Acronis

Report (2. Halbjahr 2024)

Zusammen-fassung

Acronis Cyberthreats Report (2. Halbjahr 2024): KI-gestützte Bedrohungen auf dem Vormarsch

Acronis Threat Research Unit

Autor:innen:

Alexander Ivanyuk
Senior Director, Technology

Irina Artioli
Cyber Protection Evangelist, Acronis Threat Research Unit

Robert Neumann
Leiter der Acronis Threat Research Unit

Einführung und Zusammenfassung

Der halbjährliche Acronis Cyberthreats Report berichtet über die globale Bedrohungslage, wie sie von der Acronis Threat Research Unit (TRU) und den Acronis Sensoren im 2. Halbjahr 2024 erfasst wurde. Die allgemeinen Malware-Daten in diesem Bericht wurden von Juli bis Dezember 2024 erhoben und spiegeln von uns beobachtete Bedrohungen, die in diesem Zeitraum auf Endpunkte abzielten.

Der Bericht basiert auf mehr als 1.000.000 individuellen Endpunkten, die auf der ganzen Welt verteilt sind, und enthält Statistiken mit Bedrohungen für Windows-Betriebssysteme, da diese weitaus verbreiteter sind als macOS- und Linux-Bedrohungen.

- Die Vereinigten Arabischen Emirate, Singapur und Italien waren die Länder, die im Dezember 2024 am häufigsten Ziel von Malware-Angriffen waren.
- Im 4. Quartal 2024 hat Acronis mehr als 48 Mio. URLs auf Endpunkten blockiert, was einem Anstieg von 7 % gegenüber dem 3. Quartal 2024 entspricht.
- 31,4 % aller im 2. Halbjahr 2024 empfangenen E-Mails waren Spam. Davon enthielten 1,4 % Malware oder Phishing-Links.
- Im Dezember 2024 wurde der höchste Anteil an blockierten schädlichen URLs am Endpunkt in den Vereinigten Arabischen Emiraten verzeichnet (16,2 %), gefolgt von Brasilien (13,2 %) und Singapur (12 %).
- 1.712 Fälle von Ransomware wurden im 4. Quartal 2024 bekannt. RansomHub, Akira, Play und KillSec gehörten mit insgesamt 580 Opfern zu den Hauptverantwortlichen. Die Ransomware-Bande Cl0p war im Dezember mit 68 Opfern besonders aktiv.

Cybersicherheitstrends – von Juli bis Dezember 2024:

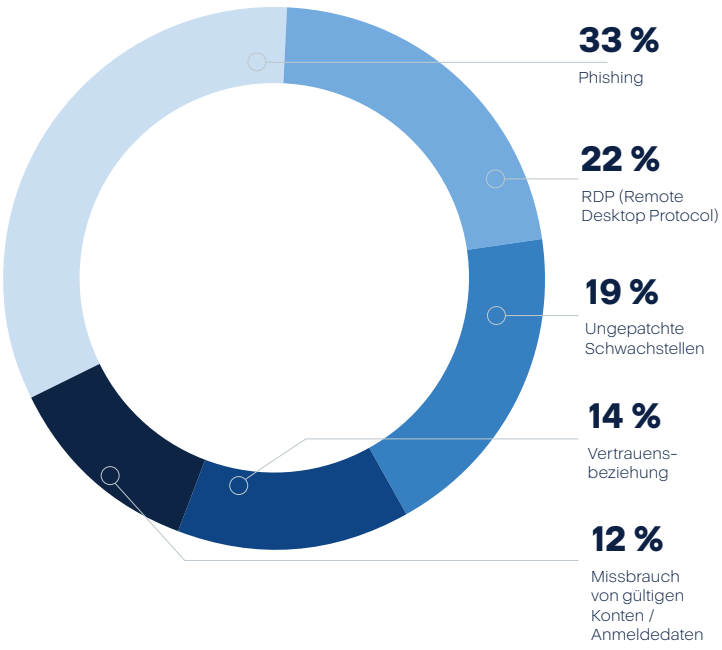
- 2024 richteten sich Ransomware-Angriffe zunehmend gegen kritische Branchen wie Transport, Gesundheitswesen und Fertigung. Die Cyberkriminellen setzten dabei personalisierte Taktiken und KI-basierte Strategien ein, um Schwachstellen auszunutzen und höhere Lösegelder zu fordern. Dieser Trend spiegelt eine Verlagerung hin zu ausgefeilteren, groß angelegten Angriffen wider, die auf maximale Störung und finanziellen Gewinn abzielen. Das unterstreicht die entscheidende Rolle, die MSPs beim Schutz von Unternehmen mit erweiterten Sicherheitsmaßnahmen und Strategien zur Reaktion auf Zwischenfälle spielen.
- Datenschutzverletzungen sind nach wie vor ein großes Problem, das Unternehmen weltweit enormen Schaden zufügt.
- ChatGPT und ähnliche generative KI-Systeme werden zunehmend eingesetzt, um Cyberangriffe zu verüben, bösartige Inhalte zu erstellen und Angriffe zu automatisieren.
- Die Anzahl der im 2. Halbjahr 2024 entdeckten Angriffe per E-Mail stieg im Vergleich zum 2. Halbjahr 2023 um 197 %, während die Zahl der angegriffenen Unternehmen im gleichen Zeitraum um 21 % zunahm.

