

KURZFASSUNG



 **CROWDSTRIKE**

GLOBAL THREAT
REPORT
2025

Wichtige Angriffs- Muster

DAS GESCHÄFT MIT SOCIAL ENGINEERING

Die Techniken für den Erstzugriff veränderten sich im Jahr 2024, da Angreifer auf menschliche Schwächen abzielten und kompromittierte Anmeldedaten und Social Engineering einsetzten, um sich Zugang zu verschaffen und sich lateral innerhalb von Organisationen zu bewegen. CrowdStrike beobachtete einen Anstieg telefonischer Social-Engineering-Kampagnen und Helpdesk-Manipulationen, was auf eine Weiterentwicklung der eCrime-Taktiken hindeutet.

- Vishing-Aktivitäten nahmen zwischen dem ersten und dem zweiten Halbjahr 2024 um 442 % zu.
- Gut aufgestellte eCrime-Gruppierungen wie CURLY SPIDER, CHATTY SPIDER und PLUMP SPIDER nutzten diese Taktiken, um Zugangsdaten zu stehlen, Remote-Sitzungen aufzubauen und sich einer Erkennung zu entziehen.
- Im Laufe des Jahres 2024 verfolgte CrowdStrike mindestens sechs ähnliche, aber wahrscheinlich unterschiedliche Kampagnen, bei denen sich Bedrohungsakteure als IT-Mitarbeiter ausgaben, die Ziele anriefen und versuchten, sie zum Aufbau von Fernsupport-Sitzungen zu überreden.

FALLSTUDIE

CURLY SPIDER

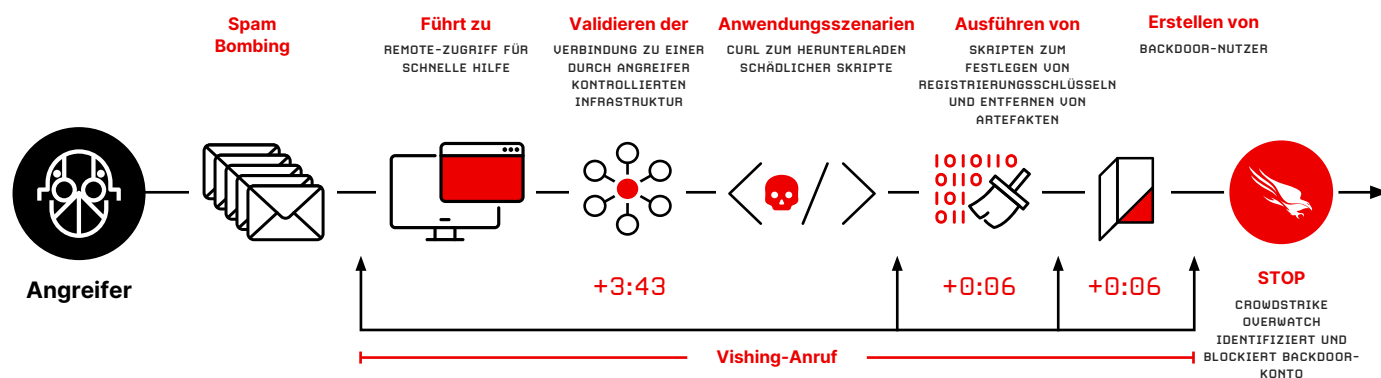


Abbildung 4. Zeitverlauf: CrowdStrike OverWatch ist schneller als CURLY SPIDER und stoppt einen Social-Engineering-Angriff in weniger als vier Minuten

Im Jahr 2024 entwickelte sich CURLY SPIDER zu einem der schnellsten und anpassungsfähigsten Angreifer im Bereich der Cyberkriminalität. In diesem Fall versuchten sie, ihre Ziele zu erreichen, ohne auf ein weiteres Gerät ausweichen zu müssen. Die gesamte Angriffskette – von der ersten Nutzer-Interaktion und Social Engineering bis hin zur Einrichtung eines Backdoor-Kontos, um Persistenz zu gewährleisten – dauerte weniger als vier Minuten.

Sobald CURLY SPIDER einen ersten Zugang erhält, ist ihr Zeitfenster begrenzt. Der Zugang besteht nur so lange, wie das Opfer am Telefon ist. Um die Kontrolle zu erweitern, besteht das unmittelbare Ziel des Angreifers darin, vor dem Ende der Sitzung einen dauerhaften Zugriff herzustellen.

