Deutsche Ausgabe

ThreatDown™
Powered by Malwarebytes

# 2024 Lagebericht zu Schadsoftware

Von Schadsoftware zu Bedrohungen: ein umfassender Leitfaden zur Verteidigung

# Inhalt

# 1. Warum Sie einen Leitfaden benötigen

## Von Schadsoftware zu Bedrohungen

Internetkriminalität ist ein florierendes und bestens organisiertes Geschäft – ein milliardenschweres Spiegelbild der legalen Wirtschaft, auf deren Kosten sie sich bereichert. Ihr verstreutes Ökosystem umfasst ganze Lieferketten und spezialisierte Organisationen wie Access-Broker, die Anmeldeinformationen von Unternehmen stehlen und weiterverkaufen, und Anbieter bösartiger Schadsoftware. Internetkriminalität kennt Markennamen, PR-Gags, Personalabteilungen, Anreizsysteme und „Mitarbeiter des Monats".

Und wie das breitere, gesetzestreue „Geschäft" verfügt sie über eine Reihe von gut funktionierenden Werkzeugen. Sitzen Sie an einem regulären Desktop-Computer in den USA oder in Europa, schauen Sie auf Software, die Ihnen auch vor 15 Jahren vertraut gewesen wäre, wie Microsoft Windows, Office und einen Webbrowser.

Internetkriminelle nutzen dagegen Infostealer, Phishing und Ransomware. Ähnlich wie bei Windows und Office handelt es bei diesen um ausgereifte und effektive Werkzeuge, deren neueste Versionen seit Jahren im Vergleich zu ihren Vorgängern nur mit marginalen Verbesserungen aufwarten. Innovation im Bereich der Internetkriminalität bedeutet daher zunehmend die Entwicklung neuer Taktiken. Der Fokus liegt heute eher darauf, wie Angriffe erfolgreich sein können, als darauf, was Schadsoftware leisten kann.

### Über diesen Bericht

Um dem neuen Fokus weg von Schadsoftware hin zu Bedrohungen Rechnung zu tragen, haben wir unseren Lagebericht zu Schadsoftware ein weiteres Mal überarbeitet. Wir haben unsere Experten gefragt, worauf IT-Teams mit knappen Ressourcen im kommenden Jahr achten sollten. Sie haben sechs Bedrohungen ausgemacht, die einige der gefährlichsten Taktiken von Internetkriminellen, die wir unter Windows, Mac und Android gesehen haben, veranschaulichen. Diese Liste ist nicht vollständig - wenn Sie jedoch diese Bedrohungen im Griff haben, sind Sie auch für alles Andere, was das Ökosystem der Cyberkriminalität bereithält, gut gerüstet.

Schadsoftware ist so gefährlich wie je. Kommt sie zum Einsatz, ist sie jedoch nur ein einzelnes Glied einer ganzen Angriffskette, die gleich mehrere Bedrohungen umfasst. IT- und Sicherheitsteams sehen sich heute mit Living-off-the-Land-(LOTL-)Angriffen, aktiven Gegnern, Zero-Day-Exploits, kompromittierten Konten, Social Engineering sowie einer ganzen Reihe weiterer Bedrohungen konfrontiert, die nicht unter die traditionelle Definition von Schadsoftware fallen.

Und vor diesem Hintergrund werden die Sicherheitsbudgets gekürzt, während sich die begrenzten Ressourcen der IT- und Sicherheitsteams mit einer immer komplexeren Umgebung konfrontiert sehen. Dies wird 2024 nicht länger funktionieren. Begrenzte Sicherheitsressourcen, schlecht integrierte Endpunktsicherheitsprodukte – um dem Druck von Gegnern rund um die Uhr standhalten zu können, braucht es einen anderen Sicherheitsansatz.

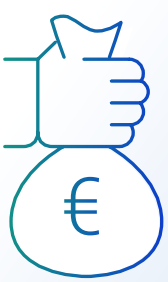
Eine effektive Cyberabwehr erfordert qualifizierte und erfahrene Sicherheitsprofis, die verdächtige Aktivitäten identifizieren und diesen jederzeit nachgehen – Tag und Nacht – sowie eine ausgefeilte, engmaschige und benutzerfreundliche Sicherheitssoftware, die nicht nur auf die Beseitigung von Schadsoftware ausgelegt ist, sondern Cyberbedrohungen jeglicher Art gewachsen ist.

# 2. Lehren aus 2023

## Wichtige Entwicklungen

Ransomware wird auch 2024 die größte Cyberbedrohung bleiben, mit der sich Unternehmen auseinandersetzen müssen. Das in Geld schwimmende Ransomware-Ökosystem verzeichnete 2023 einen starken Schub und konnte seine Taktiken weiterentwickeln.

Die Anzahl bekannter Angriffe nahm in Deutschland um 36 % zu, die weltweiten durchschnittlichen Lösegeldforderungen stiegen sprunghaft an und die höchste geforderte Summe des Jahres waren atemberaubende 74 Mio. Euro – gefordert von der Bande LockBit nach einem Angriff auf die britische Royal Mail.



**74 Mio. Euro**

Die höchste bekannte Lösegeldforderung im Jahr 2023 betrug 74 Mio. Euro und wurde von LockBit an die britische Royal Mail gerichtet.

In einem alarmierenden Bruch mit gängigen Normen nutzte die Ransomware-Bande CL0P zwei Zero-Day-Schwachstellen, um zwei verheerende automatisierte Datendiebstahl-Kampagnen durchzuführen, die innerhalb weniger Tage Tausende ahnungslose Unternehmen traf. Dieser Ansatz ermöglichte es CL0P, selbst die erfahrensten Ransomware-as-a-Service-Gruppen hinter sich zu lassen und satte 92 Mio. Euro (100 Mio. US-Dollar) einzunehmen. Ihre Taktik wird 2024 mit Sicherheit Nachahmer finden.

Weniger versierte Banden nutzten die Schwierigkeit aus, die manche Unternehmen noch immer mit der Durchführung eines effektiven Patch-Managements haben. Im Februar wurden beim größten bekannten Ransomware-Angriff, der jemals auf Nicht-Windows-Geräte ausgeführt wurde, Tausende veralteter VMWare ESXi-Server unter Ausnutzung einer zwei Jahre alten Schwachstelle kompromittiert. Und im Mai erschien wie aus dem Nichts MalasLocker und stellte mit einer Kampagne gegen Zimbra-Server, die sechs Monate ungepatcht geblieben waren, alle anderen Ransomware-Banden in den Schatten.

## Cyberbedrohungen entwickelten sich auch andernorts weiter

Nach Microsofts Entscheidung, Makros in aus dem Internet heruntergeladenen Dokumenten zu blockieren, diversifizierten Kriminelle ihre Taktiken und begannen, sich vor allem erneut für bösartige Werbung (Malvertising) zu interessieren. Zahllose Kampagnen imitierten Marken wie Amazon, Zoom und WebEx, um sowohl Windows- als auch Mac-Schadsoftware über täuschend echte Werbeanzeigen und Websites einzuschleusen. Anbieter der Werbeanzeigen waren offenbar machtlos bei dem Versuch, sie zu stoppen.

Kriminelle hatten jedoch nicht überall die Oberhand. Im August gab das US-amerikanische Justizministerium die Zerschlagung der berüchtigten Schadsoftware Qakbot bekannt und nannte diese „die größte von den USA angeführte finanzielle und technische Störung einer Botnet-Infrastruktur, die von Internetkriminellen zur Durchführung von Ransomware, Finanzbetrug und weiteren kriminellen Aktivitäten im Internet genutzt wurde."

Das Jahr 2023 sah zudem eine gemäßigtere Reaktion auf die generative KI. Die Begeisterung, die die Einführung von ChatGPT im Jahr zuvor noch hervorgerufen hatte, wich einer maßvollen Würdigung der Technologie dahinter. Ein Jahr nach dem Auftritt von ChatGPT gibt es bisher keine bedeutenden Sicherheitstools oder Cyberbedrohungen, die auf ChatGPT oder anderen KI-Lösungen basieren. Das Potenzial der KI, die Cybersicherheit tiefgreifend zu stören, bleibt jedoch nach wie vor bestehen und ihre zu erwartenden langfristigen Auswirkungen bleiben unklar.

In einem Zug, der von anderen Ländern vermutlich genau verfolgt werden wird, versuchte Großbritannien mit einem neuen Online-Sicherheitsgesetz, den Status-Quo von Social-Media- und Messaging-Unternehmen infrage zu stellen. Das Gesetz wurde weithin als die Forderung an Unternehmen interpretiert, Nachrichten von Benutzern nach illegalen Inhalten zu scannen, wofür sie die Ende-zu-Ende-Verschlüsselung (E2EE) hätten aufheben müssen. Sowohl WhatsApp als auch Signal drohten daraufhin, den britischen Markt zu verlassen, sollte das Gesetz verabschiedet werden. Ein politischer Trick ersparte allen Beteiligten eine Blamage, der umstrittene Wortlaut des Gesetzes wurde jedoch nicht geändert und sein Potenzial, gegen Verschlüsselung verwendet zu werden, bleibt bestehen.

Während die Verschlüsselung von einigen Seiten angegriffen wurde, ermöglichte sie an anderer Stelle erhebliche Verbesserungen in puncto Sicherheit. Google und Microsoft lösten ihr Versprechen ein, Passkeys zu unterstützen, eine auf Verschlüsselung basierende Alternative zu Kennwörtern, die nicht gestohlen, erraten, geknackt oder „gephisht" werden kann. Die Unternehmen haben Unterstützung für Passkeys eingeführt und ermutigen Benutzer aktiv dazu, sie zu nutzen – ein eindeutiger Gewinn im Hinblick auf Sicherheit und etwas, von dem wir 2024 vermutlich sehr viel mehr hören werden.

Die Weiterentwicklung von Cyberbedrohungen über das letzte Jahr zwang Unternehmen dazu, mit einer Weiterentwicklung ihrer eigenen Sicherheit zu reagieren. Die folgenden Kapitel erklären, was Sie über die folgenschwersten Cyberbedrohungen wissen müssen, und was Sie in puncto Rat, Techniken und Technologie benötigen, um Ihr Unternehmen zu schützen.