Wichtigste Cyber-bedrohungen und Trends im 2. Halbjahr 2024

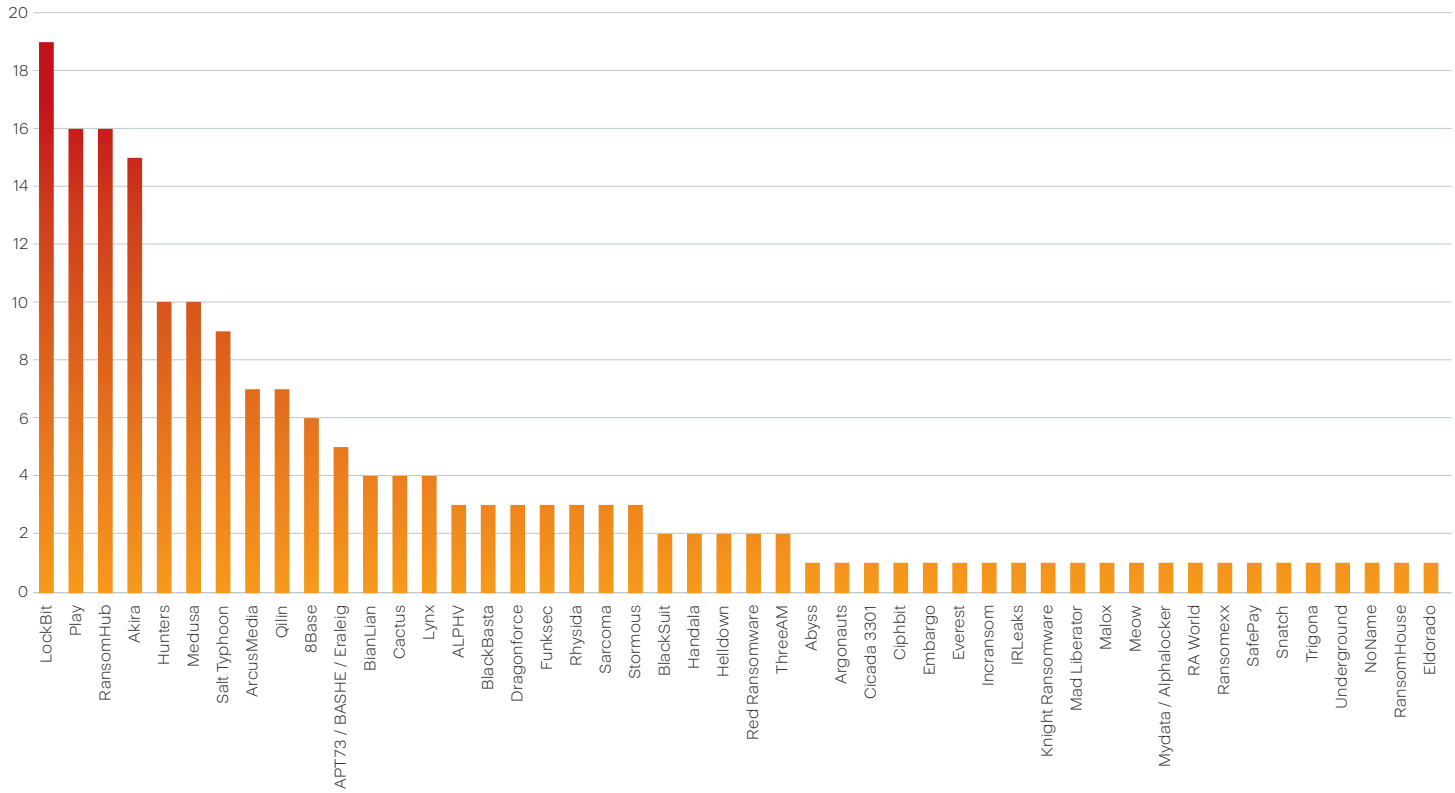
Ransomware in 2024: Anstieg um 5 % und APT-Ransomware-Gruppen nehmen MSPs ins Visier