Sobald der Remote-Zugriff gesichert ist, bewegt sich CURLY SPIDER schnell – oft noch während der aktiven Interaktion mit dem Opfer – um ihre Payloads bereitzustellen und Persistenz zu etablieren. Die meiste Zeit wird darauf verwendet, die Konnektivität sicherzustellen und Zugriffsprobleme zu beheben, um ihre in der Cloud gehosteten schädlichen Skripte zu erreichen.

Generative KI und der unternehmerische Angreifer

Obwohl GenAI noch relativ neu ist, hat CrowdStrike bereits mehrere Beispiele für Angreifer identifiziert, die diese Technologie nutzen. Die niedrige Einstiegsschwelle und die leistungsstarken Funktionen von GenAI machen es zu einem attraktiven Tool. Sie ermöglicht es Bedrohungsakteuren, überzeugende Phishing-E-Mails zu erstellen, Täuschungskampagnen durchzuführen und bösartige Skripte zu entwickeln, ein Trend, der sich voraussichtlich auch 2025 fortsetzen wird.

- Large Language Models (LLMs) und genAI-Modelle, die fotorealistische Bilder erzeugen, können mit minimalem Fachwissen überzeugende Inhalte in großem Maßstab generieren. Sie können Bemühungen im Bereich Social Engineering oder in der Informationsarbeit unterstützen.
- CrowdStrike reagierte auf [FAMOUS CHOLLIMA-Aktivitäten](#) in **304 Vorfällen über das ganze Jahr**, wobei **40 % auf Insider-Bedrohungsoperationen entfielen**. In einigen Fällen nutzten die Angreifer GenAI, um gefälschte LinkedIn-Profile zu erstellen.
- [NITRO SPIDER](#) nutzte KI-generierte Websites in Malvertising-Kampagnen, filterte Opfer durch bösartige Anzeigen und leitete andere auf durch KI-erstellte gefälschte Seiten um.

Chinas wachsende Cyber-Aktivitäten

Im Jahr 2024 erreichten Chinas Fähigkeiten im Bereich der Cyberspionage einen kritischen Wendepunkt, der durch immer dreistere Angriffe, heimlichere Taktiken und erweiterte operative Kapazitäten gekennzeichnet war. Diese Fortschritte spiegeln Chinas strategische Prioritäten im Intelligence-Bereich wider, darunter regionaler Einfluss, Technologieerwerb und die Unterdrückung von vermeintlichen Bedrohungen für die Stabilität des Regimes.

- Im Jahr 2024 waren die Angreifer mit Verbindungen zu China weiterhin in allen Sektoren und Regionen der Welt aktiv, wobei sie den Umfang ihrer Aktivitäten beibehielten, jedoch ihr Ausmaß erhöhten.
- CrowdStrike identifizierte im Jahr 2024 sieben neue Angreifer mit Bezug zu China und wies auf eine Verlagerung hin zu gezielteren und missionsspezifischeren Angriffen hin. Fünf dieser Gruppen sind einzigartig in ihrer Spezialisierung und ihrem Entwicklungsstand.
- [LIMINAL PANDA](#), [LOCKSMITH PANDA](#) und [OPERATOR PANDA](#) sind hochkompetente Angreifer mit einzigartigen Telekommunikationsnetzen, die auf Aufgaben und Toolsets abzielen. [VAULT PANDA](#) konzentriert sich auf den weltweiten Finanzdienstleistungssektor, und [ENVOY PANDA](#) ist ein zuvor leistungsschwacher Angreifer, der seine Betriebssicherheit (OPSEC) deutlich verbessert hat.

Cloudorientierte Akteure entwickeln sich weiter

Angreifer, die es auf Clouds abgesehen haben, nutzen Konfigurationsfehler, gestohlene Anmeldedaten und Cloud-Management-Tools aus, um Systeme zu infiltrieren, sich lateral zu bewegen und einen dauerhaften Zugang für Aktivitäten wie Datendiebstahl und die Bereitstellung von Ransomware aufrechtzuerhalten. Akteure, die Verbindungen zu China und Nordkorea haben, haben ihre Angriffe auf Cloud-Plattformen ausgeweitet, und eCrime-Gruppen haben fortschrittliche Taktiken wie den Missbrauch von Vertrauensbeziehungen und Insider-Bedrohungen eingesetzt, um Cloud-Ressourcen zu kompromittieren.