# 3. Big-Game-Ransomware

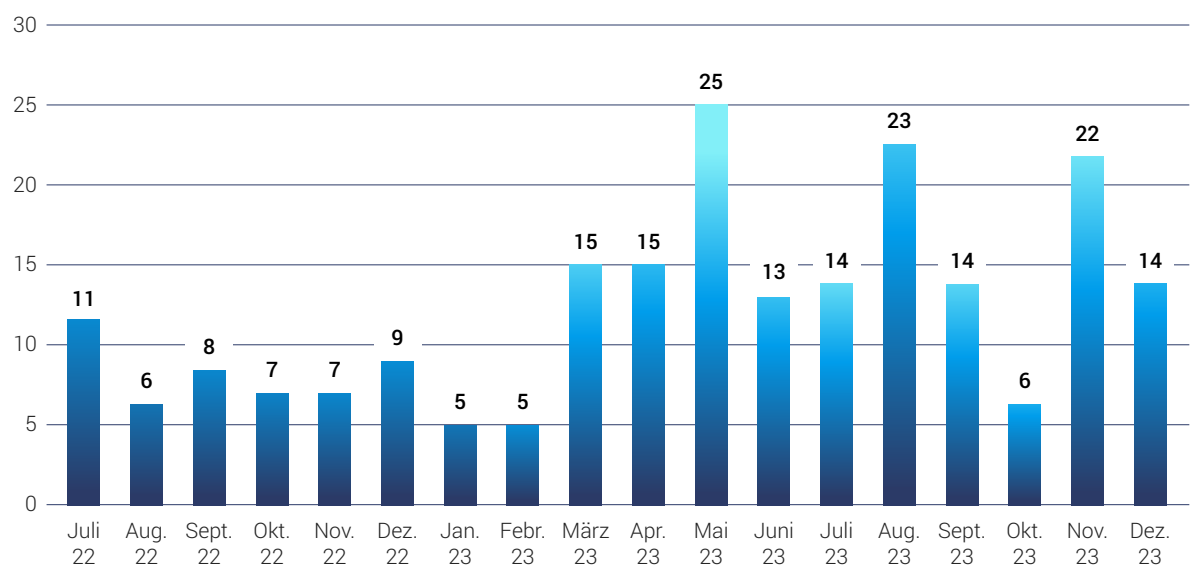
Seit ihrer Entstehung im Jahr 2018 ist Big-Game-Ransomware die gefährlichste Cyberbedrohung für Unternehmen in der ganzen Welt. Diese auf finanzstarke Unternehmen („Big Game" – „Großwild") zielenden Ransomware-Angriffe nötigen Unternehmen zur Zahlung riesiger Lösegelder, indem sie deren Daten als Geisel nehmen – entweder mittels Verschlüsselung, der Drohung die Daten zu veröffentlichen, oder beides.

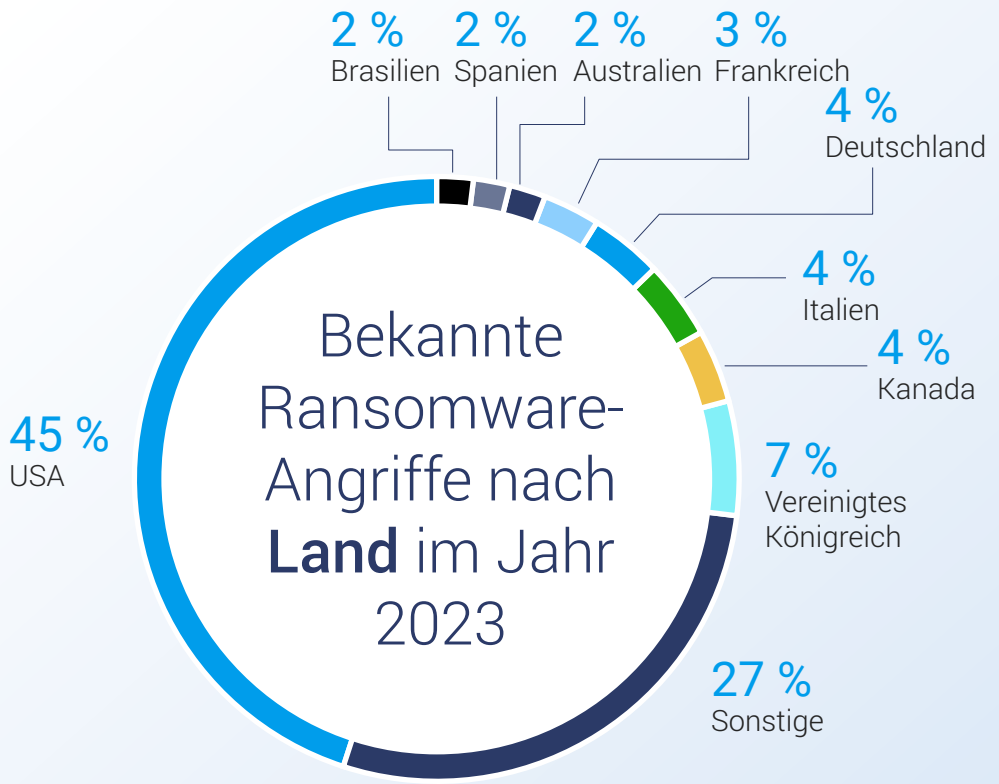
Das Problem der Big-Game-Ransomware hat sich im Jahr 2023 leider beträchtlich verschlechtert. Die Anzahl bekannter Angriffe ist weltweit um 68 % und in Deutschland um 36 % gestiegen. Laut dem Ransomware-Incident-Response-Unternehmen Coveware ist die durchschnittliche Lösegeldzahlung im ersten Quartal des Jahres weltweit auf 740 Tsd. US-Dollar gestiegen. Zudem geht das Unternehmen davon aus, dass Lösegeldzahlungen im Jahr 2023 insgesamt die Marke von einer Milliarde Dollar erreichen werden.

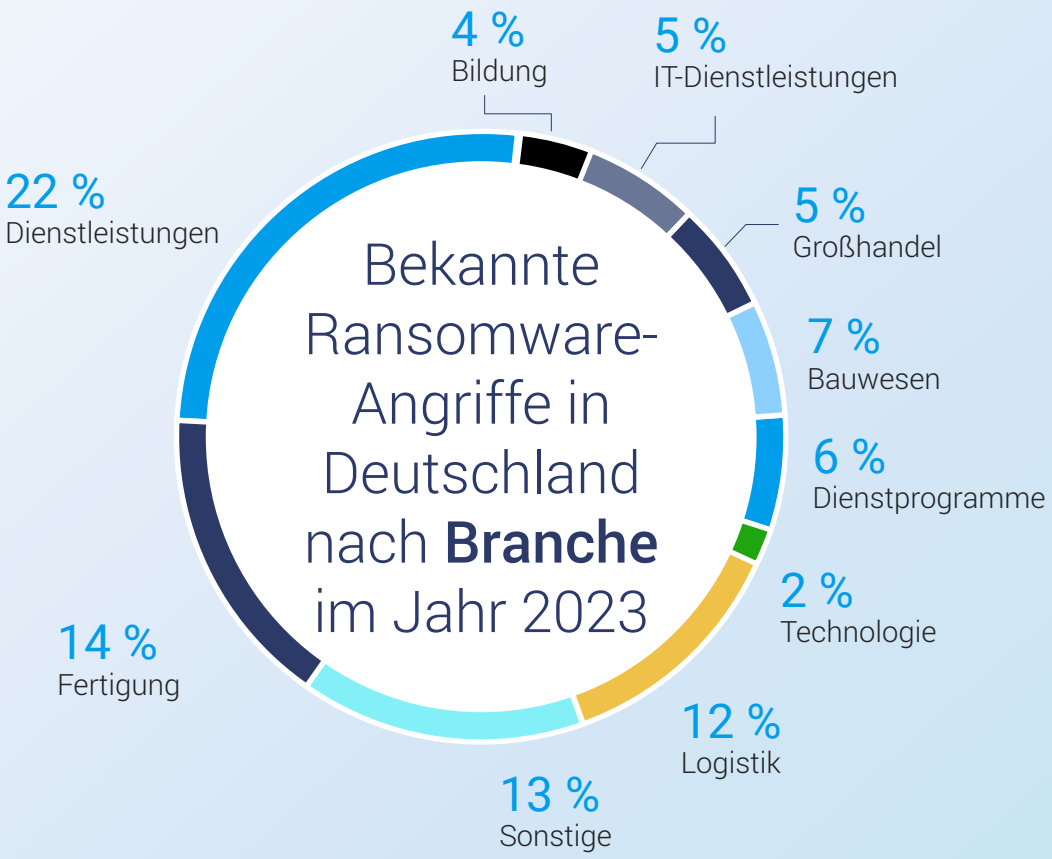
**36 %** Die Anzahl bekannter Ransomware-Angriffe in Deutschland stieg im Jahr 2023 um 36 %.

**4 %** 4 % aller Ransomware-Angriffe entfielen im Jahr 2023 auf Deutschland.

## Bekannte Ransomware-Angriffe in Deutschland nach Monat




Bekannte Ransomware-Angriffe nach **Land** im Jahr 2023
2 % Brasilien
2 % Spanien
2 % Australien
3 % Frankreich
4 % Deutschland
4 % Italien
4 % Kanada
7 % Vereinigtes Königreich
27 % Sonstige
45 % USA


Bekannte Ransomware-Angriffe in Deutschland nach **Branche** im Jahr 2023
4 % Bildung
5 % IT-Dienstleistungen
5 % Großhandel
7 % Bauwesen
6 % Dienstprogramme
2 % Technologie
12 % Logistik
13 % Sonstige
14 % Fertigung
22 % Dienstleistungen

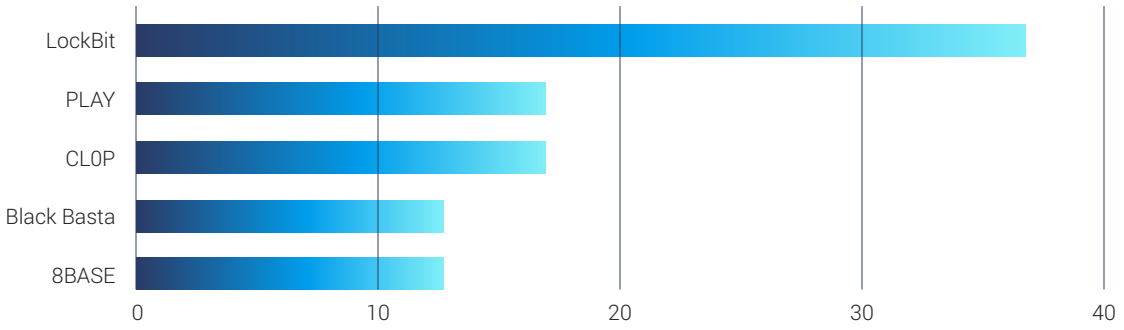
Es kann Wochen dauern, bis ein Ransomware-Angriff vorbereitet ist und kriminelle Hacker in ein Ziel eingedrungen sind, sich selbst zu Administratoren gemacht, die Umgebung erkundet, Daten gestohlen und ihre Ransomware anschließend bis in jede Ecke des Netzwerks verbreitet haben. Wurde der Angriff schließlich ausgelöst, geschieht dies zu einem Zeitpunkt, an dem das Opfer am wenigsten in der Lage ist, zu reagieren: nachts, am Wochenende oder während der Ferien. Vertreter des Ziels und der Ransomware-Bande verhandeln anschließend tage- oder sogar wochenlang in einem Darknet-Chat.

Big-Game-Angriffe können enorm lukrativ sein, sind aber auch arbeitsintensiv. Die Antwort des kriminellen Untergrunds auf das Problem der Skalierbarkeit, dem sich Big-Game-Ransomware gegenübersieht, ist Ransomware-as-a-Service (RaaS): eine Ransomware, bei der häufig drei verschiedene Arten von kriminellen Organisationen an einem einzigen Angriff zusammenarbeiten.

