklassigen Trellix-Experten unseres 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 anschließend 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.



Anwendung: Verwendung dieser Informationen

Jedes professionelle Analyseteam muss 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.

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.

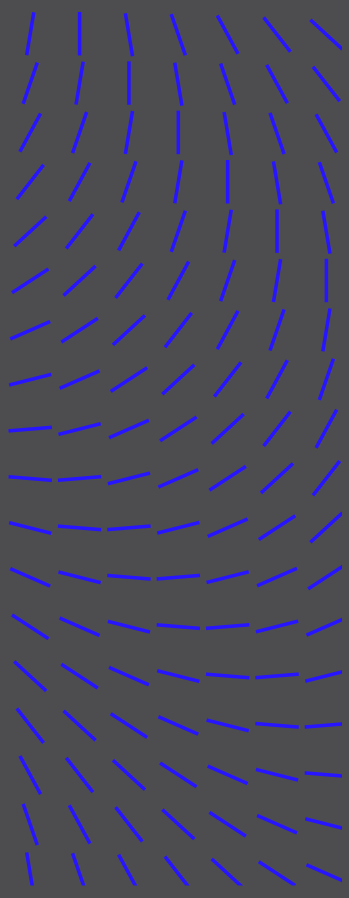
Für diesen Untersuchungsansatz stehen folgende Aspekte im Mittelpunkt:

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 bedeutet, dass eines unserer Produkte eine Datei, URL, IP-Adresse oder einen anderen Indikator erkannt und dies an uns gemeldet hat.

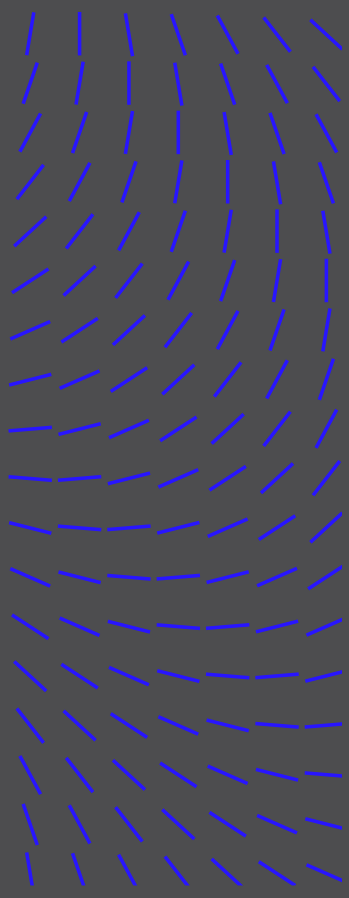
Uneinheitliche Datenerfassung: Einige Datensätze müssen sorgfältig interpretiert werden. So enthalten Telekommunikationsdaten zum Beispiel Telemetriedaten von ISP-Kunden, die in zahlreichen anderen Branchen und Sektoren tätig sind.



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.

DIE ZUKUNFT: Empfehlungen und Ressourcen

Welche Bedeutung haben die in diesem Bericht enthaltenen Informationen für Cyber-Sicherheitshelden an vorderster Front? Die Erkenntnisse und Cyber-Sicherheitsdaten sind nur dann nützlich, wenn sie auch in Maßnahmen umgewandelt werden, sodass Risiken reduziert, Entscheidungen optimiert und SecOps-Aktivitäten effizienter und kostengünstiger werden. Weitere Informationen und Ressourcen erhalten Sie unter www.trellix.com.



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

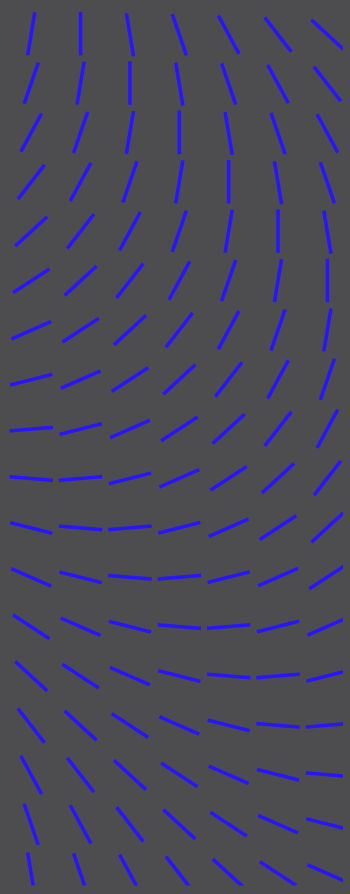
HIGHLIGHTS IM 1. QUARTAL 2023 AUF EINEN BLICK

Die Ransomware-Bedrohungslage

- **Die Ransomware-Welle:** Ransomware steht bei Cyber-Angriffen auf der ganzen Welt weiterhin an erster Stelle. Social-Engineering-Angriffe (z. B. Phishing) sollen die Angriffsopfer täuschen und dazu bringen, vertrauliche oder persönliche Informationen preiszugeben. Diese Angriffe werden nicht nur häufiger, sondern auch immer raffinierter.
- **Cuba und Play an erster Stelle:** Obwohl wir seit Anfang des Jahres bei Ransomware-Aktivitäten insgesamt einen Rückgang erleben, waren die am häufigsten vertretenen Familien im 1. Quartal Cuba (9 %) und Play (7 %).
- **LockBit lauert:** Trotz seit zwei Quartalen in Folge verminderter Aktivitäten ist LockBit weiterhin die aggressivste Ransomware, die ihre Opfer zur Zahlung der Lösegeldforderungen erpresst.
- **Magecart-Gruppe potenziell im Aufwind?** Medienberichte deuten darauf hin, dass diese auf Kreditkartendiebstahl und E-Commerce-Scalping spezialisierte Gruppe ihre Aktivitäten im 1. Quartal 2023 enorm ausgeweitet hat. Diese Akteure agieren normalerweise nicht im gleichen Umfang wie die anderen großen staatlichen APT-Akteure, was auf einen weltweiten Neuauftritt der Magecart-Gruppe hindeutet.

Ransomware-Taktiken entwickeln sich weiter

- **Finanzielle Ziele:** Es überrascht kaum, dass hinter Ransomware in erster Linie finanzielle Motive stehen. Die Versicherungsbranche (20 %) und der Finanzdienstleistungssektor (17 %) verzeichneten die meisten Erkennungen potenzieller Angriffe.
- **Mittlere Unternehmen am stärksten betroffen:** Eine Analyse unserer Leak-Website-Daten zeigt, dass die Opfer dieser Angriffe in erster Linie mittelgroße Unternehmen mit nur 51 bis 200 Mitarbeitern (32 %) sowie 10 Millionen bis 50 Millionen US-Dollar Umsatz (38 %) sind.
- **USA als Primärziel:** Die USA (15 %) waren das am häufigsten von Ransomware-Gruppen angegriffene Land. Gleichzeitig gab es hier auch die meisten Unternehmen (48 %), die nach einer erfolgreichen Attacke ihre Daten von den Angreifern „zurückkauften". Dieser Wert ist sechs Mal so hoch wie im nächsten Land auf der Liste, Großbritannien.
- **Cobalt Strike als Angriffsmittel der Wahl:** Laut Trellix-Telemetriedaten wird dieses Tool von Ransomware-Akteuren besonders häufig eingesetzt (28 % der Zwischenfälle). Obwohl der Anbieter Fortra Ende 2022 versucht hatte, die Verwendung für Bedrohungsakteure zu erschweren, scheint die Beliebtheit und Verbreitung von Cobalt Strike weiter zu wachsen.



