2025

elastic security labs

GLOBAL THREAT RESEARCH REPORT

ZUSAMMENFASSUNG

Die Zeit der geduldigen, heimlichen Angriffe weicht einer neuen Ära von Hochgeschwindigkeitsbedrohungen.

Unsere Analyse im Jahresvergleich zeigt eine klare strategische Verschiebung: Angreifer rüsten auf Geschwindigkeit um, setzen KI als Waffe ein, um neuartige Bedrohungen in großem Umfang zu erzeugen, und priorisieren die sofortige Ausführung gegenüber längerem, verborgenem Vorgehen. Diese Beschleunigung zwingt die Verteidigung dazu, sich an einen Angriffslebenszyklus anzupassen, der in Minuten statt Monaten gemessen wird, wobei schnelle, kontextreiche Entscheidungen, die sowohl auf Echtzeit- als auch auf historischen Daten basieren, zum Schlüssel für eine wirksame Verteidigung geworden sind.

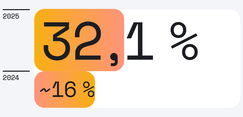
Der Elastic Global Threat Report 2025 von Elastic Security Labs analysiert diese neue Situation.

Auf der Grundlage unserer Analyse der globalen Bedrohungstelemetrie haben wir die Verhaltensweisen der Angreifer und die wichtigsten Innovationen bei der Abwehr ermittelt. Hier ist eine Vorschau dessen, was Sie erfahren werden:

#01

Die Prioritäten der Angreifer unter Windows haben sich geändert

Die Taktikkategorie **Ausführung** macht nun **32,1 %** des bösartigen Verhaltens aus – eine Verdoppelung ihres vorherigen Anteils von ca. 16 % – und hat **die Umgehung von Abwehrmechanismen** als Top-Taktik überholt. Dies unterbricht einen dreijährigen Trend und deutet auf eine strategische Verschiebung hin zum sofortigen Payload-Deployment statt anfänglicher Tarnung hin.

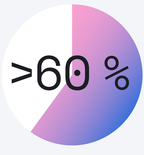


WAS DAS FÜR SIE BEDEUTET

→ Angreifer warten nicht mehr im Verborgenen ab; sie konzentrieren sich darauf, Schadcode sofort nach dem Eindringen auszuführen. Dies macht den Schutz des Laufzeitspeichers und die Verhinderung erster Zugriffe wichtiger denn je.

#02

Die Angriffsfläche in der Cloud ist stark konzentriert



Über 60 % aller Cloud-Sicherheitsereignisse lassen sich auf nur drei Angreiferziele reduzieren:

`Ziele der Angreifer`

/Erstzugriff
/Persistenz
/Zugangsdatenzugriff

WAS DAS FÜR SIE BEDEUTET

→ Über alle wichtigen Cloud-Plattformen hinweg ist diese Fokussierung auf **identitätsbasierte Angriffe** ein klares Signal dafür, dass die Verschärfung von Authentifizierungsabläufen und die Überwachung auf anomale privilegierte Zugriffe die effektivsten Möglichkeiten sind, um Ihre Cloud-Workloads zu schützen.

#03

Die Nutzung von KI als Waffe nimmt zu

+15,5 %

Wir haben einen **Anstieg der „generischen" Bedrohungen um 15,5 % festgestellt**, ein Trend, der wahrscheinlich dadurch angeheizt wird, dass Angreifer LLMs nutzen, um schnell einfache, aber effektive bösartige Loader und Tools zu erstellen.

WAS DAS FÜR SIE BEDEUTET

→ Die Zunahme KI-generierter Bedrohungen erhöht die Menge und Vielfalt der Malware, mit der Sie konfrontiert sind, dramatisch. Das bedeutet, dass Sie sich weniger auf statische Signaturen als vielmehr auf **Verhaltensanalysen und KI-gesteuerte Erkennung** verlassen sollten, um die Flut neuartiger Bedrohungen automatisch identifizieren und skalieren zu können.

#04

Der Diebstahl von Browser-Anmeldeinformationen ist ein großes Geschäft

>1 in 8

entwickelt, um Browser-Daten zu stehlen

Unsere Analyse von über **150.000 Malware**-Stichproben ergab, dass **mehr als 1 von 8 auf den Diebstahl von Browserdaten ausgelegt** ist. Dies ist nicht für den isolierten Einsatz gedacht; diese Anmeldedaten sind der Rohstoff für die **Access-Broker-Wirtschaft**, die anderen Angreifern einen stetigen Nachschub an Schlüsseln liefert, mit denen sie Unternehmens-Cloudkonten kompromittieren können.

WAS DAS FÜR SIE BEDEUTET

→ Der Browser ist ein zentrales Schlachtfeld für die sensibelsten Daten Ihres Unternehmens. Infostealer haben sich an die integrierten Browser-Schutzfunktionen angepasst, was bedeutet, dass herkömmliche Identitätskontrollen nicht mehr ausreichen.

Diese Trends sind eng miteinander verknüpft.

Ein Angreifer kann KI-generierte Malware verwenden, um Browser-Zugangsdaten zu stehlen, die dann genutzt werden, um einen ersten Zugang zu einem Cloudkonto zu erhalten. Sobald er im System ist, konzentriert er sich sofort auf die Ausführung, um Ransomware einzuschleusen oder Daten zu stehlen. Dieser Bericht verbindet die Punkte und zeigt, wie die moderne Angriffskette dieser TTPs aussieht und, was noch wichtiger ist, wie man sie an mehreren Stellen unterbrechen kann.

Die Bedrohungslandschaft ist komplex, aber durch das Verständnis von Malware und Bedrohungsverhalten sowie den Einsatz fortschrittlicher Abwehrmaßnahmen können Organisationen ihre Widerstandsfähigkeit erheblich verbessern.

SCHRITT 1
Fokussierung auf Ausführung

SCHRITT 2
Erlangung eines ersten Zugriffs auf ein Cloudkonto

SCHRITT 3
Verwendung KI-generierter Malware

SCHRITT 4
Diebstahl von Browser-Anmeldedaten

Elastic Security bietet die kollektive Intelligenz, die erweiterten Funktionen und die Einblicke, die Sie benötigen, um die heutigen Bedrohungen zu meistern und eine sicherere Zukunft aufzubauen.