Zunächst dringen kriminelle Banden, die darauf spezialisiert sind, in Unternehmensnetzwerken Fuß zu fassen, in ein Unternehmen ein. Diese böswilligen Gruppen, so genannte Initial Access Broker (IAB), wenden eine Vielzahl von Taktiken an, um in Unternehmen einzubrechen wie Phishing, Trojaner, Passwort-Spraying und das Ausnutzen von Schwachstellen in mit dem Internet verbundener Infrastruktur. In der nächsten Phase eines Angriffs verkaufen IAB den von ihnen erlangten Zugang an so genannte Ransomware-Affiliates.

Affiliates sind kriminelle Banden, die Ransomware-Angriffe ausführen. Anstatt ihre eigene Ransomware zu schreiben, kaufen Affiliates sie von einem Anbieter von Ransomware-as-a-Service (RaaS) wie LockBit, ALPHV oder Play.

## Die fünf größten Big-Game-Ransomware-Gruppen in Deutschland im Jahr 2023

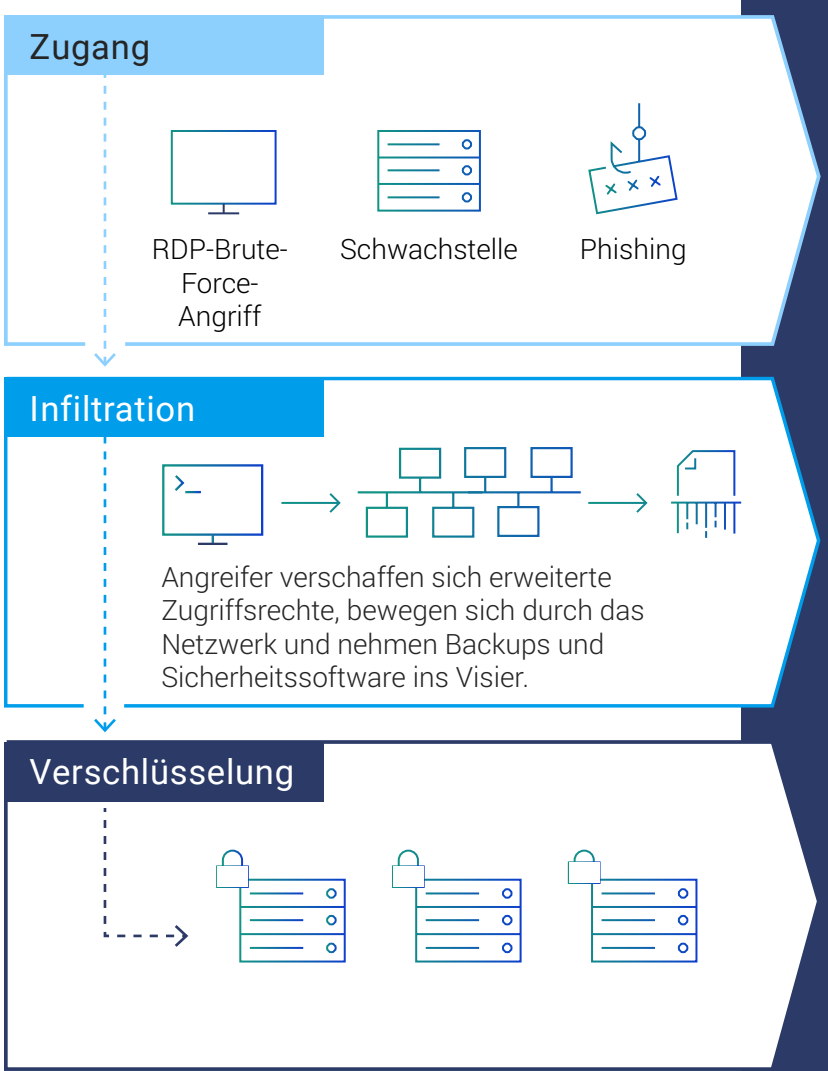



LockBit bleibt der am meisten genutzte RaaS, die Konkurrenz jedoch schließt auf.

LockBit ist weltweit und auch in Deutschland der am meisten genutzte RaaS-Anbieter. Im Jahr 2023 entfielen in Deutschland mehr als doppelt so viele Angriffe auf LockBit wie auf seinen nächsten Konkurrenten. Obwohl die Gesamtanzahl von LockBit-Angriffen gegenüber dem Vorjahr zunahm, nahm ihr Anteil an den weltweiten Angriffen von 31 % im Jahr 2022 auf 22 % im Jahr 2023 ab. Seine Konkurrenz schließt auf – ein weiteres besorgniserregendes Zeichen für den Aufschwung im Bereich Ransomware.

Die Bedrohung durch Big-Game-Ransomware steigt und die für sie verantwortlich zeichnenden Banden sind entschlossen, erfahren und gut ausgestattet. Die Abwehr von Big-Game-Ransomware erfordert einen integrierten Sicherheitsansatz, der eine branchenführende Sicherheitslösung in Kombination mit erfahrenen Bedrohungsjägern und Incident-Response-Experten umfasst.

## Angriffsphasen der Big-Game-Ransomware




## Schutz durch ThreatDown

Brute-Force-Schutz, Vulnerability Assessment, Patch Management, Anti-Exploit-Schutz sowie Filterung von Website-Inhalten verhindern verschiedene Arten des Zugriffs.

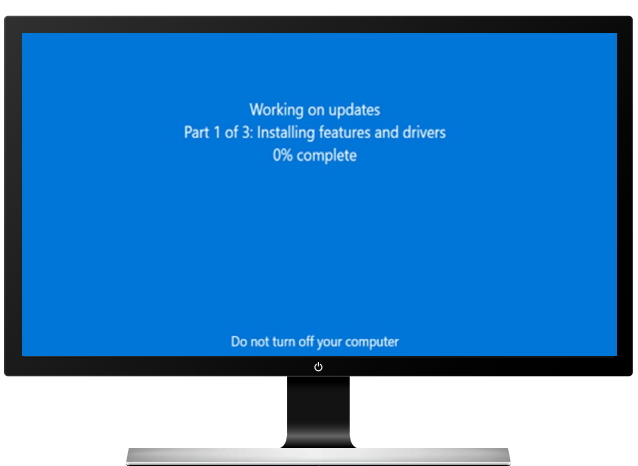
Managed Detection & Response (MDR) identifiziert Angreifer in Ihrem Netzwerk, bevor sie ihre Ransomware aktivieren können; ein Antivirusprogramm der nächsten Generation, ein App-Blocker sowie Anti-Exploit-Schutz verweigern Angreifern Zugriff auf ihre Tools; eine Filterung von Website-Inhalten blockiert Angreifern den Zugriff auf Command-and-Control-Server.

Endpoint Detection & Response (EDR) stoppt Ransomware; Ransomware Rollback stellt verschlüsselte Dateien wieder her; Incident Response bietet nach einem Angriff Sorgenfreiheit.

# 4. Malvertising

Die Verwendung bösartiger Werbung (Malvertising) zur Verbreitung von Schadsoftware ist nicht neu. 2023 erlebte sie jedoch einen Aufschwung, der sowohl für Unternehmen als auch für Privatanwender zur Bedrohung wurde. Der Anstieg lässt sich vermutlich auf die späten (jedoch notwendigen) Bemühungen von Microsoft zurückführen, Makros in aus dem Internet heruntergeladenen Dokumenten zu blockieren, was eine der erfolgreichsten Verbreitungstechniken für Schadsoftware darstellte. Als dieser Weg nicht mehr zur Verfügung stand, suchten Internetkriminelle anderswo nach neuen Möglichkeiten.

Malvertising macht sich häufig Social-Engineering-Techniken zunutze, um Schadsoftware zu installieren. Internetkriminelle erstellen Google-Suchanzeigen, die beliebte Marken imitieren und zu täuschend echten Kopien von Websites führen, auf denen Benutzer dazu verleitet werden, Schadsoftware herunterzuladen.




**Eine Malvertising-Website, die sich als Windows-Systemupdate ausgibt.**

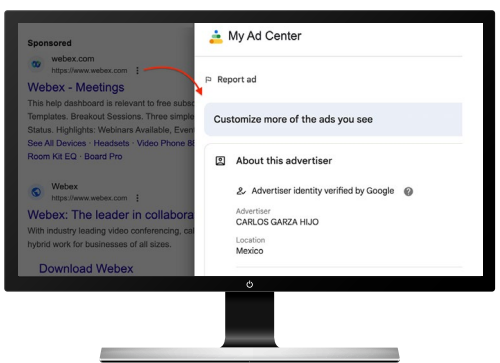
Obwohl Google und andere Anzeigen-Anbieter Malvertising das ganze Jahr über bekämpften, blieben die Bedrohungsakteure ihnen 2023 stets einen Schritt voraus und konnten Anzeigenverifizierungen umgehen.

Auf Privatanwender zielendes Malvertising kann bekannte Marken wie Amazon, Dienstprogramme wie PDF-Konverter oder aktuelle Themen wie Investitionen in Kryptowährungen nachahmen. Unternehmen werden häufig mit Anzeigen für Software-Downloads wie für Slack, Webex, Zoom und 1Password ins Visier genommen. Zudem zielten Kriminelle im Jahr 2023 auf IT-Mitarbeiter mit gefälschten Versionen von Tools wie dem Advanced IP Scanner.

## Amazon war 2023 die am häufigsten imitierte Marke.

Die Anzeigen und Websites sind täuschend echt und in der Regel sehr viel schwieriger zu erkennen als bösartige E-Mails. Malvertising nutzt außerdem ausgeklügelten Fingerprinting-Code, um festzustellen, ob ein Besucher ein Bot wie der Such-Crawler von Google oder ein Sicherheitsforscher ist. So wird sichergestellt, dass die gefälschten Seiten nur von potenziellen Opfern gesehen werden – und Angreifer länger unerkannt bleiben.

| Die fünf am häufigsten imitierten Marken | |
|---|---|
| 1 | Amazon |
| 2 | Rufus |
| 3 | Weebly |
| 4 | NotePad++ |
| 5 | TradingView |




**Der einzige Hinweis darauf, dass diese Webex-Anzeige gefälscht ist, findet sich in den Angaben zum Werbetreibenden.**

Obwohl bösartige Websites schnell identifiziert und gelöscht werden, sind sie leicht zu ersetzen und die zugrundeliegende Infrastruktur wird nur selten gestört. Da ihre Verbreitungskette für Schadsoftware so unbeeinträchtigt blieb, konnten sich bösartige Akteure 2023 auf die immer raffiniertere Gestaltung ihrer als Köder ausgelegten Websites und Schadsoftware-Payloads konzentrieren.