Staatliche rote Flaggen

- **Führende Akteure:** In den letzten sechs Monaten waren APT-Akteure mit Verbindung zu China (darunter Mustang Panda und UNC4191) am aktivsten dabei, andere Staaten anzugreifen. Mit China in Verbindung stehende Bedrohungsakteure standen mit 79,3 % aller staatlichen Aktivitäten an erster Stelle, gefolgt von nordkoreanischen, russischen und iranischen Akteuren.
- **Aktivste APT-Gruppe:** Mustang Panda war auch das 3. Quartal in Folge die aktivste APT-Gruppe weltweit (72 %) – ein Hinweis auf Chinas ständige und zunehmende Cyber-Aktivitäten im Zusammenhang mit Spionage und Störmaßnahmen.

Schwachstellenanalyse

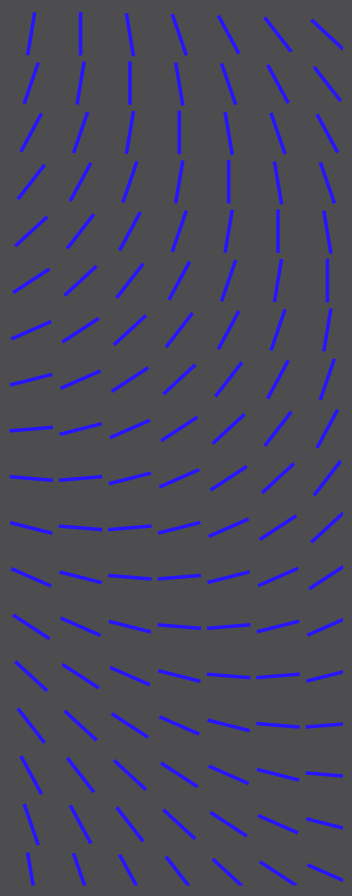
- **Fehlende Behebung bekannter Schwachstellen:** Bei den meisten kritischen Schwachstellen dieses Quartals handelt es sich um bereits bekannte Probleme, die jedoch aus verschiedenen Gründen noch nicht behoben wurden.
- **Schnee von gestern:** Eine im Februar dieses Jahres bekannt gewordene Apple-Schwachstelle ließ sich bis zum FORCEDENTRY-Exploit zurückverfolgen, der von der NSO-Gruppe für ihre Pegasus-Spyware verwendet wurde (veröffentlicht 2021).

E-Mail-Sicherheit

- **Neue Angriffswege:** Obwohl Microsoft angefangen hat, Makro-Anhänge in der Office-Plattform zu blockieren, haben Bedrohungsakteure schnell weitere Methoden für Angriffe auf Windows-Geräte gefunden, z. B. SEO Poisoning, OneNote und ZIP-Anhänge.
- **Verdächtige Marken:** Neben generischen Phishing-E-Mails missbrauchen kriminelle Akteure immer häufiger seriöse Markennamen und Services wie PayPal, Google, DWeb und IPFS, um Opfer zu betrügen und ihre Online-Anmeldedaten zu stehlen.

Unbefugter Zugriff auf die Cloud

- **Taktikwechsel:** Da immer mehr Unternehmen von lokaler Infrastruktur auf preisgünstigere und skalierbare Optionen von Amazon, Microsoft, Google und anderen Anbietern wechseln, nehmen Angriffe auf Cloud-Infrastrukturen zu.
- **Gültige Konten:** Obwohl raffinierte Angriffe mit Mehrfaktor-Authentifizierung, Proxys und API-Ausführung zunehmen, erfolgen die meisten Angriffe über gültige Konten – sie sind mindestens doppelt so häufig wie der zweithäufigste Angriffsvektor. Das ist ein deutlicher Hinweis auf das erhebliche Risiko unbefugter Zugriffe, da Cyber-Kriminelle die Anmeldedaten für legitime Konten oder Websites kompromittieren und verkaufen, um Angriffe durchzuführen.



ANALYSEN, EINBLICKE UND DATEN IN DIESEM BERICHT

Sicherheitszwischenfälle

Die in diesem Abschnitt vorgestellten Sicherheitszwischenfälle sind aus öffentlichen Berichten bekannt. Im 1. Quartal des Jahres 2023 setzten Angreifer auf der Suche nach leicht erreichbaren Einfallstoren auf Windows-Binärdateien, Drittanbieter-Tools, selbst entwickelte Malware und Penetrationstest-Tools für Angriffe. PowerShell und die Windows-Befehlszeile werden auch weiterhin gern zum Ausführen von Aufgaben genutzt, die Persistenz, Verankerung und Exfiltration ermöglichen.

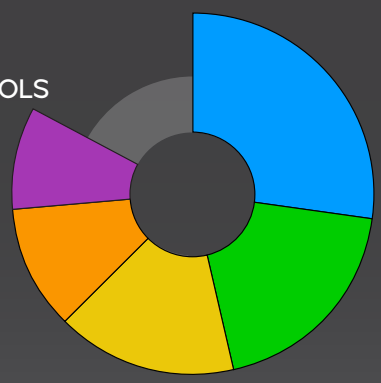
TOP 5 DER IM 1. QUARTAL 2023 BEI ZWISCHENFÄLLEN VERWENDETEN WINDOWS-BINÄRDATEIEN

1. PowerShell
2. Windows CMD
3. Geplanter Task
4. RunDLL32
5. WMIC

Schädliche DLL-Dateien sowie über die Windows-Verwaltungsinstrumentation ausgeführte Befehle runden die Top 5-Liste ab. Bedrohungsakteure nutzen für ihre Zwecke gern ungeschützte und unüberwachte Binärdateien, die bereits im System vorhanden sind und die Skripte ausführen oder Tastatureingaben akzeptieren.

In vielen Fällen sind Drittanbieter-Tools, Freeware und Penetrationstest-Tools fester Bestandteil eines Angriffszyklus und dienen Bedrohungsakteuren dazu, Persistenz zu erlangen, Skripte auszuführen, gesuchte Informationen zu entdecken und zu sammeln sowie Berechtigungen zu eskalieren, um Installationen mit erhöhten Berechtigungen auszuführen und auf Bereiche, Ressourcen oder Daten zuzugreifen, die nur berechtigten Konten zur Verfügung stehen.