Wir haben die Angriffe auf Managed Service Provider (MSPs) weiter beobachtet und die Datenanalyse auf den Zeitraum Januar bis Dezember 2024 ausgeweitet. Unseren Analysen zufolge setzten Cyberkriminelle am häufigsten E-Mail-Phishing-Kampagnen ein, gefolgt von der Ausnutzung von Schwachstellen in Remote-Desktop-Protokollen (RDP) und Remote-Access-Tools.

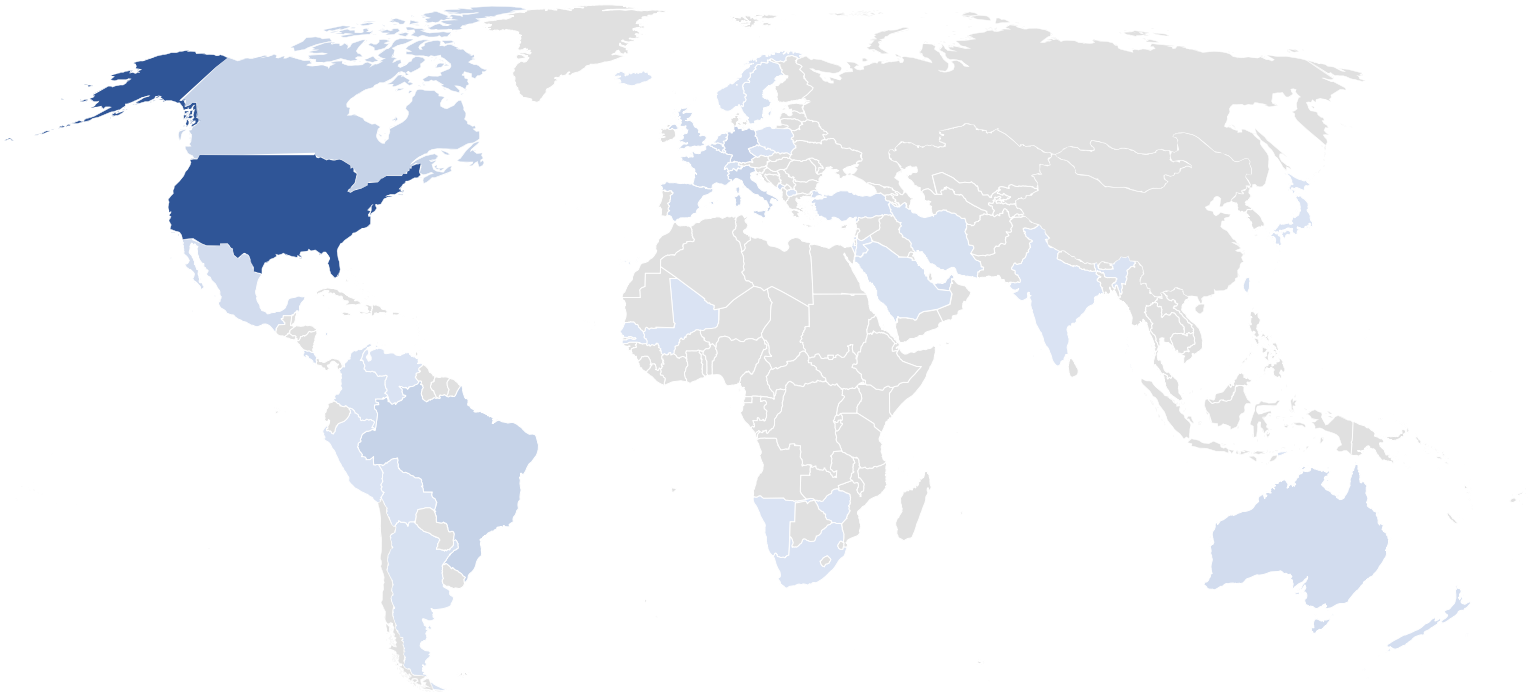
Erstvektor	Anzahl der Opfer
Phishing	62
RDP (Remote Desktop Protocol)	40
Ungepatchte Schwachstellen	35
Vertrauensbeziehung	26
Missbrauch von gültigen Konten / Anmeldedaten	22