- Der Missbrauch eines gültigen Benutzernamens ist zur primären Taktik des Erstzugriffs geworden und macht in der ersten Hälfte des Jahres 2024 **35 % der Cloud-Vorfälle** aus. Angreifer verwenden zunehmend Taktiken, um unerkannt zu bleiben, und versuchen, an Zugangsdaten zu gelangen, um gültige Benutzerkonten ins Visier zu nehmen.
- Im Jahr 2023 entfielen auf den eCrime-Angreifer [SCATTERED SPIDER](#) **30 % aller Cloud-Einbrüche**. Diese Zahl sank im **Jahr 2024 auf 13 %**, auch weil viele Nationalstaaten und opportunistische Bedrohungsakteure zunehmend auf die Cloud-Kontrollebene abzielen.
- In **75 % der beobachteten Fälle** haben cloudorientierte Angreifer Indikatoren aus Protokolldateien entfernt, um einer Erkennung zu entgehen.



Wachsende Schwachstellenausnutzung

Angreifer nehmen zunehmend internetfähige Netzwerk-Appliances ins Visier und nutzen deren inhärente Sicherheitsschwächen aus, um einen ersten Zugriff zu erlangen, wenn die Sichtbarkeit der Endpunkterkennung und -Reaktion (Endpoint Detection and Response, EDR) eingeschränkt ist. Sie erreichen die Remote-Codeausführung (Remote Code Execution, RCE) mit Techniken wie der Verkettung von Exploits oder dem Missbrauch legitimer Produktfunktionen und nutzen bekannte Schwachstellen häufig für die wiederholte Kompromittierung derselben Geräte um. Angreifer haben es weiterhin auf Appliances am Ende ihrer Lebensdauer abgesehen, da veraltete Systeme mit ungepatchten Schwachstellen Einfallstore in Zielumgebungen bieten.

- Bedrohungsakteure zielen auf Schwachstellen im proprietären Betriebssystem (OS) der Netzwerk-Appliance ab. Diese Schwachstellen sind attraktive Ziele, da sie es Angreifern potenziell ermöglichen, einen Fehler auszunutzen, um mehrere Produkte mit demselben Betriebssystem anzugreifen.
- Die Verkettung mehrerer Schwachstellen bietet Angreifern weitere Vorteile. Zunächst ermöglicht es ihnen, nicht authentifizierte RCE zu erreichen, indem sie mehrere Exploits in einem Angriff kombinieren. Zum anderen untergräbt Exploit-Chaining den auf Schweregradbewertungen basierenden Patching-Prozess, den viele Unternehmen anwenden.
- Um neue Schwachstellen zu entdecken oder legitime Produktfunktionen zu missbrauchen, werden Angreifer wahrscheinlich schneller als in den Vorjahren technische Blogs nutzen und öffentliche Proof-of-Concept-Exploits (POC) operationalisieren.

SaaS-Ausnutzung wird voraussichtlich anhalten

Im Laufe des Jahres 2024 beobachtete CrowdStrike Intelligence, dass mehrere eCrime- und gezielt vorgehenden Eindringlinge den Zugang zu cloudbasierten Software as Service (SaaS)-Anwendungen nutzten, um Daten zu erhalten, die laterale Bewegungen, Erpressung und Angriffe auf Dritte erleichtern. Bedrohungsakteure haben sich oft Zugang zu diesen Anwendungen verschafft, indem sie Identitäten für die einmalige Anmeldung (Single Sign-On, SSO) kompromittiert haben. Da die Cloud-Nutzung zunimmt, gehen wir davon aus, dass Angreifer ihre Methoden im Jahr 2025 verfeinern werden, wodurch die Nutzung von SaaS zu einer kritischen und sich weiterentwickelnden Bedrohung wird.

- In der ersten Hälfte des Jahres 2024 hatten cloudbasierte Bedrohungsakteure häufig Microsoft 365 ins Visier genommen, wobei **bei 22 % der Angriffe auf SharePoint und bei 17 % auf Outlook zugegriffen wurde**.
- SCATTERED SPIDER hat kompromittierte SSO-Konten genutzt, um auf eine Vielzahl integrierter SaaS-Anwendungen zuzugreifen, darunter Chat, Kundenbeziehungsmanagement, Verwaltung von Anmeldeinformationen, Dokumentenspeicherung, Produktivität und Sicherheitstools.
- Bei vielen Angriffen durchsuchten Angreifer SaaS-Anwendungen nach den folgenden Informationen: 1) Kontoanmeldeinformationen und Dokumentation der Netzwerkarchitektur, um sich lateral zu bewegen, und 2) Cyberversicherungs- und Umsatzdaten, um Erpressungsforderungen zu bekräftigen.