TOP 5 DER IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTEN DRITTANBIETER-TOOLS

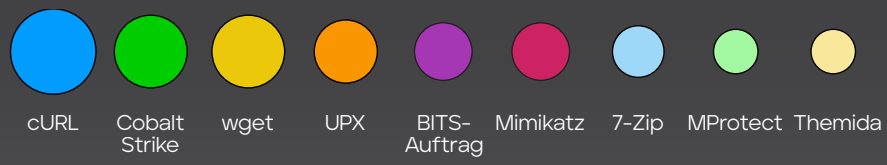


TOOL-KATEGORIEN

- Dateiübertragung
- Software-Packer
- Post-Exploitation-Tools
- Remote-Zugriffs-Tools
- Archivdienstprogramme

IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTE DRITTANBIETER-TOOLS

KONKRETE TOOLS



Gefährlichere Drittanbieter-Tools wie Cobalt Strike, Mimikatz und Sharphound können sowohl für legitime Zwecke als auch von Bedrohungsakteuren eingesetzt werden, um an Kennwörter zu gelangen, Beacons zu setzen oder Berechtigungen auszuweiten. Sobald ein Angreifer eine Umgebung kompromittieren konnte, kann er mit Dateiübertragungstools wie cURL auf extern gespeicherte Schaddaten zugreifen oder mit Rclone Daten in Cloud-Speicher exfiltrieren.

Im 1. Quartal 2023 waren die Magecart-Gruppe, APT29 und APT41 die drei aktivsten Bedrohungsgruppen und APTs, die Benutzer nach ihrem geografischen Standort und der Branche auswählten und versuchten, an Geld zu gelangen, Staatsgeheimnisse aufzudecken oder die Infrastruktur zu beschädigen. Eine Überraschung war für uns, dass die Magecart-Gruppe bereits auf dem ersten Listenplatz stand, obwohl sie nur selten im gleichen Umfang agiert wie die anderen staatlichen APTs. Wir werden die Aktivitäten der Gruppe auch in den kommenden Monate im Auge behalten und herausfinden, ob die aktuellen Daten einen weltweiten Neuauftritt der Gruppe einleiten.

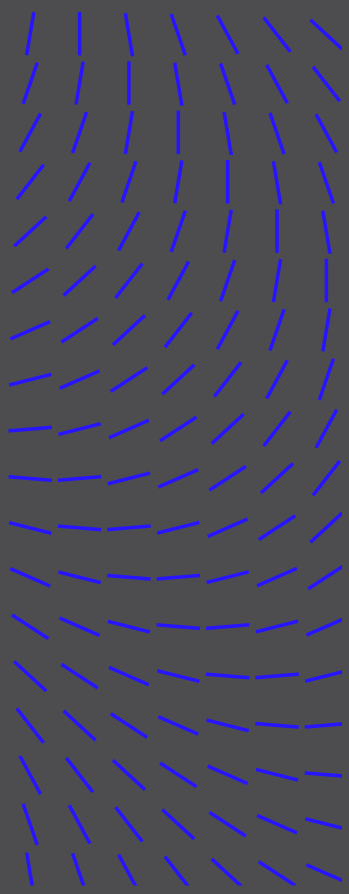
Frühere weltweite Kampagnen setzten auf weniger komplexe breitgefächerte Techniken, um alle Benutzer zu erreichen, die auf gefährliche Links klicken oder Schadinhalte herunterladen könnten. Gezielte Angriffe werden immer raffinierter und erreichen zunehmend bessere Persistenz in der Fertigungsbranche, im Finanzsektor sowie im Gesundheitswesen. Die beiden übrigen Sektoren – Telekommunikation und Energieversorgung – waren zwar seltener von weltweiten Kampagnen betroffen, sind aber beide gleichermaßen wichtig. Außerdem besteht die Möglichkeit, dass die darin vertretenen Unternehmen möglicherweise nur keine Kompromittierungen gemeldet oder sie überhaupt nicht gemerkt haben.

TOP 8 DER IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTEN AKTIVEN BEDROHUNGSAKTEURE

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

TOP 5 DER IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTEN ANGEGRIFFENEN SEKTOREN

1.	Fertigungs-unternehmen	8 %
2.	Finanzsektor	7 %
3.	Gesundheitswesen	6 %
4.	Telekommunikation	5 %
5.	Energieversorgung	5 %



Gemeldete Zwischenfälle, die von unserem Forscherteam analysiert und bestätigt wurden, umfassen eine Vielzahl von Informationen, Korrelationen oder Attributionen zu einem konkreten Bedrohungsakteur, einer Bedrohungsgruppe oder einem raffinierteren APT-Akteur. Die Tools, Techniken und Prozeduren sowie die verwendeten Malware-Familien umfassen Loader- und Downloader-Malware, Remote-Zugriff-Trojaner (RATs), Programme zum Diebstahl von Informationen sowie Ransomware. Anhand der Ereignisse aus dem 1. Quartal 2023, die wir per Insights analysiert und bereitgestellt haben, konnten wir die Ukraine als häufigstes Angriffsziel identifizieren, wobei die USA dicht auf dem zweiten Platz folgten.

Die Ransomware-Familien The Royal Ransom, Trigona und Maui waren im 1. Quartal 2023 am häufigsten vertreten. Trellix hat vor Kurzem eine detaillierte Analyse von Royal Ransom und der Funktionsweise der ausführbaren Dateien unter Windows und Linux veröffentlicht. Obwohl die Daten zu den hier präsentierten Statistiken explizit von unserer Insights-Plattform stammen, sind viele weitere Ereignisse in der weltweit vernetzten Infrastruktur aufgetreten. Dazu gehören auch bekannte Ereignisse, die veröffentlicht oder unter Verschluss gehalten wurden, sowie Zwischenfälle, die noch nicht identifiziert bzw. behoben wurden.

TOP 5 DER IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTEN ANGEGRIFFENEN LÄNDER

7 % 

Aus den öffentlich gewordenen Ereignissen, die wir analysieren konnten, ergab sich die Ukraine als am häufigsten von Bedrohungsakteuren angegriffenes Land, dicht gefolgt von den USA.

1.	Ukraine	7 %
2.	USA	7 %
3.	Deutschland	4 %
4.	Südkorea	3 %
5.	Indien	3 %

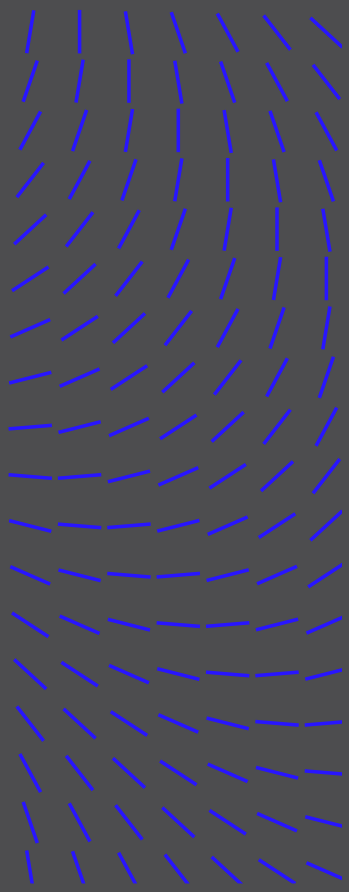
Ransomware

Die unten gezeigten Statistiken beziehen sich auf die Kampagnen, nicht auf die Erkennungen selbst. Unsere globalen Telemetriedaten haben Kompromittierungsindikatoren (IOCs) aufgezeigt, die zu verschiedenen Kampagnen von verschiedenen Ransomware-Gruppen gehören.