Ransomware-Gruppen, die MSPs angreifen



Länder mit den meisten Angriffen auf MSPs



Anteil

1 %

62 %

MSPs werden zunehmend zum Hauptziel von Cyberangriffen und sehen sich mit den gleichen primären Angriffsvektoren konfrontiert wie andere Opfer. Unsere detaillierte Analyse der Angriffe auf MSPs im Jahr 2024 zeigt, dass Phishing mit 62 erfassten Vorfällen die vorherrschende Methode bleibt, gefolgt von der Ausnutzung ungepatchter Schwachstellen, dem Missbrauch von RDP und Angriffen, die Vertrauensbeziehungen ausnutzen. Kompromittierte Anmeldedaten und die Infiltration der Lieferkette bleiben ebenfalls wichtige Einfallstore. Diese Angriffsvektoren sind zwar nicht neu, aber nach wie vor alarmierend effektiv gegen MSPs, was auf Lücken in grundlegenden Sicherheitspraktiken hinweist.

Eine neue und besonders beunruhigende Entwicklung ist jedoch, dass MSPs zunehmend von Ransomware-Gruppen angegriffen werden, die mit hochentwickelten permanenten Bedrohungen (Advanced Persistent Threats, APTs) in Verbindung stehen. Diese professionellen Banden nutzen spionageähnliche Taktiken wie gestohlene Anmeldedaten, Social Engineering und Lieferkettenangriffe, um MSP-Netzwerke zu infiltrieren und Ransomware in den Systemen von MSP-Kund:innen zu verbreiten. Durch das Einbetten von Malware in vertrauenswürdige Software-Updates oder das Ausnutzen von Schwachstellen in Remote-Access-Lösungen nutzen APT-Banden die Vertrauensbeziehung zwischen einem MSP und seinen Kund:innen aus, um größeren Schaden anzurichten.

KI-generierte Cyberbedrohungen: Welche Herausforderungen galt es zu bewältigen?

In der sich ständig weiterentwickelnden Welt der Cybersicherheit sind KI-gestützte Cyberbedrohungen zu einem der drängendsten Probleme im Jahr 2024 geworden. Während KI weiterhin verschiedene Branchen revolutioniert, hat sie auch Cyberkriminelle in die Lage versetzt, immer raffiniertere Angriffe zu starten. Von der Entwicklung von Malware bis hin zum Social Engineering ist KI in den Händen von Cyberkriminellen sowohl ein Innovationswerkzeug als auch eine Waffe.