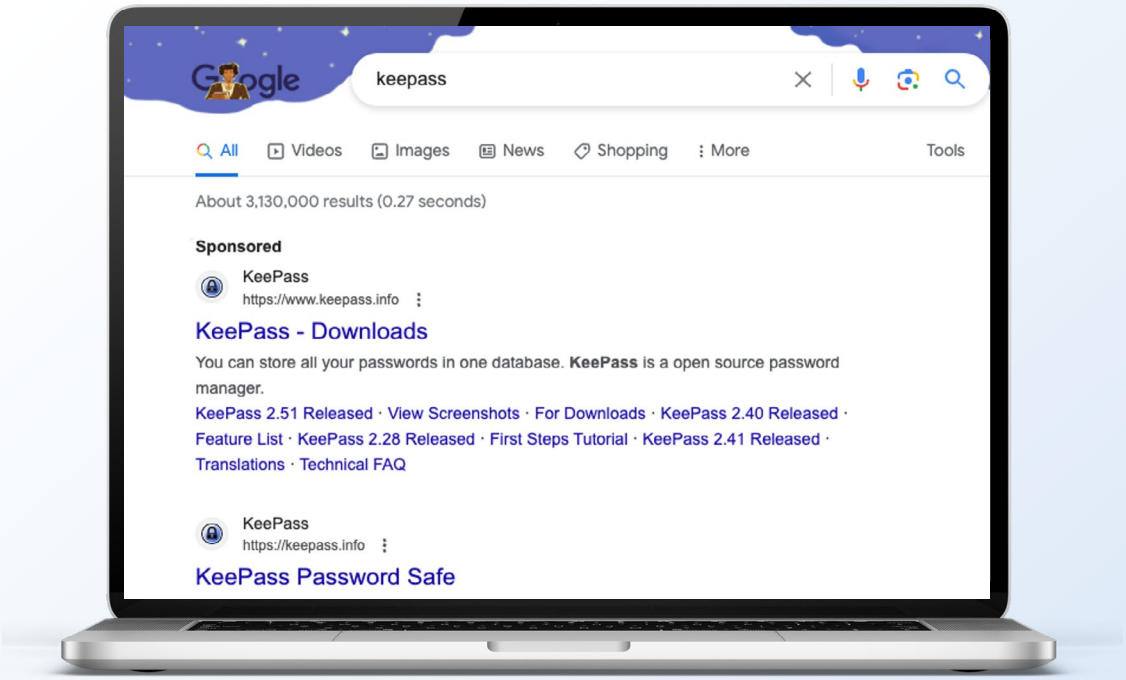
Schadsoftware-Payloads variieren je nach Kampagne, zum Einsatz kommen jedoch häufig Infostealer wie IcedID, Aurora Stealer und BatLoader. Diese Programme stehlen Anmeldeinformationen von Browsern oder Computern von Benutzern und schaffen so die Voraussetzung für Ransomware-Angriffe.

| Die fünf am häufigsten entdeckten Schadsoftware-Arten | |
|---|---|
| 1 | Aurora Stealer |
| 2 | Vidar |
| 3 | Redline Stealer |
| 4 | BatLoader |
| 5 | IcedID |

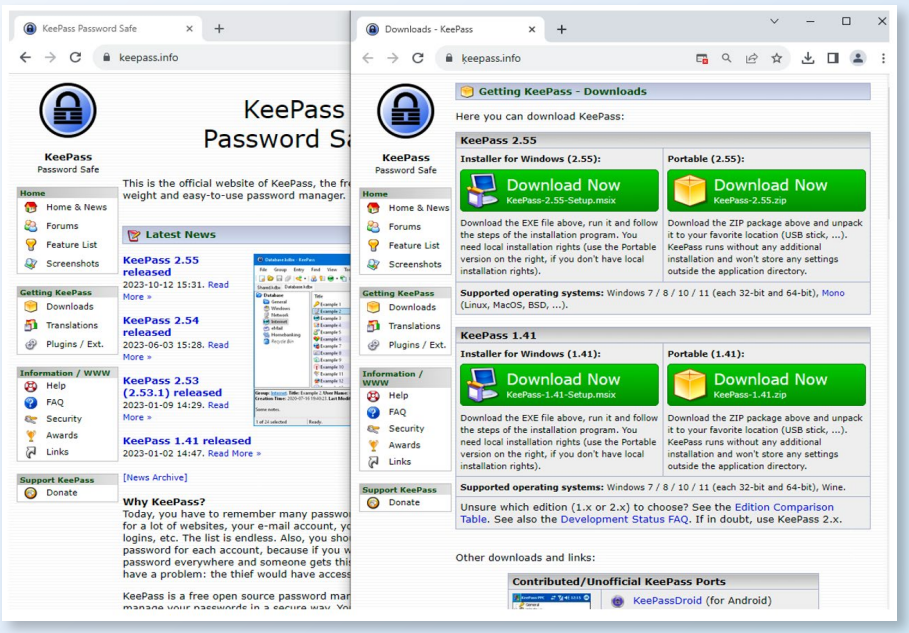
Die Ransomware-Bande Royal zum Beispiel nutzte AnyDesk als einen Malvertising-Köder für BatLoader, mit dem als Vorstufe für einen Ransomware-Angriff ein Cobalt-Strike-Beacon abgelegt wurde.

Malvertising bietet Kriminellen eine Reihe von Vorteilen gegenüber bösartigen E-Mail-Anhängen. Benutzer wissen sehr viel weniger über Malvertising und sind nur selten geschult, es zu erkennen. Und selbst, wenn sie es sind, bietet das streng kontrollierte Format der Suchanzeigen Benutzern nur sehr wenige Anhaltspunkte, anhand derer sie sie überprüfen können. Suchanzeigen können auch gezielt auf bestimmte Suchbegriffe, geographische Gebiete und demografische Gruppen ausgerichtet werden, sodass Ziele nur die Kampagnen sehen, die ihr Interesse erregen.

| Die fünf am häufigsten missbrauchten Wirte | |
|---|---|
| 1 | Dropbox |
| 2 | Discord |
| 3 | 4sync |
| 4 | GitLab |
| 5 | Google |




**Eine bösartige Anzeige für den Passwortmanager KeePass, die einer legitimen Anzeige täuschend ähnlich ist.**




**Die wirkliche KeePass-Website (links) neben einer Malvertising-Website (rechts).**

Malvertising nimmt dramatisch zu, da Kriminelle nach Alternativen zu Makros suchen, mit denen sie Schadsoftware wie Trojaner, Infostealer und Ransomware verbreiten können. Um sich gegen Malvertising schützen zu können, braucht es eine effektive Filterung von Website-Inhalten, die Schadsoftware verbreitende Websites stoppen kann, sowie eine branchenführende Sicherheitslösung als Sicherheitsnetz, damit sich Angriffe nicht ausbreiten können.

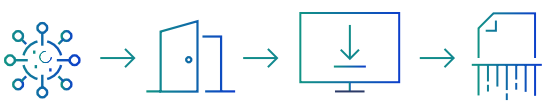
## Phasen eines Malvertising-Angriffs

### Bösartige Anzeige


### Bösartige Website

Schadsoftware, getarnt als legitime Software, wird heruntergeladen.

### Schadsoftware



Schadsoftware stiehlt Daten, lädt weitere Schadsoftware herunter oder schafft den Zugang für einen Ransomware-Angriff.

### Ransomware

## Schutz durch ThreatDown

Eine Filterung von Website-Inhalten blockiert bösartige Websites; ein Antivirusprogramm der nächsten Generation stoppt Schadsoftware.

Managed Detection & Response (MDR) identifiziert und untersucht verdächtiges Verhalten in Ihrem Netzwerk; eine Filterung von Website-Inhalten blockiert Angreifern den Zugriff auf Command-and-Control-Server.

Endpoint Detection & Response (EDR) stoppt Ransomware; Ransomware Rollback stellt verschlüsselte Dateien wieder her; Incident Response bietet nach einem Angriff Sorgenfreiheit.

# 5. Zero-Day-Ransomware

Big-Game-Ransomware ist aufgrund ihres destabilisierenden Potenzials und ihrer verheerenden Auswirkungen die größte Cyberbedrohung, der sich Unternehmen heute gegenübersehen. So groß ihre existentielle Bedrohung auch ist, ist mit ihr dennoch nur eine anscheinend harmlose Anzahl von Angriffen verbunden, was ein Licht auf das Problem der Skalierbarkeit von Big-Game-Ransomware wirft. Big-Game-Ransomware-Angriffe sind begrenzt, da sie auf menschliche Arbeit angewiesen sind. Es kann Wochen dauern, bis Angriffe und Verhandlungen abgeschlossen sind. Mehr Angriffe erfordern mehr Leute. Daher werden viele potenzielle Ziele übergangen.

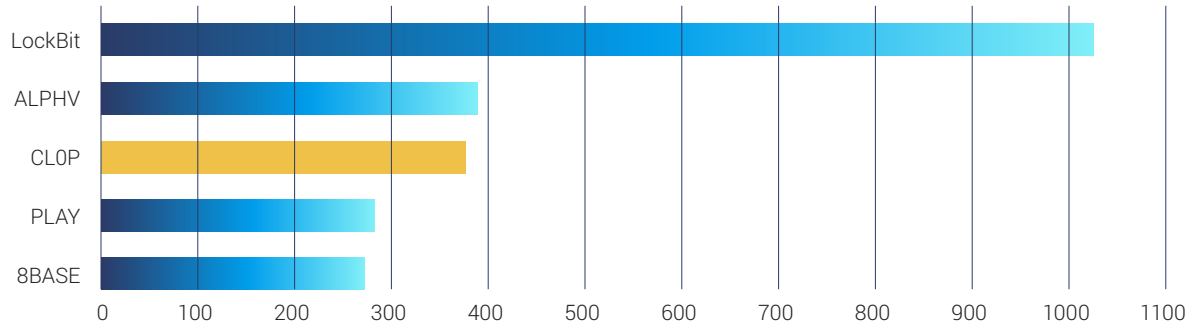
2023 gelang es der Ransomware-Bande CL0P jedoch, die Barriere der Skalierbarkeit zu überwinden. Sie erschütterte die Sicherheitswelt mit einer Reihe kurzer, automatisierter Kampagnen, die Hunderte von ahnungslosen Zielen gleichzeitig mit Angriffen auf der Basis von Zero-Day-Exploits trafen.

Die wiederholte Ausnutzung von Zero-Days, d. h. neu entdeckten Sicherheitslücken, signalisierte eine neue Stufe an Fähigkeiten für eine Ransomware-Bande. Innerhalb weniger Wochen war CL0P die drittaktivste Big-Game-Ransomware-Gruppe des Jahres und stellte sogar Rivalen in den Schatten, die 2023 jeden Monat aktiv waren.

Die Ausnutzung von Zero-Day-Schwachstellen bedeutete, dass Unternehmen sich nicht mit Sicherheitsupdates und herkömmlichen Erkennungstechniken für Schadsoftware schützen konnten.

Bezeichnenderweise waren die Angriffe nicht auf Verschlüsselung angewiesen. In beiden Kampagnen stahl die Bande CL0P Daten der Opfer und drohte damit, diese zu veröffentlichen, wenn das Lösegeld nicht gezahlt werde – der Einsatz von Ransomware war nicht notwendig.