Fazit

Zu Beginn des Jahres 2025 entwickelt sich die Landschaft der Cybersicherheit weiterhin rasant und stellt Organisationen in allen Sektoren und Regionen vor große Herausforderungen. Die Resilienz, Innovationskraft und Anpassungsfähigkeit der Angreifer machen umso deutlicher, dass ein umfassendes Verständnis der heutigen Bedrohungen in allen Aspekten der Landschaft notwendig ist.

Social Engineering verbreitete sich im Jahr 2024, als Angreifer neue Methoden für den Erstzugriff erforschten, um Sicherheitsvorkehrungen zu umgehen. GenAI wurde zu einem wichtigen Werkzeug für Angreifer, insbesondere zur Unterstützung von Social-Engineering-Kampagnen und hochdynamischen Kampagnen für Intelligence Operations (IO). CrowdStrike geht davon aus, dass diese 2025 von Angreifern eingesetzt wird.

Gezielte eCrime-Angriffe stellen nach wie vor eine anhaltende Bedrohung für bestimmte Sektoren dar. Im Laufe des Jahres 2024 erwiesen sich eCrime-Angreifer bei der Verfolgung ihrer Ziele als hartnäckig und glichen ihr weniger raffiniertes Vorgehen oft durch den Erwerb von fundierten Kenntnissen über die Sektoren, Regionen und damit verbundenen Technologien der Opfer aus.

Gezielt vorgehende Angreifer waren im Jahr 2024 aktiv und innovativ und passten ihre Taktiken an, um geopolitische und strategische Ziele zu erreichen und gleichzeitig verstärkte Verteidigungsmaßnahmen zu umgehen. Es wird erwartet, dass die Angreifer mit Verbindungen zu Russland weiterhin aggressiv auf einen Sieg in der Ukraine hinarbeiten und sich dabei auf verdeckte Operationen zur Informationsbeschaffung konzentrieren, die sich gegen die Ukraine und NATO-Mitglieder richten. Die Angreifer, die mit China in Verbindung stehen, werden wahrscheinlich von langfristigen Investitionen in Cyberprogramme profitieren, was sich in verstärkten OPSEC-Praktiken, einem anhaltend hohen Einsatztempo und einer regen globalen Eindringlingsaktivität äußert.

Die Ausnutzung von Schwachstellen bleibt ein kritischer Punkt. Es wird erwartet, dass Bedrohungsakteure weiterhin aggressiv Geräte an der Netzwerkperipherie ins Visier nehmen, insbesondere Netzwerk-Appliances. SaaS-Anwendungen sind ebenfalls im Fadenkreuz. Nachdem eCrime- und gezielt vorgehende Angreifer im Jahr 2024 den Zugang zu cloudbasierten SaaS-Anwendungen genutzt haben, um Daten für laterale Bewegungen, Erpressung und Angriffe auf Dritte zu erhalten, geht CrowdStrike davon aus, dass die Ausnutzung von SaaS im Jahr 2025 eine Bedrohung darstellen wird, die es im Auge zu behalten gilt.

Im Laufe des Jahres 2024 erweiterten unternehmerische Angreifer die Reife und Raffinesse ihrer Operationen über Sektoren und Regionen hinweg. Während sich diese Bedrohungen im Jahr 2025 weiterentwickeln, bleibt das CrowdStrike Counter Adversary Operations Team weiterhin bestrebt, Bedrohungsakteure zu identifizieren, zu verfolgen und zu stören, wann und wo immer dies möglich ist.

Empfehlungen

1

Das gesamte Identitätsökosystem sichern

Angreifer zielen zunehmend auf Identitäten ab, indem sie Zugangsdaten stehlen, die Multifaktor-Authentifizierung (MFA) umgehen und Social Engineering betreiben, während sie sich über vertrauenswürdige Beziehungen heimlich lateral zwischen lokalen, Cloud- und SaaS-Umgebungen bewegen. Dadurch können sie sich als legitime Nutzer ausgeben, Zugriffsrechte erweitern und der Entdeckung entgehen.