TOP 5 DER IN ÖFFENTLICHEN BERICHTEN IM 1. QUARTAL 2023 GENANNTEN RANSOMWARE-FAMILIEN

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

Relativ häufig verzeichnen wir zu Beginn eines Jahres, insbesondere im Januar, einen Rückgang bei Cybercrime-Aktivitäten. Dieser Trend könnte den Rückgang der Aktivitäten von Hive und Cuba erklären. Außerdem dürfte die Stilllegung des Hive-Netzwerks durch das FBI und Europol Ende Januar die Aktivitäten dieser Gruppe erheblich beeinträchtigt haben. Die LockBit-Familie ist weiterhin eine erhebliche Größe im Ransomware-Sektor und hat sich sehr erfolgreich darauf spezialisiert, die Opfer aggressiv zur Zahlung von Lösegeldern zu zwingen.



TOP 5 DER IM 1. QUARTAL 2023 BEI ZWISCHENFÄLLEN VERWENDETEN RANSOMWARE-FAMILIEN

8 %

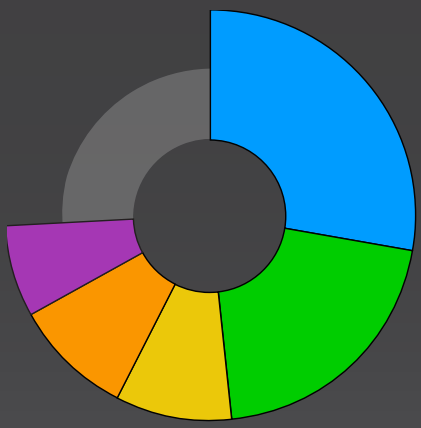
Cuba war die aktivste Ransomware-Gruppe, dicht gefolgt von Play und LockBit.

- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

IM 1. QUARTAL 2023 VERWENDETE RANSOMWARE-TOOLS

28 %

Cobalt Strike kam in diesem Quartal bei fast einem Drittel aller Ransomware-Zwischenfälle zum Einsatz. Trotz Bemühungen des Herstellers, Bedrohungsakteuren den Missbrauch des Tools zu erschweren, wuchs der Anteil sogar noch.



- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC

AM STÄRKSTEN VON RANSOMWARE-GRUPPEN BETROFFENE LÄNDER, 1. QUARTAL 2023

15 %

Die USA sind in diesem Quartal auch weiterhin das am stärksten von Ransomware-Aktivitäten betroffene Land, dicht gefolgt von der Türkei.

1.	USA	15 %
2.	Türkei	14 %
3.	Portugal	10 %
4.	Indien	9 %
5.	Kanada	9 %

AM STÄRKSTEN VON RANSOMWARE-GRUPPEN BETROFFENE BRANCHEN, 1. QUARTAL 2023

1.	Versicherungswesen	20 %
2.	Finanzdienstleistungen	17 %
3.	Pharmaindustrie	7 %
4.	Telekommunikation	4 %
5.	Outsourcing und Hosting	4 %

Ransomware-Gruppen erpressen ihre Opfer, indem sie deren Informationen auf so genannten „Leak-Websites" veröffentlichen, um festgefahrene Verhandlungen in Schwung zu bringen oder auf Zahlungsverweigerung zu reagieren. Unsere Trellix-Experten nutzen das Open-Source-Tool RansomLook, um Daten aus den Beiträgen zu erfassen und die Ergebnisse anschließend zu normalisieren und zu ergänzen, sodass eine anonymisierte Opferanalyse möglich wird.

Dabei muss beachtet werden, dass nicht alle Ransomware-Opfer auf den jeweiligen Leak-Websites erscheinen. Viele Opfer zahlen das Lösegeld und werden nicht erwähnt. Die Zahlen unten sind ein Gradmesser für die Opfer, die von Ransomware-Gruppen erpresst oder bestraft wurden, und sollten nicht mit der Gesamtzahl der Opfer gleichgesetzt werden.

RANSOMWARE-GRUPPEN MIT DEN MEISTEN IN LEAK-WEBSITES GEMELDETEN OPFERN, 1. QUARTAL 2023

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

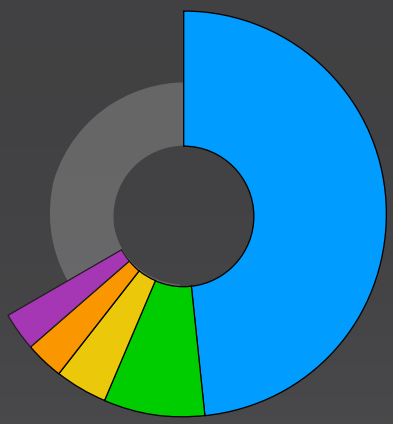
LAUT LEAK-WEBSITES VON RANSOMWARE-GRUPPEN AM STÄRKSTEN BETROFFENE BRANCHEN, 1. QUARTAL 2023

1.	Industriegüter und -dienstleistungen	25 %
2.	Einzelhandel	14 %
3.	Technologie	11 %
4.	Gesundheitswesen	8 %
5.	Finanzdienstleistungen	6 %

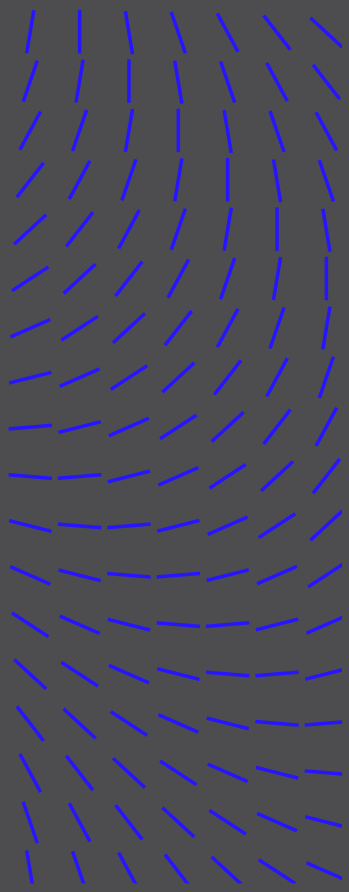
TOP 5 DER LÄNDER MIT UNTERNEHMEN, DIE IM 1. QUARTAL 2023 AUF LEAK-WEBSITES GELISTET WURDEN

48 %

der betroffenen Unternehmen, die auf Leak-Websites von Ransomware-Gruppen gelistet wurden, haben ihren Sitz in den USA.