**Die fünf aktivsten Ransomware-Gruppen im Jahr 2023 nach bekannten Angriffen**




CL0P war die drittaktivste Gruppe, obwohl sie für die meiste Zeit des Jahres nicht tätig war.

Zwischen dem 18. und 31. Januar führte CL0P einen automatisierten Angriff auf Unternehmen aus, die das Datenübertragungstool GoAnywhere MFT von Fortra verwenden. Die Bande nutze eine Zero-Day-Schwachstelle aus, um nicht autorisierte Konten in den Umgebungen der Opfer zu erstellen, die anschließend dazu genutzt wurden, Daten zu stehlen und bösartige Tools zu installieren. Im März begannen Daten von rund 100 Opfern, die kein Lösegeld zahlten, auf einer Datenleck-Website von CL0P zu erscheinen.

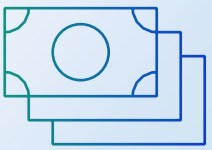
Kurze Zeit später kehrte die Bande mit einer noch größeren Kampagne zurück, die auf einer Sicherheitslücke in der Dateiübertragungssoftware MOVEit Transfer von Progress basierte. Die Schwachstelle wurde dazu genutzt, eine Webshell zu installieren, die zum Stehlen von Dateien aus der Datenbank der Software verwendet wurde.

Die Ausnutzung begann am 27. Mai, Progress Software informierte seine Kunden über die Schwachstelle am 31. Mai. Eine Woche später übernahm CL0P die Verantwortung für die Angriffe.

Die Angriffe erfolgten nach dem Muster eines Blitzeinbruchs, was bedeutete, dass die gestohlenen Daten nicht so sorgfältig ausgewählt werden konnten und nicht so sensibel waren, wie es im Falle eines manuellen Angriffs möglich gewesen wäre. Dies führte dazu, dass sich viele Opfer weigerten, ein Lösegeld zu zahlen. Das Ransomware-Incident-Response-Unternehmen Coveware vermutet jedoch, dass es der Gruppe gelang, dies zu kompensieren, indem es überdurchschnittlich hohe Lösegelder verlangte und am Ende etwa 100 Mio. US-Dollar (92 Mio. Euro) mit dieser einen Kampagne verdiente.

## 92 Mio. Euro

Es wird geschätzt, dass CL0P mit ihrer MOVEit-Transfer-Zero-Day-Kampagne zwischen 75 und 100 Mio. US-Dollar (70 bis 92 Mio. Euro) erpresste.



Die Folge davon ist, dass CL0P für 2024 über ein Vermögen verfügt, das in den Kauf oder die Entdeckung neuer Sicherheitslücken reinvestiert werden kann. Und es hat gezeigt, dass Ransomware über seine etablierten Grenzen hinaus skaliert werden kann. Es ist kaum vorstellbar, dass andere Ransomware-Gruppen nicht versuchen werden, diese Taktik 2024 zu kopieren.

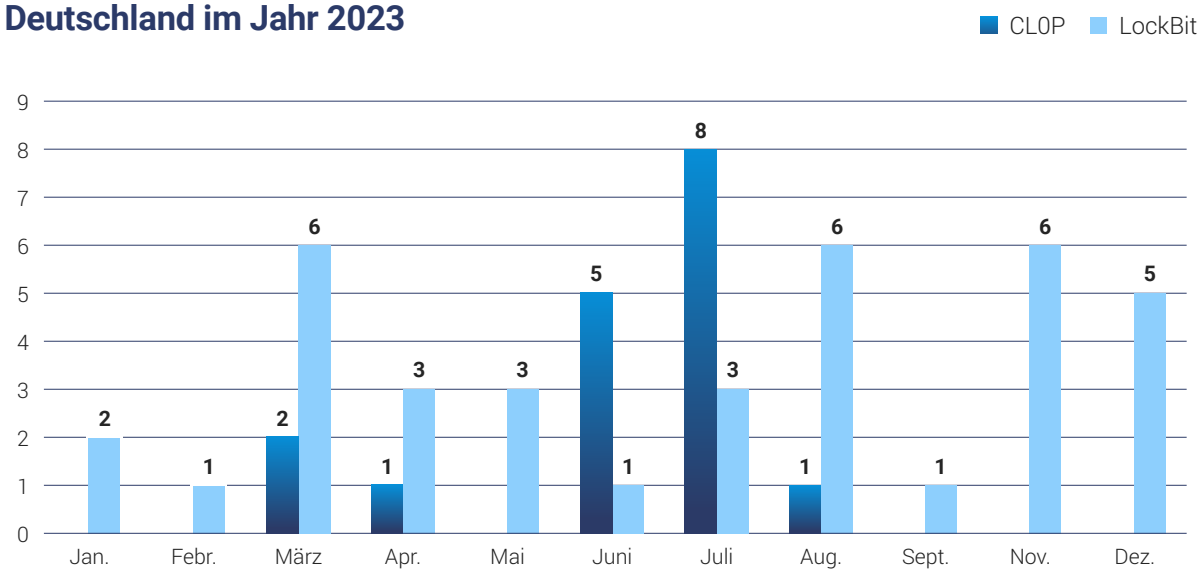
## CVE-2023-0669

Die erste Kampagne von CL0P nutzte CVE-2023-0669 aus, eine zuvor unbekannte Remotecodeausführungs-Schwachstelle in GoAnywhere MFT.

## CVE-2023-34362

Die erfolgreichste Kampagne von CL0P nutzte CVE-2023-34362 aus, eine zuvor unbekannte SQL-Injection-Schwachstelle in MOVEit Transfer.

## Monatliche Angriffe von LockBit und CL0P in Deutschland im Jahr 2023




LockBit war in jedem Monat des Jahres aktiv, dennoch wurde CL0P mit Angriffen, die nur wenige Wochen dauerten, einer seiner Hauptrivalen.

## Erklärung auf der CL0P-Website

CL0P traf so viele Unternehmen, dass sich die Gruppe gezwungen sah, auf ihrer Website diese Erklärung abzugeben, um die Verhandlungen mit Hunderten von Opfern zu vereinfachen.

> WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
>
> ***STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE***
>
> ***STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
>
> ***STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
>
> ***STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
>
> ***STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
>
> ***STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***
>
> ***STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH***

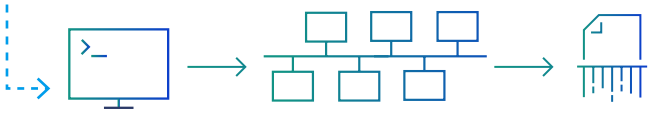
Zero-Day-Ransomware ist eine wachsende Bedrohung, die eine ernsthafte Gefahr für Unternehmen darstellt. Sie nutzt unbekannte Schwachstellen aus und ist daher schwierig zu entdecken. Die Abwehr von Zero-Day-Ransomware erfordert einen integrierten Sicherheitsansatz mit einer branchenführenden Sicherheitslösung und erfahrenen Bedrohungsjägern, die verdächtige Aktivitäten in Ihrem Netzwerk finden und ihnen nachgehen.

## Phasen eines Zero-Day-Ransomware-Angriffs

### Zugang

Zero-Day-Schwachstelle

### Infiltration



Angreifer setzen Tools ein und stehlen Daten

## Schutz durch ThreatDown

Vulnerability Assessment und Patch Management gewährleisten, dass Systeme schnell geschützt sind, sobald ein Patch verfügbar ist.

Managed Detection & Response (MDR) identifiziert und untersucht verdächtiges Verhalten in Ihrem Netzwerk; eine Filterung von Website-Inhalten blockiert Angreifern den Zugriff auf Command-and-Control-Server; ein Antivirusprogramm der nächsten Generation stoppt bösartige Hintertüren.

# 6. Living-off-the-Land-Angriffe

Als Living off the Land (LOTL) wird eine verdeckte Cyberangriffsmethode bezeichnet, bei der Kriminelle bösartige Aktivitäten mittels legitimer IT-Admin-Tools wie Powershell, PsExec oder der Windows-Verwaltungsinstrumentation (WMI) durchführen.

Da selbst die bösartige Verwendung dieser Werkzeuge dem ungeübten Auge wie normale Netzwerkaktivität erscheinen kann, sind LOTL-Angriffe für IT-Teams nur sehr schwer zu erkennen.

Ransomware-Banden wie LockBit, ALPHV und Royal nutzen LOTL-Techniken, um unerkannt zu arbeiten, während sie Angriffe innerhalb von Unternehmensnetzwerken vorbereiten und dazu Rechte ausweiten, Befehle ausführen, Skripte herunterladen, sich seitlich durch das Netzwerk bewegen, Daten stehlen und Ransomware installieren.

Ransomware-Affiliates von LockBit zum Beispiel haben PowerShell dazu benutzt, schädlichen Code aus Google Tabellen herunterzuladen, und mit der Windows-Aufgabenplanung bösartige VBScripts ausgeführt. Affiliates von ALPHV haben die Windows-Aufgabenplanung ebenfalls verwendet und mit ihr bösartige Gruppenrichtlinienobjekte (GPO) konfiguriert. Und die Ransomware-Gruppe Royal hat den Volumeschattenkopie-Dienst von Windows zum Löschen von Snapshot-Backups benutzt und so Wiederherstellungsbemühungen behindert.

LOTL-Angriffe sind für viele Internetkriminelle äußerst attraktiv. Datendiebstahl- und Advanced-Persistent-Threat-(APT-)Gruppen können niemals zu Schadsoftware greifen und dennoch LOTL-Techniken nutzen, um jahrelang unerkannt zu bleiben, während Internetkriminelle jeglicher Art mit Remote-Zugriff-Tools wie RDP und AnyDesk ganz zufrieden sind, da diese eine enorme Kontrolle bieten, ohne weiter aufzufallen.

Um LOTL-Angriffe abwehren zu können, benötigen IT- und Sicherheitsteams ein genaues Verständnis ihrer Umgebung, damit sie Anomalien wie unbekannte Admin-Tools (bzw. bekannte Tools in unbekannten Händen), ungewöhnliche Datennutzungsmuster oder untypische Arbeitszeiten entdecken können.