Organisationen sollten Phishing-resistente MFA-Lösungen wie Hardware-Sicherheitsschlüssel einsetzen, um unbefugten Zugriff zu verhindern. Strenge Identitäts- und Zugriffsrichtlinien sind unerlässlich, einschließlich Just-in-Time-Zugriff, regelmäßige Kontoprüfungen und bedingte Zugriffskontrollen. Tools zur Erkennung von Identitätsbedrohungen müssen das Verhalten sowohl auf Endgeräten als auch in lokalen, Cloud- und SaaS-Umgebungen überwachen, um die Erweiterung von Zugriffsrechten, unbefugten Zugriff oder die Erstellung von Backdoor-Konten zu melden. Die Integration dieser Tools in XDR-Plattformen (Extended Detection and Response) gewährleistet umfassende Transparenz und einen einheitlichen Schutz vor Angreifern.

Darüber hinaus sollten Organisationen Nutzer darin schulen, Vishing- und Phishing-Versuche zu erkennen, und gleichzeitig eine proaktive Überwachung aufrechtzuerhalten, um identitätsbasierte Bedrohungen zu erkennen und darauf zu reagieren.

2

Lücken in der domänenübergreifenden Sichtbarkeit beseitigen

Die zunehmende Verwendung von „Hands-on-keyboard“-Techniken und legitimen Tools durch Angreifer erschwert die Erkennung und Reaktion. Im Gegensatz zu herkömmlicher Malware können Angreifer mit diesen Methoden herkömmliche Sicherheitsmaßnahmen umgehen, indem sie Befehle ausführen und legitime Software verwenden, um normale Vorgänge nachzuahmen.

Um dem entgegenzuwirken, müssen Organisationen ihre Erkennungs- und Reaktionsstrategien modernisieren. XDR und die nächste Generation von Sicherheitsinformations- und Ereignismanagement (SIEM)-Lösungen bieten eine einheitliche Sichtbarkeit über Endgeräte, Netzwerke, Cloud-Umgebungen und Identitätssysteme hinweg und ermöglichen es Analysten, verdächtige Verhaltensweisen zu korrelieren und den gesamten Angriffspfad zu sehen.

Proaktive Bedrohungssuchen und Threat Intelligence verbessern die Erkennung weiter, indem sie potenzielle Angriffsmuster identifizieren und Einblicke in die TTPs (Taktiken, Techniken und Prozeduren) der Angreifer bieten. Mit Echtzeit-Informationen können Organisationen über aufkeimende Bedrohungen auf dem Laufenden bleiben, Angriffe vorhersehen und kritische Sicherheitsmaßnahmen priorisieren.

3

Die Cloud als Kerninfrastruktur schützen

Cloud-fokussierte Angreifer nutzen Konfigurationsfehler, gestohlene Anmeldedaten und Cloud-Management-Tools aus, um Systeme zu infiltrieren, sich lateral zu bewegen und einen dauerhaften Zugang für böswillige Aktivitäten wie Datendiebstahl und die Bereitstellung von Ransomware aufrechtzuerhalten.

Cloudnative Plattformen zum Schutz von Anwendungen (Cloud-Native Application Protection Platforms, CNAPPs) mit Cloud-Erkennungs- und Reaktionsfunktionen (Cloud Detection and Response, CDR) sind unerlässlich, um diesen Bedrohungen entgegenzuwirken.

Diese Lösungen bieten Anwendern einen einheitlichen Überblick über ihre Cloud-Sicherheitslage und helfen ihnen, Konfigurationsfehler, Schwachstellen und Bedrohungen durch Angreifer schnell zu erkennen, zu priorisieren und zu beheben. Darüber hinaus wird durch die Durchsetzung strenger Zugriffskontrollen – wie rollenbasierter Zugriff und bedingte Richtlinien – die Angriffsfläche kritischer Systeme begrenzt und eine kontinuierliche Überwachung auf Anomalien sichergestellt, zu denen Anmeldungen von unerwarteten Standorten aus gehören.

Auch regelmäßige Audits sind für die Aufrechterhaltung der Sicherheit von entscheidender Bedeutung. Automatisierte Tools können zu freizügige Speichereinstellungen, ungeschützte APIs und ungepatchte Schwachstellen aufdecken. Durch häufige Überprüfungen der Cloud-Umgebungen wird sichergestellt, dass ungenutzte Berechtigungen und veraltete Konfigurationen umgehend behoben werden.

