zscaler™ | ThreatLabz

ThreatLabz–Report 2022 zur aktuellen Ransomware–Lage

Inhalt

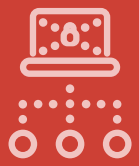
Einführung

Beinahe täglich liest man neue Schlagzeilen zu Ransomware–Angriffen. Leider kann man dies aber nicht damit abtun, dass sich reißerische Artikel gut verkaufen: Das ThreatLabz–Team von Zscaler hat für den Zeitraum zwischen Februar 2021 und März 2022 einen Anstieg der Anzahl der Ransomware–Angriffe gegenüber dem Vorjahr um weitere 80 % festgestellt — ein trauriger Rekord, der zudem nie dagewesene Schäden mit sich brachte.

Die Mehrzahl der erfolgreichen und zunehmend lukrativen Angriffskampagnen lässt sich drei wichtigen Trends zuordnen:

Supply-Chain-Angriffe unter Ausnutzung von Geschäftsbeziehungen zu vertrauenswürdigen Anbietern. Diese Angriffe zeichnen sich durch ein besonders hohes Schadenspotenzial aus, da sie sich häufig gegen Dutzende (teilweise auch Hunderte oder gar Tausende) von Organisationen auf einmal richten.

Ransomware-as-a-Service bezieht sich auf die massenhafte Verbreitung von Ransomware über Affiliate-Netzwerke. Hacker, die auf unbefugte Netzwerkzugriffe spezialisiert sind, arbeiten dabei Hand in Hand mit etablierten Ransomware-Gruppen und erhalten einen bestimmten Anteil der Gewinne.



Angriffe mit mehrfacher Erpressung, bei denen mehrere Taktiken wie Datendiebstahl, Distributed Denial of Service (DDoS), Kommunikation mit Kunden usw. zum Einsatz kommen, um möglichst hohe Lösegelder einzustreichen.

Diese Taktiken können großen Schaden anrichten. Branchenexperten prognostizieren, dass Ransomware die Vorgehensweise sein wird, die im Jahr 2022 am häufigsten bei Sicherheitsverletzungen durch externe User und Supply-Chain-Angriffen zum Einsatz kommt, und dass die weltweiten Kosten für Ransomware-Schäden bis 2024 auf 42 Milliarden US-Dollar ansteigen werden.

Diese Trends haben dafür gesorgt, dass Ransomware auf der Liste der Cybersicherheitsprobleme für Unternehmen aller Branchen ganz weit oben steht. Im Report „CISOs im Brennpunkt“ hat Aimpoint 2022 festgestellt, dass CISOs weltweit Ransomware für die größte Bedrohung für ihre Unternehmen halten.

Wie kann man also die die neuesten Ransomware-Varianten erkennen und sich vor ihnen schützen? In diesem Report finden Unternehmen alle nötigen Informationen.

ThreatLabz analysiert Daten aus über 200 Milliarden täglichen Transaktionen und 150 Millionen blockierten Angriffen pro Tag in der gesamten Zscaler Zero Trust Exchange in Verbindung mit Bedrohungsinformationen von Zscaler ThreatLabz, um die am weitesten verbreiteten Bedrohungsarten zu bestimmen, neue Trends zu identifizieren und den Schutz für Zscaler-Kunden zu verbessern. Im Rahmen dieses Reports untersuchte ThreatLabz Ransomware-Daten vom 1. Februar 2021 bis zum 31. März 2022, um die aktivsten Ransomware-Familien und die zugehörigen Taktiken zu ermitteln. Die daraus resultierenden Erkenntnisse, Prognosen und Empfehlungen sind in diesem Report zusammengefasst, um die Entwicklung optimaler Ransomware-Strategien zu unterstützen.

Haupterkenntnisse

Die Häufigkeit von Ransomware-Angriffen nahm im Vergleich zum Vorjahr um 80 % zu, wie die Analyse aller in der Zscaler-Cloud beobachteten Ransomware-Payloads ergab.