- USA
- Großbritannien
- Deutschland
- Kanada
- Indien



GRÖSSE DER UNTERNEHMEN, DIE IM 1. QUARTAL 2023 AUF LEAK-WEBSITES GELISTET WURDEN

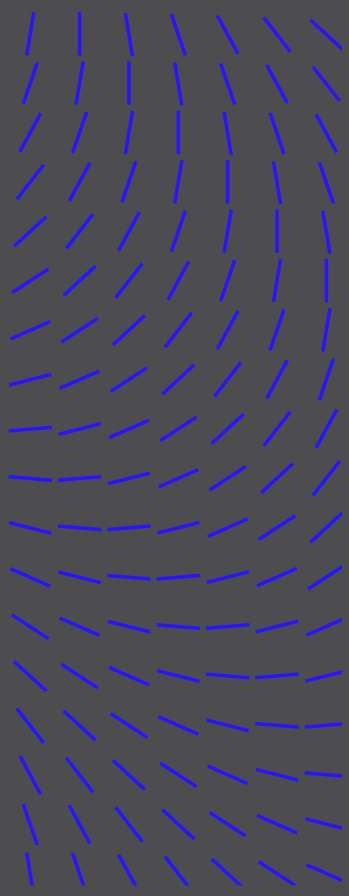
MITARBEITERZAHL		JAHRESUMSATZ	
1.	51–200	32 %	1. 10 Mio.–50 Mio. USD	38 %
2.	1.001–5.000	22 %	2. 1 Mrd.–10 Mrd. USD	23 %
3.	11–50	15 %	3. 1 Mio.–10 Mio. USD	21 %
4.	201–500	15 %	4. 100 Mio.–250 Mio. USD	11 %
5.	501–1.000	15 %	5. 500 Mio.–1 Mrd. USD	7 %

Aktivitäten staatlicher Akteure

Die Erkenntnisse zu den Aktivitäten staatlicher Akteure wurden aus mehreren Quellen zusammengetragen, um ein besseres Bild der Bedrohungslandschaft zu gewinnen und Beobachtungsfehler zu verringern. Zunächst präsentieren wir die Statistik, die aus der Korrelation der Kompromittierungsindikatoren für staatliche Akteure und den Telemetriedaten von Trellix-Kunden gewonnen wurden. Danach folgen die Erkenntnisse aus verschiedenen Berichten, die von der Sicherheitsbranche veröffentlicht und von der Threat Intelligence-Gruppe gründlich überprüft und analysiert wurden.

Wie bereits erwähnt, beziehen sich diese Statistiken auf die Kampagnen, nicht auf die Erkennungen selbst. Aufgrund zahlreicher Protokollverdichtungen, des Einsatzes von Bedrohungssimulationen durch unsere Kunden und allgemeiner Korrelationen mit der Knowledge Base für Bedrohungsdaten werden die Daten manuell gefiltert, um unsere Analyseziele zu erfüllen.

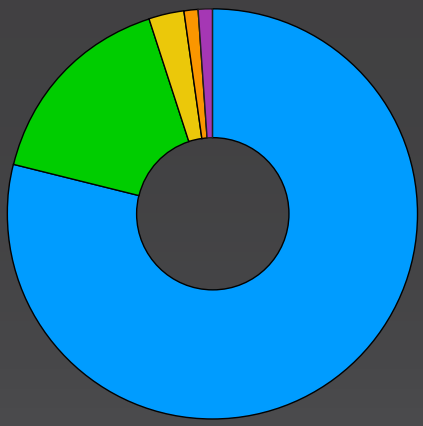
Wir beobachten, dass mit China in Verbindung stehende Bedrohungsakteure die weltweite Bedrohungslandschaft dominieren, wobei die meisten Erkennungen im 1. Quartal 2023 auf Mustang Panda zurückgehen. Da die chinesischen APT-Gruppen in erster Linie auf Sideloading und andere Tarntechniken setzen, werden sie ihre Malware-Tools vermutlich weniger häufig wechseln als andere Bedrohungsakteure. Das könnte zu höheren Erkennungszahlen führen, die auf eine weit verbreitete Nutzung eines Tools hindeuten, obwohl es nur sehr stark von chinesischen Gruppen eingesetzt wird.



LÄNDER MIT DEN MEISTEN AKTIVITÄTEN STAATLICHER AKTEURE, 1. QUARTAL 2023

79 %

Auf China entfiel im 1. Quartal 2023 der Großteil aller staatlichen Aktivitäten.



AKTIVSTE GRUPPEN VON BEDROHUNGSAKTEUREN, 1. QUARTAL 2023

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

BEI AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE MITRE ATT&CK-TECHNIKEN, 1. QUARTAL 2023

1.	LDLL-Side-Loading	14 %
2.	Entschleierung/Dekodierung von Dateien oder Informationen	11 %
3.	Eintrittstool-Übertragung	10 %
4.	Daten vom lokalen System	10 %
5.	Erkennung von Dateien und Verzeichnissen	10 %

BEI AKTIVITÄTEN STAATLICHER AKTEURE AM HÄUFIGSTEN GENUTZTE BÖSWILLIGE TOOLS, 1. QUARTAL 2023

38 %

Auf PlugX entfielen im 1. Quartal 2023 insgesamt 38 % aller böswilligen staatlichen Aktivitäten.

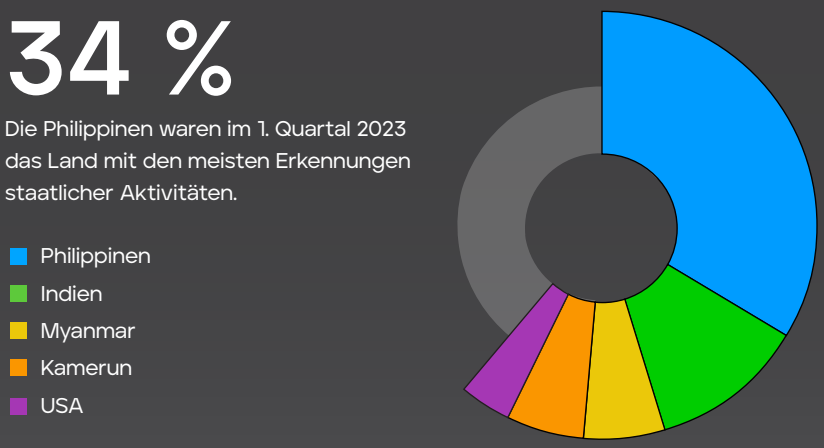
1.	PlugX	38 %
2.	Cobalt Strike	35 %
3.	Raspberry Robin	14 %
4.	BLUEHAZE/DARKDEW MISTCLOAK	3 %
5.	Mimikatz	3 %

Indien ist eines der führenden Länder Asiens, das in der Lage ist, starke Cyber-Programme aufzubauen. Einige Gruppen, insbesondere mit China verbundene Bedrohungsakteure, haben großes Interesse an indischen Entwicklungen in den Bereichen Technologie, Militär und Politik gezeigt. Eine signifikante Zahl von Erkennungen in Indien kann Mustang Panda zugeschrieben werden.

LÄNDER MIT DEN MEISTEN ERKENNUNGEN STAATLICHER AKTIVITÄTEN, 1. QUARTAL 2023

34 %

Die Philippinen waren im 1. Quartal 2023 das Land mit den meisten Erkennungen staatlicher Aktivitäten.



BRANCHEN MIT DEN MEISTEN ERKENNUNGEN STAATLICHER AKTIVITÄTEN, 1. QUARTAL 2023

Schwachstellenanalyse

Experten für Reverse Engineering und Schwachstellenanalysen aus dem Trellix Advanced Research Center beobachten ständig die neuesten Schwachstellen, um Kunden darüber informieren zu können, wie diese Schwachstellen von Bedrohungsakteuren missbraucht werden und wie sich die Wahrscheinlichkeit und der Schweregrad dieser Angriffe minimieren lässt.