4

Priorisierung von Schwachstellen mit einem auf den Angreifer ausgerichteten Ansatz

Angreifer nutzen zunehmend öffentlich bekannte Schwachstellen aus und setzen Exploit-Chaining ein, indem sie mehrere Schwachstellen kombinieren, um schnellen Zugriff zu erhalten, ihre Zugriffsrechte zu erweitern und Abwehrmaßnahmen zu umgehen. Diese mehrstufigen Angriffe stützen sich oft auf öffentliche Ressourcen wie POC-Exploits und technische Blogs, die es den Angreifern ermöglichen, effektive und schwer zu entdeckende Nutzlasten zu erstellen.

Um diesen Bedrohungen entgegenzuwirken, müssen Organisationen dem regelmäßigen Patchen oder Aktualisieren kritischer Systeme Priorität einräumen, insbesondere bei häufig angegriffenen internetbasierten Diensten wie Webservern und VPN-Gateways. Die Überwachung auf subtile Anzeichen von Exploit-Chaining, wie z. B. unerwartete Abstürze oder Versuche zur Erweiterung von Zugriffsrechten, kann dabei helfen, Angriffe zu erkennen, bevor sie sich ausbreiten.

Tools wie [CrowdStrike Falcon® Exposure Management](#), das mit nativer KI-Priorisierung entwickelt wurde, ermöglichen es Teams, Störfaktoren zu reduzieren und sich auf die wichtigsten Schwachstellen zu konzentrieren, insbesondere auf solche, die kritische und risikoreiche Systeme betreffen. Durch die Einführung proaktiver Sicherheitsansätze, die Erkennung von Schwachstellen auf der gesamten Angriffsfläche und die Nutzung von Automatisierung können Unternehmen ausgeklügelte Bedrohungen abwehren und die Möglichkeiten der Angreifer einschränken.

5

Den Angreifer kennen und vorbereitet sein

Wenn ein Cyberangriff innerhalb von Minuten – oder sogar Sekunden – stattfindet, kann eine gute Vorbereitung den Unterschied zwischen Eindämmung und Katastrophe ausmachen. Ein informationsgestützter Ansatz ermöglicht es Sicherheitsteams, über eine reaktive Verteidigung hinauszugehen, indem sie verstehen, welcher Angreifer sie ins Visier nimmt, wie er vorgeht und welche Ziele er verfolgt. Mithilfe von Threat Intelligence, der Erstellung von Profilen der Angreifer und der Analyse von Vorgehensweisen können Sicherheitsteams Ressourcen priorisieren, Abwehrmaßnahmen anpassen und aktiv nach Bedrohungen suchen, bevor diese eskalieren. Die Threat Intelligence von CrowdStrike deckt nicht nur bekannte Bedrohungen auf, sondern antizipiert auch neue und sich entwickelnde Vorgehensweisen, sodass Sicherheitsverantwortliche immer einen Schritt voraus sind. Durch die nahtlose Integration von Informationen in Sicherheits-Workflows können Organisationen ihre Reaktionszeiten verkürzen, Angreifer stören und diese Informationen in Maßnahmen umsetzen.

Obwohl Technologie für die Erkennung und Verhinderung von Angriffen von entscheidender Bedeutung ist, bleibt der Nutzer ein entscheidendes Glied in der Kette, um Kompromittierungen zu verhindern. Organisationen sollten Programme zur Sensibilisierung von Nutzern initiieren, um die anhaltende Bedrohung durch Phishing und damit zusammenhängende Social-Engineering-Techniken zu bekämpfen. Bei Sicherheitsteams gilt: Übung macht den Meister. Fördern Sie eine Umgebung, in der regelmäßig Tabletop- und Red Team/Blue Team-Übungen durchgeführt werden, um Lücken zu identifizieren und Schwachstellen in Ihren Cybersicherheitsprozessen und Reaktionen zu beseitigen.

Vollständigen Bericht herunterladen

Der CrowdStrike Global Threat Report 2025 bietet eine umfassende Analyse der wichtigsten Trends und Ereignisse bei Cyber-Bedrohungsaktivitäten im Jahr 2024. Laden Sie ein kostenloses Exemplar des Berichts unter <https://www.crowdstrike.com/global-threat-report/> herunter.



Über CrowdStrike

[CrowdStrike](#) (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit geschäftskritischer Unternehmensbereiche neu.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

CrowdStrike: We stop breaches.

Weitere Informationen: <https://www.crowdstrike.com/de-de/>

Folgen Sie uns: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#) | [YouTube](#)

Jetzt kostenlos testen: www.crowdstrike.com/free-trial-guide