Im Folgenden beschreiben wir die wichtigsten KI-basierten Bedrohungen, die 2024 entstanden sind:

1. Cyberkriminelle missbrauchen KI für ihre Zwecke

OpenAI hat bestätigt, dass Cyberkriminelle ChatGPT und andere generative KI-Tools nutzen, um Malware zu entwickeln, Fehlinformationen zu verbreiten und Spearphishing-Kampagnen zu starten. In einer Reihe von Fällen haben Cyberkriminelle in jüngster Zeit KI eingesetzt, um die Effektivität ihrer Angriffe zu erhöhen:

- TA547 (auch bekannt als Scully Spider) nutzte einen KI-generierten PowerShell-Loader, um den Rhadamanthys-Infostealer einzuschleusen.
- Die chinesische Gruppe SweetSpecter hat OpenAI-Mitarbeiter:innen mit Phishing-E-Mails angegriffen, die bösartige Anhänge enthielten, was ein weiterer Beweis dafür ist, wie Cyberkriminelle KI nutzen, um ihre Angriffe effektiver zu machen.

Darüber hinaus haben Gruppen wie die iranischen CyberAv3ngers und von der nordkoreanischen Regierung unterstützte Hacker KI-Tools wie ChatGPT eingesetzt, um ihre Angriffe auf kritische Infrastrukturen zu verstärken und sensible Daten zu stehlen. Diese Entwicklungen spiegeln die wachsenden Fähigkeiten weniger versierter Angreifender wider, die nun in der Lage sind, mit Hilfe generativer KI ausgefeilte Angriffe durchzuführen.

2. Generative KI und die Entwicklung von Malware

Generative KI-Tools, darunter unregulierte Modelle wie WormGPT, FraudGPT und DarkBERT, ermöglichen es Cyberkriminellen, individuell angepasste Malware und Hackerskripte zu entwickeln. Ein eindrucksvolles Beispiel ist ein 25-jähriger Japaner, der ChatGPT nutzte, um in nur sechs Stunden Ransomware zu schreiben.

Diese KI-Modelle ermöglichen es Cyberkriminellen, herkömmliche Abwehrmaßnahmen zu umgehen, indem sie neue Angriffsvektoren generieren, die der Erkennung entgehen. Dieser Trend macht eine robuste, mehrschichtige Verteidigungsstrategie notwendig.

3. Nordkoreas Einsatz von KI für Cyberangriffe

Die Cyberangriffe Nordkoreas sind durch den Einsatz von KI raffinierter geworden. Durch den Einsatz von KI zur Erstellung gefälschter LinkedIn-Profile und Deepfake-Videos ist es nordkoreanischen Hackern gelungen, in global agierende Unternehmen einzudringen. Diese KI-generierten betrügerischen Personas führten zu erheblichen Sicherheitsverletzungen, einschließlich des Diebstahls von Kryptowährung und sensiblen Verteidigungsdaten.

4. KI-basierte Angriffe auf Software-Lieferketten

Der weit verbreitete Einsatz KI-gestützter Tools hat die Software-Lieferkette zu einem Hauptziel für Cyberkriminelle gemacht. Beispielsweise haben Cyberkriminelle vor Kurzem bösartige Pakete in das Python Package Index (PyPI) Repository hochgeladen und sich dabei als beliebte KI-Modelle wie ChatGPT und Claude ausgegeben. Diese Pakete, die Tausende von Downloads verzeichneten, enthielten einen Java-basierten Infostealer namens JarkaStealer. Nach der Installation stahl die Malware sensible Daten, darunter Informationen zu Webbrowsern und Session-IDs.