Wenig überraschend zeigte sich im 1. Quartal 2023, dass zu den schwerwiegendsten Schwachstellen die Umgehung von Patches für ältere CVEs, Lieferkettenfehler durch die Nutzung veralteter Bibliotheken oder seit langem gepatchte Schwachstellen gehören.

Ein Beispiel ist CVE-2022-47966, eine kritische (9,8) Schwachstelle in Zoho ManageEngine-Produkten, die in diesem Januar die Runde machte. ManageEngine wird von tausenden Unternehmen auf der ganzen Welt genutzt, sodass wir nicht überrascht waren, als die aktive Ausnutzung dieser Schwachstelle entdeckt wurde. Interessant fanden wir etwas anderes: Die Schwachstelle ging auf die Nutzung von Apache Santuario 1.4.1 zurück, eine fast 18 Jahre alte fehlerhafte Version, die XML-Injektionsangriffe ermöglichte. Im Oktober patchte Zoho die Schwachstelle in seiner Produkt-Suite, und fast drei Monate später (im 1. Quartal) veröffentlichte CISA eine Warnung über die aktive Ausnutzung und die dringende Patch-Empfehlung für Unternehmen.

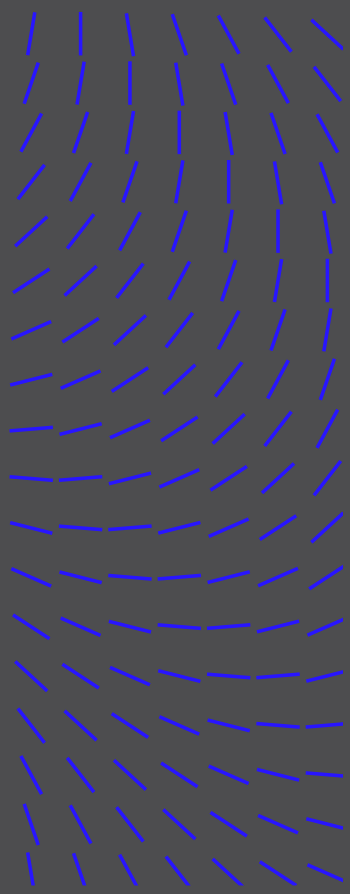
Ein weiteres Beispiel ist CVE-2022-44877, eine kritische Schwachstelle in Control Web Panel (CWP). Obwohl diese Schwachstelle nicht direkt mit unserem vorhergehenden Beispiel zusammenhängt, hat sie viel damit gemeinsam: Es handelt sich erneut um eine kritische (9,8) Remote-Code-Ausführung (RCE), die im Januar vielfach ausgenutzt wurde, obwohl seit Oktober ein Patch zur Verfügung stand. Die Ursache war ebenfalls nicht sonderlich raffiniert: Befehlsinjektion mit einer gewöhnlichen Shell-Variablenerweiterung in einem URL-Parameter.

Ein drittes Beispiel ist CVE-2021-21974, eine Schwachstelle im VMware ESXi-Dienst OpenSLP, die bereits im Februar 2021 geschlossen wurde – fast genau zwei Jahre vor dem plötzlichen Wiederauftauchen aufgrund einer aktiven Ausnutzung. Als wir in unserem Bug-Report vom Februar von dieser Schwachstelle berichteten, fanden wir mit Shodan etwa 48.000 aus dem Internet erreichbare Server, die immer noch anfällige ESXi-Versionen ausführten. Aktuell liegt diese Zahl immer noch bei mehr als 38.000 – das sind gerade einmal 22 % weniger.

Datum	Anzahl anfälliger ESXi-Server laut Shodan
Ende Februar 2023	48.471
Ende April 2023	38.047

Wir fanden selbst einige Fälle, als wir Anfang des Jahres Apple-Geräte untersuchten: CVE-2023-23530 und CVE-2023-23531. Diese beiden Schwachstellen unterscheiden sich von den zwei vorhergehenden Beispielen, da ihre Auswirkung auf eine lokale Erhöhung von Berechtigungen beschränkt ist und keine RCE darstellt. Das ist jedoch kein Grund, sie nicht ernst zu nehmen, da eine sehr ähnliche Schwachstelle beim FORCEDENTRY-Exploit ausgenutzt wurde, mit dem die NSO-Gruppe im Jahr 2021 ihre Pegasus-Spyware in den Systemen verankerte. Tatsächlich nutzen die beiden von uns entdeckten CVEs die gleiche Primitive, die als Grundlage für den FORCEDENTRY-Exploit diente: die harmlose Klasse NSPredicate. Der Ansatz von Apple zum Schließen der FORCEDENTRY-Lücke bestand jedoch lediglich darin, eine umfangreiche Blockierungsliste anzulegen, um Ausnutzungsmöglichkeiten für NSPredicate zu minimieren. Das zugrunde liegende Problem wurde damit nicht behoben.

Es wäre zu einfach, auf solche Trends zu verweisen und zu schlussfolgern, dass Anbieter die Sicherheit nicht ernst nehmen, oder das Recycling alter Exploits durch Bedrohungsakteure und Forscher beklagen. Aber das wäre falsch. Schwachstellenforscher analysieren verschiedene Varianten, weil das eine effektive Möglichkeit ist, die Prioritäten echter Bedrohungsakteure nachzuvollziehen. Das Aufdecken einer Umgehungsmöglichkeit für Fehlerbehebungen oder eine alte CVE in einem selten gepatchten Produkt bietet fast immer eine bessere Rendite, als das Rad neu zu erfinden. Unternehmen, die das verstehen, sollten daraus folgende Schlussfolgerung ziehen: Auch wenn hochmoderne Technologien zur Bedrohungserkennung in der heutigen Zeit unverzichtbar sind, haben grundlegende Prinzipien wie Patch-Prozesse und Lieferkettenüberprüfungen längst nicht ausgedient.



E-Mail-Sicherheit

Die Statistiken zur E-Mail-Sicherheit basieren auf Telemetriedaten, die aus verschiedenen, bei Kunden in aller Welt installierten E-Mail-Sicherheits-Appliances generiert wurden.

Phishing-Angriffe, die seriöse Marken imitieren und Benutzer dazu verleiten, ihre Anmeldeinformationen weiterzugeben, sind gerade im Aufschwung. Dabei setzen solche E-Mail-Angriffe verstärkt auf DWeb, IPFS und Google Übersetzer. Angreifer nutzten auch Freemail- und vergleichbare Dienste wie PayPal-Rechnungen und Google Formulare, um Vishing-Attacken durchzuführen und eine Erkennung zu vermeiden. Auf ähnliche Weise wurden in diesem Zeitraum auch neue Marken wie Scribd und LesMills, aber auch Google Play-Geschenkkarten ausgenutzt.

Bei der im 1. Quartal 2023 eingesetzten Malware, die für diese Angriffe eingesetzt wurde, legten im Vergleich zum letzten Jahr vor allem Formbook und Agent Tesla zu. Ein Grund dafür könnte sein, dass sich beide Malware-Familien im Gegensatz zu Remcos, Emotet und Qakbot leicht beschaffen und einsetzen lassen.