„Für eine wirksame Erkennung von LOTL-Angriffen ist ein Verständnis der Umgebung außerordentlich wichtig. Bewaffnet mit diesen Ausgangsdaten, können Sicherheitsanalysten Anomalien oder Ausreißer erkennen, die an und für sich nicht bösartig, für die Umgebung jedoch ungewöhnlich sind.“

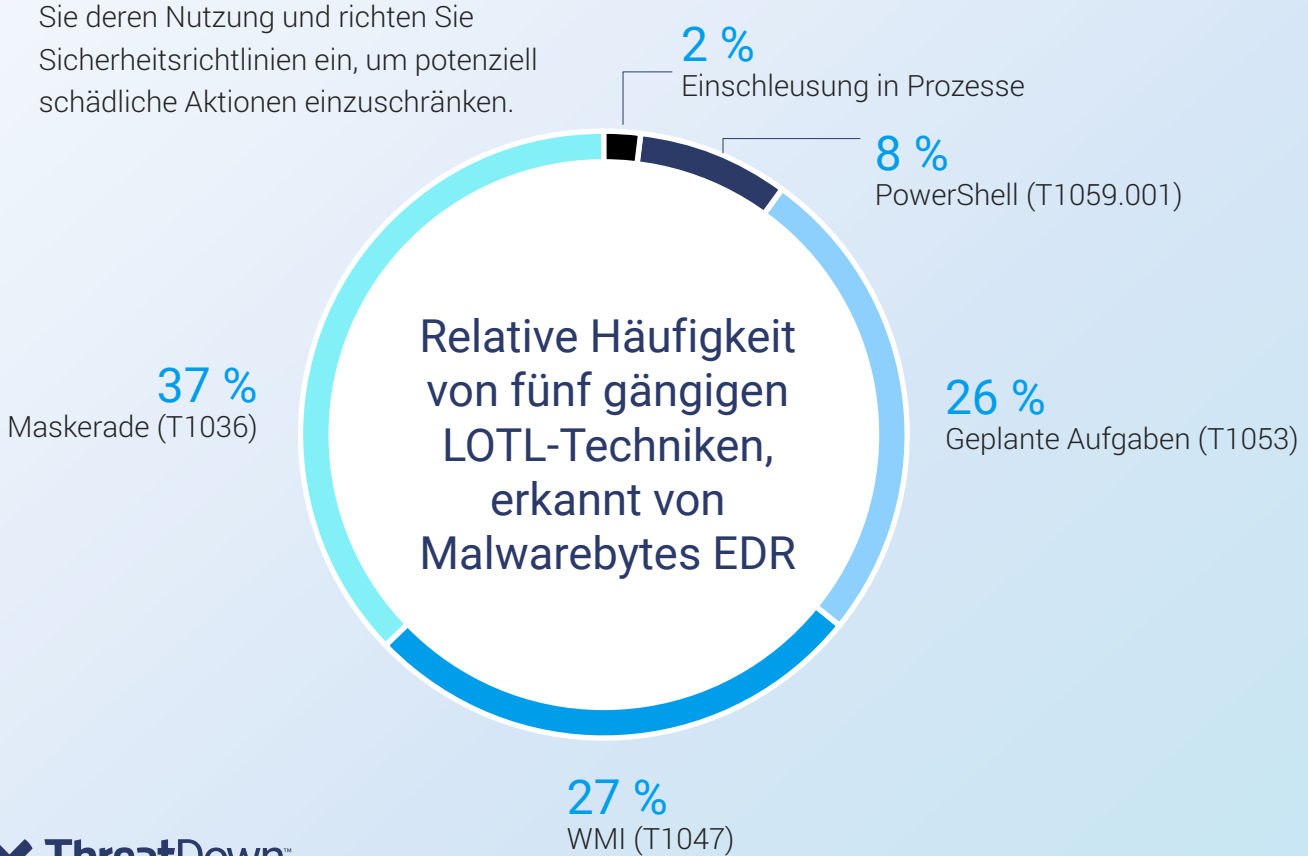
**Hiep Hinh**
Principal MDR Analyst, Malwarebytes

## Abwehr von LOTL-Angriffen

- **Nutzen Sie MDR**, damit menschliche Experten Ihre Endpunkte rund um die Uhr auf ungewöhnliche Muster, Anzeichen von Gefährdungen oder Verbindungen überwachen.
- **Nutzen Sie Threat-Intelligence-Feeds,** um Ihre Überwachung anhand von Informationen zu den neuesten Angriffstechniken und Gefährdungsindikatoren zu optimieren.
- **Führen Sie moderne Überwachungstools ein,** die speziell darauf ausgelegt sind, ungewöhnliches Benutzer- oder Systemverhalten zu erkennen.
- **Begrenzen Sie den Zugriff auf häufig missbrauchte Tools** auf Benutzer, die sie wirklich benötigen, überwachen Sie deren Nutzung und richten Sie Sicherheitsrichtlinien ein, um potenziell schädliche Aktionen einzuschränken.

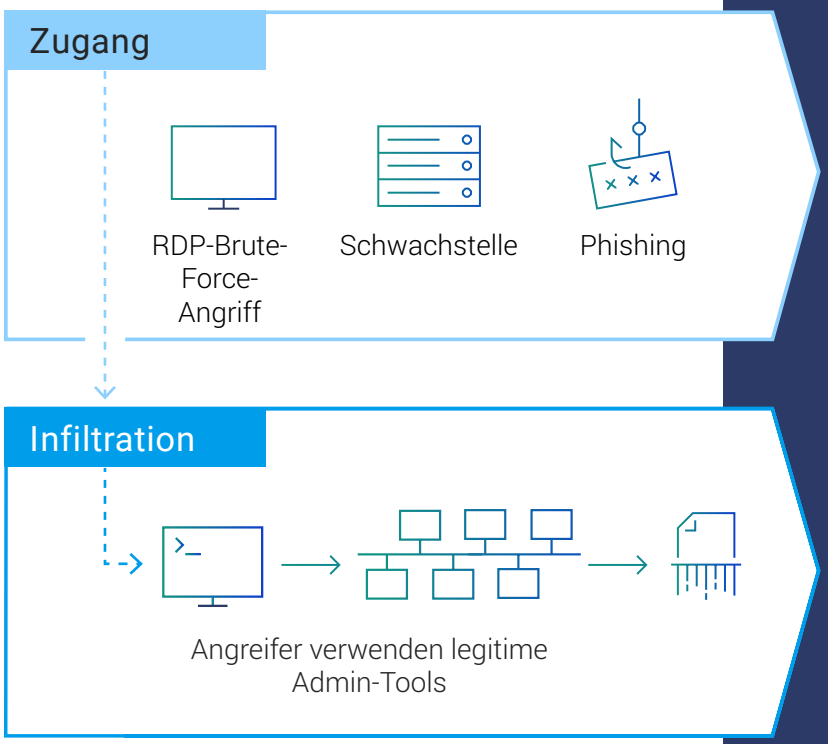
Angreifer lieben Remote-Desktop-Software. Um LOTL-Angriffe zu erschweren, deaktivieren Sie das Remote Desktop Protokoll (RDP) und blockieren Sie sämtliche Remote-Desktop-Tools, die Ihr Unternehmen in der Regel nicht verwendet wie Anydesk, Dameware Mini Remote und Splashtop.

Bei einem LOTL-Angriff, der vom MDR-Team von Malwarebytes gestoppt wurde, verwendeten Internetkriminelle eine ganze Reihe von legitimen Tools, um der Erkennung zu entgehen. Sie nutzten wscript, um eine Windows-Skriptdatei (WSF) auszuführen, mit der ein PowerShell-Skript ausgeführt wurde, das bösartige Dateien herunterlud, die wiederum von rundll32 ausgeführt wurden.



Internetkriminelle, die auf LOTL-Techniken setzen, nutzen legitime IT-Admin-Tools statt Schadsoftware und sind daher nur äußerst schwierig zu entdecken. Für eine Abwehr von Living-off-the-Land-Angriffen braucht es erfahrene Bedrohungsjäger, die mit einer branchenführenden EDR-Lösung in Ihrem Netzwerk nach verdächtigen Aktivitäten suchen und diesen nachgehen.

## Phasen eines Living-off-the-Land-Angriffs




## Schutz durch ThreatDown

Brute-Force-Schutz, Vulnerability Assessment, Patch Management, Anti-Exploit-Schutz sowie Filterung von Website-Inhalten verhindern verschiedene Arten des Zugriffs.

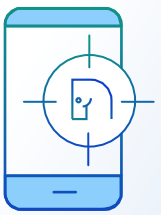
Managed Detection & Response (MDR) identifiziert und untersucht verdächtiges Verhalten in Ihrem Netzwerk; ein App-Blocker verweigert Angreifern Zugriff auf ihre Tools; eine Filterung von Website-Inhalten blockiert Angreifern den Zugriff auf Command-and-Control-Server.

# 7. Android-Banking-Trojaner

Banking-Trojaner stellen eine der größten Bedrohungen für Android-Geräte dar. Raffiniert und gut getarnt, kombinieren sie clevere technische Taktiken mit Social Engineering, um Benutzer zu täuschen, die Schutzfunktionen von Google Play zu umgehen und Geld direkt aus den Bankkonten von Benutzern zu stehlen.

Banking-Trojaner geben sich als reguläre Apps aus wie QR-Code-Scanner, Fitnesstracker und beliebte Anwendungen wie Instagram. Nach ihrer Installation können die Apps ihre Umgebung testen, um sicherzugehen, dass sie sich auf einem echten Gerät und nicht im Labor eines Forschers befinden. Sie können nach einer SIM-Karte suchen oder sicherstellen, dass sie nicht auf einem gerooteten Gerät oder in einem Emulator laufen. Werden die Bedingungen des Banking-Trojaners erfüllt, wird von ihm eine zweite, bösartige App installiert.

Die Schadstoffware kann überprüfen, ob sie auf einem gerooteten Gerät oder in einer emulierten Umgebung läuft, ob eine SIM-Karte vorhanden ist, sowie weitere Umgebungstests vornehmen, um einem Reverse Engineering zu entgehen. Sie kann auch für einige Zeit inaktiv bleiben, bevor sie mit einem Update bösartigen Code herunterlädt und auf diese Weise versucht, die Sicherheitschecks von Google Play Protect zu umgehen.



**88.500**

Malwarebytes erkannte im Jahr 2023 88.500 Android-Banking-Trojaner.

**72 %**

aller Smartphones laufen mit Android, kein Betriebssystem ist weiter verbreitet, noch nicht einmal Windows.

Einige Trojaner tun dies, indem sie die App von einem externen Server herunterladen. Um netzwerkbasierte Erkennungssysteme zu umgehen, können sie dazu eine legitime Hosting-Plattform wie das Content Delivery Network (CDN) von Discord verwenden.

Andere Trojaner sind sogenannte Dropper, die die zweite App bereits enthalten. Drittanbieter-Dienste wie Zombinder nutzen einen komplizierten Bindemechanismus, um eine bösartige Payload in einer harmlosen Hostanwendung zu verstecken.

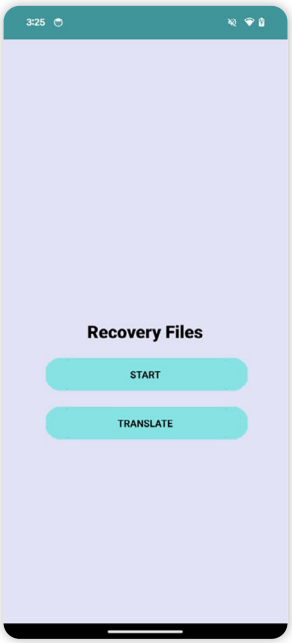
Die bösartige App wird unerkannt auf dem Zielgerät installiert und tarnt sich typischerweise hinter einem leeren Symbol und einem leeren Eintrag, wenn ein Benutzer versucht, die App-Infos zu lesen.