Bei Ransomware-Angriffen mit Doppelerpressung wurde ein Zuwachs um 117 % verzeichnet, was darauf hindeutet, dass immer mehr Strategien auf Datendiebstahl ausgelegt sind. Besonders stark betroffen waren hier die Branchen Gesundheitswesen (+643 %), Gastronomie (+460 %), Bergbau (+229 %), Bildungswesen (+225 %), Medien (+200 %) und Fertigung (+190 %).

Knapp 20 % der Angriffe mit Doppelerpressung entfielen auf die Fertigung, die damit wie bereits im Vorjahr wieder die Liste der am stärksten betroffenen Branchen anführte.

Supply-Chain-Angriffe im Allgemeinen — und solche, bei denen Ransomware eingesetzt wird, im Besonderen — sind auf dem Vormarsch. Durch Ausnutzen der Geschäftsbeziehungen potenzieller Opfer zu vertrauenswürdigen Zulieferern gelingt es Ransomware-Angreifern, Dutzende von Organisationen mit einem Schlag zu treffen — einschließlich solcher, die über robuste Schutzmechanismen zur Abwehr externer Angreifer verfügen. Im vergangenen Jahr machten mehrere groß angelegte Supply-Chain-Angriffe u. a. auf Kaseya und Quanta Schlagzeilen. Teilweise nutzten Angreifer dabei die Log4j-Schwachstelle aus.

Ransomware-as-a-Service greift zunehmend um sich. Der Trend zur Zusammenarbeit zwischen Ransomware-Gruppen und kriminellen Partnern, die sich auf unbefugte Netzwerkzugriffe spezialisieren, hält weiter an. Für einen Anteil an den Gewinnen (in der Regel rund 80 % des erbeuteten Lösegelds) verschaffen diese Hacker sich im Gegenzug Zugriff auf die IT-Umgebungen großer Organisationen und implementieren den von der Ransomware-Gruppe bereitgestellten Schadcode. Im vergangenen Jahr wurde die Mehrzahl der aktivsten Ransomware-Typen (8 von insgesamt 11) primär über derartige RaaS-Modelle verbreitet.

Die Strafverfolgungsbehörden greifen härter durch. Insbesondere Ransomware-Gruppen, die es auf systemrelevante Sektoren abgesehen hatten, standen im vergangenen Jahr weltweit im Visier der Strafverfolgungsbehörden. So wurden 2021 Vermögenswerte von REvil (verantwortlich für die Angriffe auf Kaseya und JSB), DarkSide (verantwortlich für den Angriff auf Colonial Pipeline) und Egregor (eine neue Variante von Maze, der verbreitetsten Ransomware-Familie des letzten Jahres) beschlagnahmt.

Ransomware-Gruppen verschwinden nicht, sondern treten unter neuen Namen auf. Auf den zunehmenden Druck seitens der Strafverfolgungsbehörden haben viele Ransomware-Gruppen mit einem Rebranding reagiert, d. h. sie treten unter neuen Namen auf, wenden aber weiterhin die gleichen (bzw. sehr ähnliche) Taktiken an. Aus DarkSide wurde BlackMatter, DoppelPaymer wurde zu Grief und Avaddon zu Haron und Midas. So benennt auch die von der US-Regierung sanktionierte Gruppe Evil Corp ihre Ransomware-Operationen immer wieder um.

Ukraine-Konflikt: Weltweit herrscht Alarmstufe Rot. Im direkten Zusammenhang mit dem Krieg in der Ukraine wurden bereits verschiedene Angriffskampagnen verzeichnet, bei denen teilweise eine Kombination aus mehreren Taktiken eingesetzt wurde (z. B. HermeticWiper und PartyTicket-Ransomware). Bisher richteten sich diese Aktivitäten primär gegen Ziele in der Ukraine; Regierungsbehörden warnen jedoch vor einer Zunahme der Angriffe auf ausländische Organisationen im weiteren Verlauf des Konflikts.