AM HÄUFIGSTEN IN E-MAILS GENUTZTE MALWARE-TAKTIKEN, 1. QUARTAL 2023

44 %

Formbook machte im 1. Quartal 2023 fast die Hälfte aller E-Mail-Malware aus, dicht gefolgt von Agent Tesla.

AM HÄUFIGSTEN MIT PHISHING-E-MAILS ANGEGRIFFENE LÄNDER, 1. QUARTAL 2023

30 %

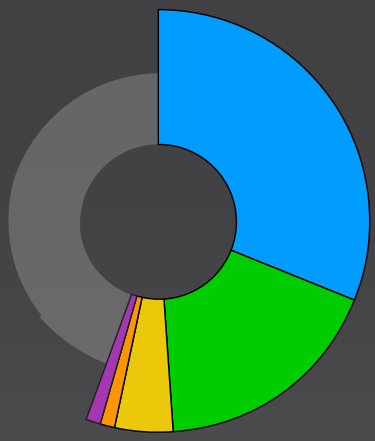
Die USA und Südkorea waren im 1. Quartal 2023 am häufigsten Ziele von E-Mail-Phishing-Versuchen – auf sie entfielen fast zwei Drittel aller weltweiten Phishing-Angriffe.

1.	USA	30 %
2.	Südkorea	29 %
3.	Taiwan	10 %
4.	Brasilien	8 %
5.	Japan	7 %

AM HÄUFIGSTEN MIT PHISHING-E-MAILS ANGEGRIFFENE PRODUKTE UND MARKEN, 1. QUARTAL 2023

38 %

Obwohl hunderte Marken angegriffen wurden, machten Microsoft-Produkte im 1. Quartal 2023 bei weitem den Löwenteil aus.



- Microsoft
- Google-Captcha
- Outlook
- GCash
- USPS

AM HÄUFIGSTEN VON BÖSWILLIGEN E-MAILS BETROFFENE BRANCHEN, 1. QUARTAL 2023

1.	Behörden	11 %
2.	Finanzdienst-leistungen	8 %
3.	Fertigungs-unternehmen	6 %
4.	Technologie	6 %
5.	Unterhaltung	5 %

STARK MISSBRAUCHTE WEB-HOSTING-ANBIETER, 1. QUARTAL 2023

1.	IPFS	41 %
2.	Google Übersetzer	33 %
3.	Dweb	16 %
4.	Amazon AWS Appforest	3 %
5.	Firebase OWA	3 %

BEI PHISHING-ANGRIFFEN AM HÄUFIGSTEN GENUTZTE UMGEHUNGSTECHNIKEN, 1. QUARTAL 2023

79 % Umgehungen mit 302-Weiterleitungen wurden im 1. Quartal 2023 am häufigsten bei Phishing-Angriffen eingesetzt.

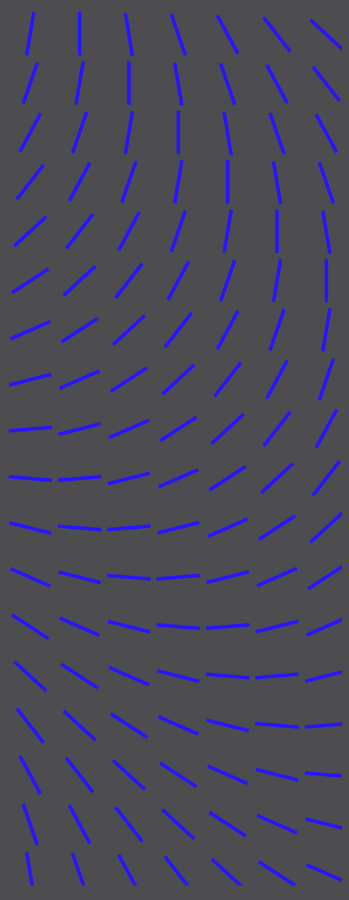
46 % Captcha-basierte Angriffe nahmen im 1. Quartal 2023 gegenüber dem 4. Quartal 2022 erheblich zu.

Netzwerksicherheit

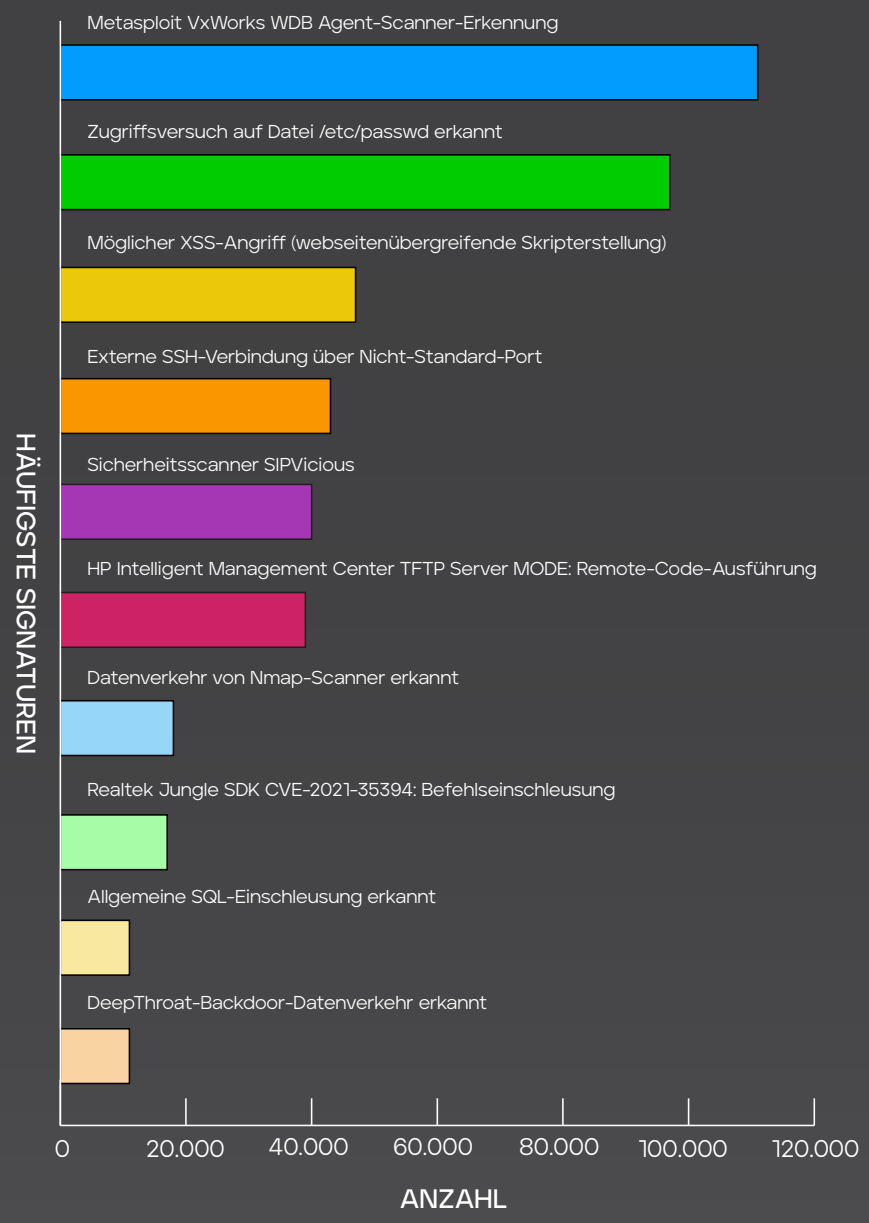
Im Zuge der Erkennung und Blockierung von Netzwerkangriffen auf unsere Kunden untersuchen die Forscher des Trellix Advanced Research Center-Teams unterschiedliche Bereiche der Angriffskette – von der Erkundung und Erstkompromittierung bis zur C&C-Kommunikation (Command-and-Control) und TTPs für laterale Bewegungen.