Nach ihrer Installation fordert die bösartige App den Benutzer unter dem Vorwand der Verbesserung der Anwendungsfunktionalität auf, Zugriff auf die Bedienungshilfen zu gewähren. Dies ermöglicht ihr, andere Apps zu überwachen und gefälschte Benutzeroberflächen über sie zu legen. Mit diesen Overlays werden personenbezogene Daten wie Kennwörter erfasst.

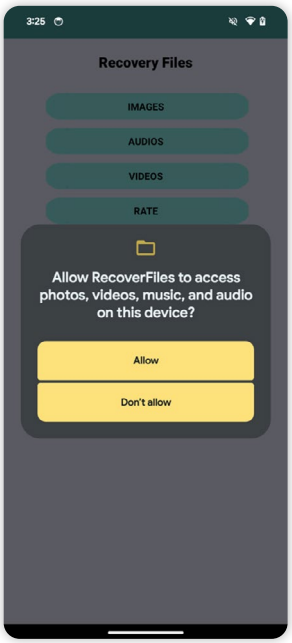
Die App richtet zudem einen verborgenen Abfangmechanismen ein, um unbemerkt vom Benutzer Token für die Multi-Faktor Authentifizierung (MFA) aus Textnachrichten zu erfassen.

Sobald sie die Berechtigung für die Bedienungshilfen erhalten hat, initialisiert die Schadsoftware ihr Automated-Transfer-System-(ATS-)Framework, eine komplexe Reihe von Skripten und Befehlen, die speziell dafür entwickelt wurden, ohne Benutzereingriff automatisierte Banktransaktionen abzuwickeln.

Das ATS-Framework nutzt die abgegriffenen Anmeldeinformationen dazu, nicht autorisierte Überweisungen an Konten der Angreifer zu veranlassen. Dies imitiert echtes Benutzerverhalten, sodass Betrugserkennungssysteme umgangen werden.

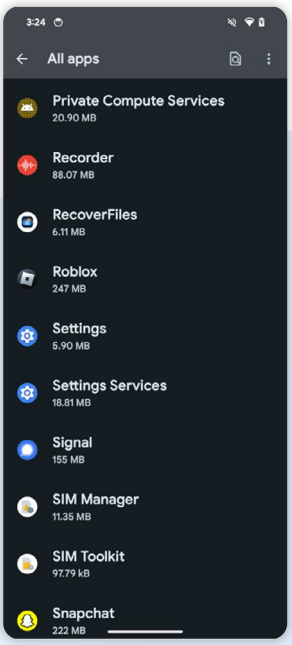



Der Startbildschirm eines Banking-Trojaners, versteckt in einer Dateiwiederherstellungs-App.

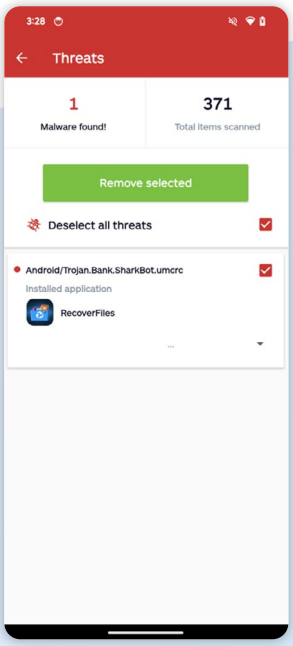



Die App fragt nach der Berechtigung zum Zugreifen auf Dateien, zum Datenaustausch mit anderen Apps sowie zum Senden von Zahlungen via Google Play.


Sie verfügt nach der Installation über kein Symbol.




In der App-Liste wird die App jedoch aufgeführt.



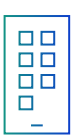

Malwarebytes erkennt die App als den Banking-Trojaner SharkBot.

Banking-Trojaner sind raffinierte, heimtückische Bedrohungen, die sich hinter voll funktionsfähigen, regulären Apps verstecken. Sie kopieren Online-Banking-Kennwörter und nutzen diese, um im Verborgenen Geld direkt aus Bankkonten zu stehlen. Um sich gegen Banking-Trojaner zu schützen, ist ein branchenführender mobiler Schutz erforderlich, der Schadsoftware auf Android-Geräten erkennen und entfernen kann.

## Phasen eines Banking-Trojaner-Angriffs

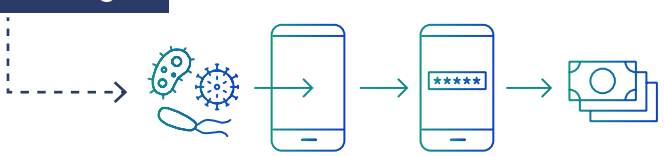
### Installation


### Infektion



Ein Banking-Trojaner wird versteckt in einer regulären App heruntergeladen.

### Verbreitung




Sobald er installiert wurde, führt er eine zweite, bösartige App aus. Diese App stiehlt Online-Banking-Kennwörter und führt betrügerische Transaktionen durch.

## Schutz durch ThreatDown

Mobile Security erkennt und entfernt Banking-Trojaner und andere Android-Schadsoftware.

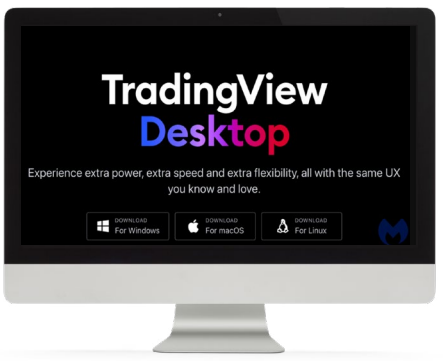
# 8. Neue Mac-Schadsoftware-Taktiken

Entgegen früheren Ansichten hat es schon immer Schadsoftware für Macs gegeben. Macs werden nur von anderen Arten von Erkennungen heimgesucht. Internetkriminelle stützen sich bei Macs nicht so sehr auf Ransomware, sondern bevorzugen aggressive, unerwünschte Adware, um sich auf der Plattform zu bereichern. Mac-Schadsoftware entwickelte 2023 eine Reihe von Taktiken, die uns in Erinnerung rufen: Es gibt keinen „Apple-Zauber“, der verhindert, dass die bösartigen Tools und Taktiken, die bei Windowsfunktionieren, auch bei Macs erfolgreich sein können.

Die Internetkriminalität folgt dem Geld und Windows-Heimcomputer – sowie Netzwerke aus Windows-Bürorechnern – waren in der Vergangenheit ein sehr viel größeres, verbundeneres und lukrativeres Ziel für Internetkriminelle. Vieles spricht jedoch dafür, dass sich dies ändert. Die Nachfrage nach Macs wächst trotz abnehmender PC-Verkäufe. Das Betriebssystem macOS von Apple erreicht in den USA mit seinen vielen Varianten mittlerweile einen Anteil von 31 % unter den Desktop-Betriebssystemen, und ein Viertel aller Unternehmen betreibt irgendwo in ihrem Netzwerk auch Macs.

**11%**

Schadsoftware machte im Jahr 2023 11 % aller Erkennungen auf Macs aus.




**Eine Malvertising-Website bietet Schadsoftware-Downloads für Windows, Mac und Linux.**

Es gibt Anzeichen dafür, dass Kriminelle dies zur Kenntnis genommen haben und sich auf die zunehmende Beliebtheit der Plattform einstellen, indem sie ihre Angriffsketten um Optionen für Mac erweitern und Angriffe gleichzeitig auf Windows- und Mac-Benutzer ermöglichen.

Im September entdeckte Malwarebytes eine Kampagne von Internetkriminellen, die die Schadsoftware Atomic Stealer (AMOS) unter Mac-Benutzern über bösartige Anzeigen verbreitete, die vorgaben, die Finanz-App TradingView zu verkaufen.

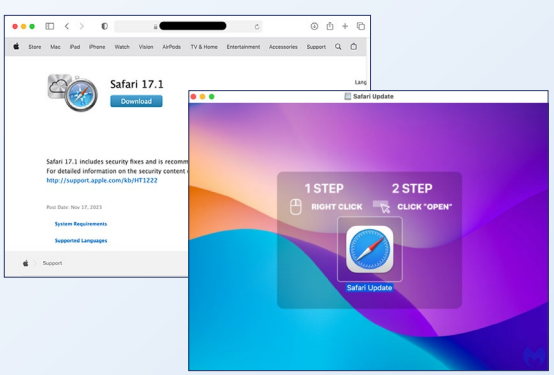
Die bösartige Anzeige leitete Opfer zu einer glaubwürdig wirkenden Köder-Website mit dem Markenzeichen von TradingView und getrennten Download-Schaltflächen für Windows, Mac und Linux. Windows- und Linux-Benutzer machten Bekanntschaft mit dem Fernzugriffstrojaner NetSupport RAT, Mac-Benutzer dagegen mit Atomic Stealer.

AMOS ist ein Infostealer für Mac, der Kennwörter, Browser-Daten, Cookies, Dateien und Kryptowährungen abgreifen kann. Kampagnen von Internetkriminellen, die AMOS nutzen, können den Infostealer über eine webbasierte Verwaltungskonsole steuern, die als „Dienstleistung“ (ähnlich wie legitime Cloud-Anwendungen) für 1000 US-Dollar (921 Euro) pro Monat verkauft wird.

Im November wurde entdeckt, dass eine gefälschte Browser-Update-Kette namens ClearFake ebenfalls AMOS verbreitet. ClearFake nutzt kompromittierte Websites, um Benutzer zum Herunterladen von Schadsoftware zu verleiten, die sich als Browser-Sicherheitsupdate ausgibt.

Die Kampagnen-Infrastruktur ermittelt, welchen Browser das Opfer benutzt, sodass das jeweils passende Update angezeigt wird. Gefälschte Browser-Updates zielen in der Regel auf Windows-Benutzer. Das Auftauchen von auf Safari zielenden Websites zum Verbreiten von Schadsoftware für macOS ist eine neue Entwicklung.

Die Zusatzkosten, die durch das Hinzufügen einer macOS-Option zu einer etablierten Verteilungskette für Windows-Schadsoftware anfallen, sind gering. Wenn Mac sich auch 2024 dem Trend fallender PC-Verkäufe widersetzt, wird es Internetkriminellen zunehmend leichter fallen, sich für Kampagnen gegen die Plattform zu entscheiden.