5. FBI warnt vor Betrugsversuchen mit KI

Das FBI schlägt Alarm, weil KI-Systeme eingesetzt werden, um das Ausmaß und die Raffinesse von Betrugsversuchen zu erhöhen. Von Romance Scams bis zu gefälschten Investitionsangeboten – KI-generierte Inhalte erleichtern es Cyberkriminellen, ihre Opfer zu täuschen. Durch die Erstellung täuschend echter Texte, Bilder und sogar Deepfake-Videos können Cyberkriminelle Betrugskampagnen entwickeln, die überzeugender sind oder eine größere Reichweite haben.

Die zwei Seiten von KI: Innovation vs. Missbrauch

Der Vormarsch der KI in der Cyberkriminalität verdeutlicht den doppelten Charakter dieser Technologie. Einerseits bietet KI ein enormes Innovationspotenzial mit Einsatzmöglichkeiten in Bereichen wie Gesundheit, Finanzen und Logistik. Andererseits ermöglicht ihr Missbrauch Cyberkriminellen immer ausgefeiltere, skalierbare und automatisierte Angriffe. Dies unterstreicht die dringende Notwendigkeit umfassender Cybersicherheitsstrategien, die mit der rasanten Entwicklung der Bedrohungen Schritt halten können.

Als Reaktion auf die Zunahme von KI-basierten Cyberbedrohungen erweitert Acronis kontinuierlich sein Cybersicherheitsangebot, um sicherzustellen, dass Unternehmen und Privatanwender:innen für die nächste Generation von Cyberangriffen gerüstet sind. Acronis Advanced Security + Extended Detection and Response (XDR) bietet proaktives Monitoring, KI-basierte Bedrohungserkennung und Echtzeit-Reaktionsmöglichkeiten, mit denen Unternehmen neuartige Bedrohungen neutralisieren können, bevor sie großen Schaden anrichten.

4 Tipps zur Abwehr von KI-basierten Bedrohungen

1 **Implementieren Sie ein mehrschichtiges Sicherheitskonzept**

Nutzen Sie eine Kombination aus Verhaltensanalyse, heuristischer Erkennung und KI-gestützter Überwachung, um KI-generierte Bedrohungen zu erkennen und zu blockieren.

2 **Behalten Sie KI-Schwachstellen im Auge**

Aktualisieren Sie regelmäßig Ihre Software und Sicherheitsprotokolle, um sich vor KI-Schwachstellen und Exploit-Versuchen zu schützen.

3 **Schulen Sie Ihr Personal und Ihre Partner**

Wissen macht den Unterschied. Bieten Sie regelmäßige Schulungen zur Erkennung von Phishing-Versuchen, Deepfakes und anderen Social-Engineering-Taktiken an, die auf KI basieren.

4 **Nutzen Sie KI für Ihren Schutz**

So wie Cyberkriminelle KI nutzen, um ihre Angriffe zu verbessern, sollten auch Cybersicherheitsanbieter KI einsetzen, um Bedrohungen schneller und effektiver zu erkennen und zu neutralisieren.

Fazit

Die Zunahme KI-gestützter Cyberbedrohungen im Jahr 2024 stellt eine bedeutende Veränderung in der Cybersicherheitslandschaft dar. Da KI sowohl die Angriffe als auch die Abwehr weiter verbessert, ist es für Unternehmen entscheidend, robuste KI-gestützte Sicherheitsmaßnahmen zu ergreifen, um Bedrohungen immer einen Schritt voraus zu sein. Die fortschrittlichen Sicherheitslösungen von Acronis sind darauf ausgelegt, diese Herausforderungen zu meistern, und bieten umfassenden Schutz vor der wachsenden Bedrohung durch KI-gestützte Cyberkriminalität. Die Kombination aus proaktiver Überwachung, Verhaltensanalyse und KI-gestützten Abwehrmechanismen ermöglicht es Unternehmen, sich vor ständig neuen KI-basierten Bedrohungen zu schützen.

Acronis

Acronis Threat Research Unit

Erfahren Sie mehr unter
www.acronis.com