WICHTIGSTE MALWARE-CALLBACK-TRENDS IM 1. QUARTAL 2023

Rückgang bei STOP-Ransomware-Aktivitäten	94 %
Zunahme bei LockBit-Ransomware, die von Amadey verteilt wird	25 %
Steigerung bei Android-Malware-Aktivitäten	12,5 %
Steigerung bei Ursnif-Aktivitäten	10 %
Steigerung bei Smoke Loader-Aktivitäten	700 %
Steigerung bei Amadey-Aktivitäten	400 %
Steigerung bei Cobalt Strike-Aktivitäten	300 %
Steigerung bei Emotet-Aktivitäten	200 %



SCHWERWIEGENDSTE ANGRIFFE AUF ÖFFENTLICH ZUGÄNGLICHE DIENSTE, 1. QUARTAL 2023



Cloud-Zwischenfälle

Cloud-Infrastruktur-Angriffe auf Dienste von Amazon, Microsoft, Google und andere nehmen weiter zu. Die Tabelle unten bietet eine kurze Beschreibung der Cloud-basierten Telemetriedaten, aufgeschlüsselt nach Kunde und Cloud-Anbieter.

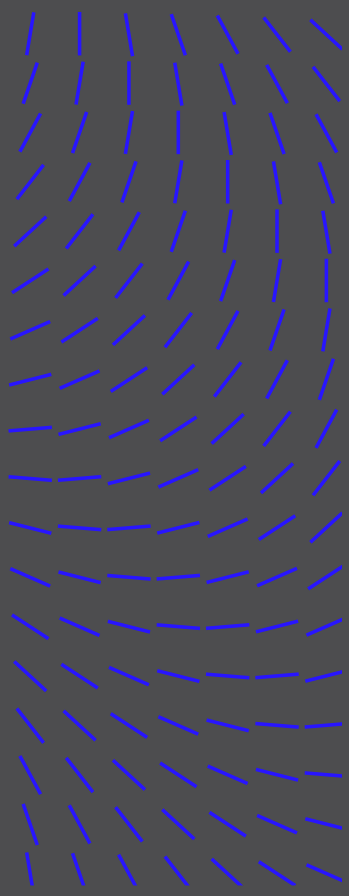
ERKENNUNGEN NACH MITRE ATT&CK-TECHNIKEN, 1. QUARTAL 2023

	AWS	Microsoft Azure	GCP
Gültige Konten	3.437	4.312	997
Änderung der Datenverarbeitungsinfrastruktur des Cloud-Kontos	4.268	0	17
Nicht-Standard-Port	115	0	17
Mehrfaktor-Authentifizierung	190	1.534	22
Netzwerkdienst-erkennung	141	93	0
Brute-Force-Angriff	25	1.869	22
Proxy	299	2.744	135
Konto-erkennung	264	68	787
E-Mail-Weiterleitungs-regel	25	0	22
Ausführung über API	1.143	0	252

METHODEN

Erfassung: Trellix und unsere 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-Sicherheitsnetzwerken 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 Angriffsmethoden, 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 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.

RESSOURCEN

Threats-Report-Archive

The Mind of the CISO

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

A Royal Analysis of Royal Ransom

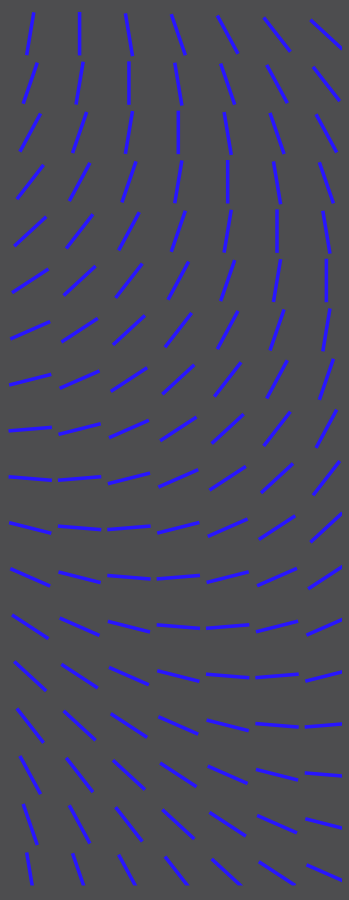
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

Threats-Report-Archive ansehen

Trellix Advanced Research Center

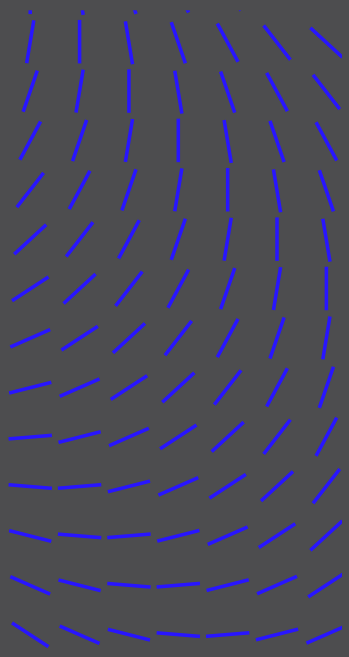


ÜBER DAS TRELLIX ADVANCED RESEARCH CENTER

Das Trellix Advanced Research Center hat die umfassendste Richtlinie der Cyber-Sicherheitsbranche und ist Vorreiter bei neuen Methoden, Trends und Akteuren der weltweiten Bedrohungslandschaft. Als führender Partner von Sicherheitsteams in aller Welt liefert das Trellix Advanced Research Center Informationen und neueste Inhalte für Sicherheitsanalysten und stärkt gleichzeitig unsere führende XDR-Plattform. Außerdem bietet die Threat Intelligence-Gruppe des Trellix Advanced Research Center unseren weltweiten Kunden Bedrohungsdaten-Produkte und -Services an.

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 förderte Trellix die technologische Innovationsfähigkeit durch Machine Learning und Automatisierung, um über 40.000 Geschäfts- und Behördenkunden durch Living Security zu stärken.



Weitere Informationen finden Sie unter Trellix.com.

Trellix

Über Trellix

Trellix ist ein globales Unternehmen, das die Zukunft der Cyber-Sicherheit 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 fördern die Sicherheitsexperten von Trellix die technologische Innovationsfähigkeit durch Machine Learning und Automatisierung, um über 40.000 Geschäfts- und Behördenkunden zu stärken.

072022-05