**Ein gefälschtes Safari-Update imitiert die offizielle Apple-Website und ist sogar in verschiedenen Sprachen verfügbar.**

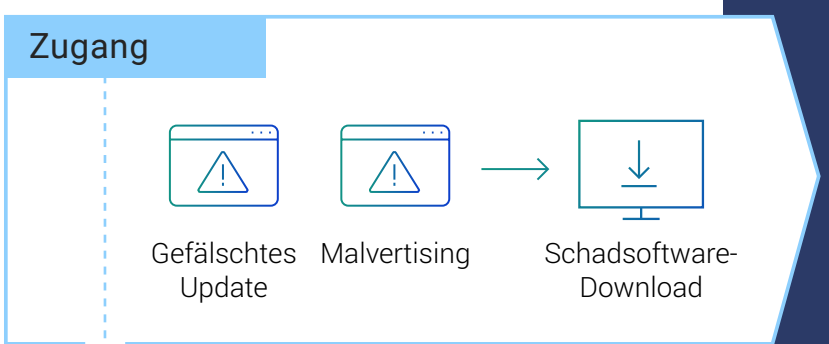
LOCKBIT 3.0

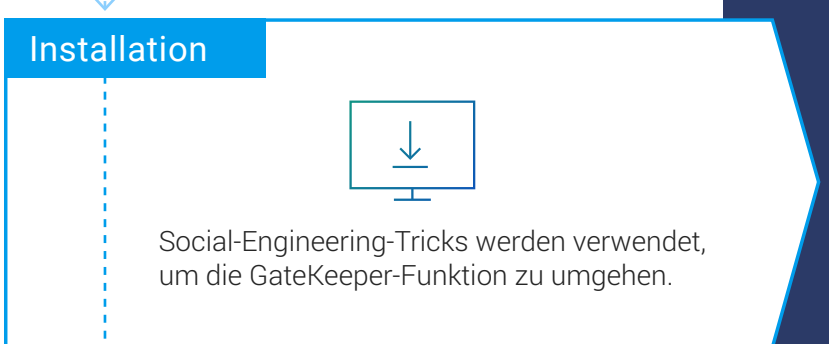
Im April stolperten Forscher über eine Mac-Version von LockBit, der weltweit gefährlichsten Ransomware. Obwohl sich das Tool im Versuchsstadium befand, meldete die Ransomware-Gruppe LockBit, dass sie dabei sei, ihre Mac-Ransomware „aktiv zu entwickeln“.

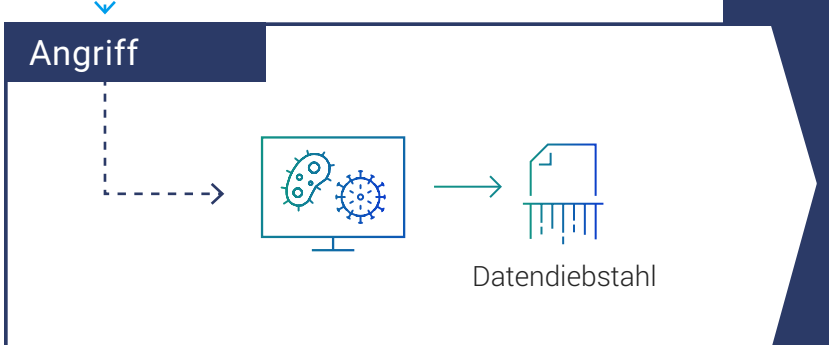

Erkennungen unter macOS im Jahr 2023
4 %
PUP.JDI
4 %
Adware.NewTab
5 %
PUP.PCVARK
5 %
PUP.MacKeeper
6 %
Adware.Crossrider
11%
Schadsoftware-Erkennungen
11%
OSX.VSearch
11%
OSX.Genieo
13 %
Adware.
30 %
Sonstige

Macs werden immer beliebter und Internetkriminelle fügen ihren Malvertising- und gefälschten Browser-Update-Kampagnen Optionen für Macs wie den Atomic Stealer hinzu. Die Abwehr von Mac-Schadsoftware erfordert ein Antivirusprogramm der nächsten Generation, das in der Lage ist, Mac-Schadsoftware zu erkennen.

## Phasen eines Atomic-Stealer-Angriffs




## Schutz durch ThreatDown

Eine Filterung von Website-Inhalten kann Websites, die für Malvertising und gefälschte Updates verwendet werden, blockieren.

Ein Antivirusprogramm der nächsten Generation kann Mac-Schadsoftware stoppen.

# 9. Wie Sie sich vorbereiten

Laut Mark Twain wiederholt sich die Geschichte zwar nicht, aber sie reimt sich. Das sich seit Jahrzehnten hartnäckig wiederholende Muster in der Cybersicherheit ist, dass sich Bedrohungen häufig von der Ausnutzung von Software-Schwachstellen hin zur Ausnutzung menschlicher Schwächen weiterentwickeln.

In dieser Zeit hat die Cybersicherheit vor allem viel Mühe darauf verwandt, ersteres anzugehen. Schließlich können Technologien und die Prozesse, durch die sie hervorgebracht werden, auf eine Weise verbessert werden, wie es bei Menschen nicht möglich ist. Mit Hingabe und Ausdauer können Systeme langsam sicherer gemacht werden – können Erkennungsfähigkeiten verbessert, Angriffsflächen verringert, Testmöglichkeiten erweitert und Updates häufiger durchgeführt werden – sodass das Zeitfenster für die technische Ausnutzung geschlossen wird.

Und dennoch ist es genau dieses Muster, das im Bereich der Internetkriminalität Innovation vorantreibt.

Verbesserungen bei der Webbrowser-Sicherheit führten dazu, dass die routinemäßige Ausnutzung von Browsern und Plugins zugunsten von Social-Engineering-Angriffen wie gefälschten Updates und Malvertising verschwand.

Ransomware ist zu einer milliardenschweren Branche geworden, indem sie von automatisierten E-Mail-Kampagnen auf manuelle Big-Game-Angriffe umgestiegen ist, bei denen kriminelle Hacker den Kampf direkt mit IT- und Sicherheitsmitarbeitern aufnehmen.

Verbesserungen bei Backups und der Erkennung hat eine zunehmende Anzahl von Ransomware-Banden dazu veranlasst, ihre bösartige Verschlüsselung um die Androhung der Veröffentlichung der gestohlenen Daten zu ergänzen – ein menschliches Dilemma, das keine Software lösen kann. Es hat ebenso die Einführung von Living-off-the-Land-(LOTL-) Techniken angetrieben, die von Software ohne menschliche Hilfe nur schwer zu erkennen ist.

Diese Entwicklung hat dazu geführt, dass Menschen eine zunehmend wichtige Rolle bei der Bedrohungserkennung spielen. Ganz gleich, wie groß Ihr Unternehmen ist – wie erfolgreich Sie 2024 dabei sein werden, die gefährlichsten Cyberbedrohungen auszuschalten, hängt entscheidend davon ab, wie Sie es schaffen, modernste Sicherheitssoftware mit erfahrenen Sicherheitsmitarbeitern zusammenbringen.

# 10. Wir stellen vor: ThreatDown-Pakete

ThreatDown geht die heutigen Herausforderungen im Bereich Cybersicherheit mit den preisgekrönten Technologien und Diensten von Malwarebytes an, die Schutz über den gesamten Angriffszyklus bieten: von der Reduzierung der Angriffsfläche, über die Prävention, Erkennung und Reaktion bis hin zur vollständigen Beseitigung.

## ThreatDown Core

**Core** liefert umfassende Prävention gegen Schadsoftware, Zero-Day-Bedrohungen und mehr. **Die Lösung** umfasst preisgekrönte Technologien, die die Verwaltung der Endpunktsicherheit spürbar vereinfachen.

## ThreatDown Advanced

**Advanced** bietet erstklassigen Schutz in einer einzigen, benutzerfreundlichen Lösung zu einem vernünftigen Preis. Für Unternehmen mit kleinen Sicherheitsteams und begrenzten Ressourcen entwickelt, umfasst **Advanced** preisgekrönte Technologien, die die Verwaltung des Endpunktschutzes deutlich vereinfachen.

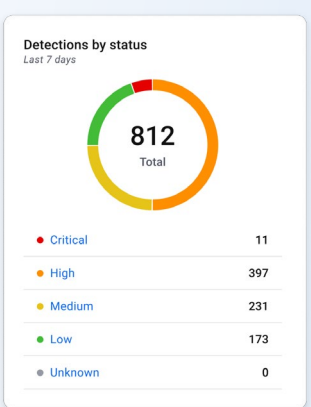
## ThreatDown Elite

**Elite** bietet umfassenden Schutz in einer einzigen Lösung und unvergleichliche Benutzerfreundlichkeit zu einem vernünftigen Preis. **Elite** wurde speziell für Unternehmen mit kleinen (bzw. gar keinen) Sicherheitsteams entwickelt, die nicht über die Ressourcen verfügen, um alle Sicherheitswarnungen zu bearbeiten. Es umfasst preisgekrönte Technologien sowie 24x7x365 Überwachung und Reaktion durch Sicherheitsexperten.

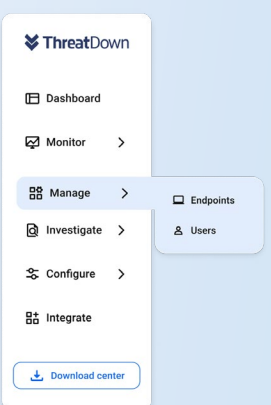
## ThreatDown Ultimate

**Ultimate** liefert den umfassendsten Schutz über den gesamten Angriffszyklus: von einer überlegenen Reduzierung der Angriffsfläche bis hin zu einer komplett verwalteten 24x7x365 Prävention, Erkennung, Reaktion und vollständigen Bereinigung.

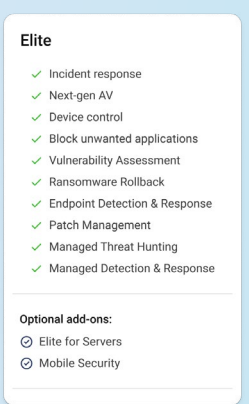
**Bedrohungen beseitigen.**




**Komplexität beseitigen.**




**Kosten beseitigen.**



# Wir verstehen – Sicherheit ist schwierig. Sicherheitsprodukte sollten es nicht sein.

Ein Überblick über die Fähigkeiten unserer einzelnen ThreatDown-Pakete, die sechs kritischen Cyberbedrohungen anzugehen.

| Was Sie erhalten | Core | Advanced | Elite | Ultimate |
|---|---|---|---|---|
| Incident Response | ✓ | ✓ | ✓ | ✓ |
| Neuestes Antivirus | ✓ | ✓ | ✓ | ✓ |
| Gerätesteuerung | ✓ | ✓ | ✓ | ✓ |
| Blockierung unerwünschter Anwendungen | ✓ | ✓ | ✓ | ✓ |
| Vulnerability Assessment | ✓ | ✓ | ✓ | ✓ |
| Ransomware-Rollback | | ✓ | ✓ | ✓ |
| Endpoint Detection & Response | | ✓ | ✓ | ✓ |
| Patch Management | | ✓ | ✓ | ✓ |
| Managed Threat Hunting | | ✓ | | |
| Managed Detection & Response (includes threat hunting) | | | ✓ | ✓ |
| Filterung von Website-Inhalten | | | | ✓ |
| Add-ons | ✓ | ✓ | ✓ | ✓ |

## Testen Sie noch heute unsere ThreatDown-Pakete!

Überlassen Sie uns Ihre Endpunktsicherheit. Setzen Sie auf die Lösung, die eine überragende Angriffsabwehr, die benutzerfreundlichste Verwaltung und die beste Leistung für Ihre Sicherheitsinvestition bietet.

**Los geht's**

ThreatDown™ Powered by Malwarebytes

ThreatDown™
Powered by Malwarebytes

One Albert Quay, 2nd Floor
Cork, Irland
+1-800-520-2796