Zero Trust ist und bleibt die beste Verteidigungsstrategie. Die beste Chance auf Minderung des Risikos von Sicherheitsverletzungen und Schadensbegrenzung im Fall eines erfolgreichen Angriffs bieten sogenannte Defense-in-Depth-Strategien. Dazu gehören Maßnahmen zur Verkleinerung der Angriffsfläche, Zugriffskontrollen nach dem Prinzip der minimalen Rechtevergabe sowie die kontinuierliche Überwachung der gesamten IT-Umgebung mit Überprüfung sämtlicher Daten.

Die Entwicklung von Ransomware

Ransomware ist eine Art von Malware, mit der Cyberkriminelle aktiv auf die Störung des Unternehmensbetriebs abzielen. Bei Ransomware-Angriffen werden geschäftskritische Dateien in unlesbarer Form verschlüsselt. Die Angreifer fordern dann ein Lösegeld für die Entschlüsselung der Dateien. Die Höhe der Lösegeldforderungen hängt von der Anzahl der infizierten Systeme und dem Wert der verschlüsselten Daten ab. Grundsätzlich gilt: Je mehr für das Unternehmen auf dem Spiel steht, desto mehr Geld wird verlangt.

Ende 2019 wurde eine Weiterentwicklung der Ransomware-Taktiken in Form von Datenexfiltration beobachtet, was üblicherweise als Ransomware-Angriff mit Doppelerpressung bezeichnet wird. Wenn Opfer solcher Angriffe sich weigern, das Lösegeld für die Entschlüsselung zu zahlen, und stattdessen versuchen, die Daten anhand von Sicherungskopien wiederherzustellen, drohen die Angreifer mit der Offenlegung der gestohlenen Daten. Seit Ende 2020 kommt es auch immer wieder vor, dass Angreifer die Website oder das Netzwerk des Opfers mit DDoS-Attacken bombardieren. Dadurch soll der Geschäftsbetrieb noch stärker beeinträchtigt und das Opfer so zu Verhandlungen gezwungen werden.

2021 und zu Beginn des Jahres 2022 stellen Supply-Chain-Angriffe den schädlichsten Ransomware-Trend dar. Bei diesen bildet ein erfolgreicher Angriff auf einen Anbieter (meist ein Software- oder anderer Technologie-Anbieter) die Grundlage für Angriffe auf Unternehmen, die auf dessen Produkte angewiesen sind, in der zweiten Phase. Schätzungen zufolge kam es in der zweiten Hälfte des Jahres 2021 zu 51 % mehr Supply-Chain-Angriffen. Cyberkriminelle haben durch Exploits beliebter Softwareprodukte wie SolarWinds, Kaseya und Log4j für Aufregung gesorgt und es ist davon auszugehen, dass sich dieser Trend in den kommenden Jahren noch verstärken wird.

Verlauf von Ransomware-Angriffen

Die heutigen Ransomware-Angriffe verlaufen in der Regel in den folgenden Phasen:

1. **Erstzugriff:** Angreifer nutzen eine Vielzahl von Einfallsvektoren, um sich Zugriff auf Systeme zu verschaffen. Dazu gehören Phishing-E-Mails, das Ausnutzen von Schwachstellen in Remote- oder VPN-Tools (Virtual Private Network) sowie die Verwendung von Brute-Force-Tools oder gestohlenen Anmeldedaten, um auf RDP-Verbindungen (Remotedesktopprotokoll) zuzugreifen. Supply-Chain-Angriffe sind eine weitere Methode, um Organisationen zu infiltrieren.

2. **Laterale Ausbreitung:** Nach dem erfolgreichen Erstzugriff sammeln Angreifer Informationen über die Infrastruktur der Opfer und bewegen sich lateral zwischen den Netzwerksystemen, wobei sie bei Bedarf Zugriffsberechtigungen anpassen und Persistenzmechanismen einrichten. Währenddessen katalogisieren sie wichtige Daten, die gestohlen oder verschlüsselt werden sollen, und platzieren Payloads, die später ausgeführt werden.

3. **Datenexfiltration:** Im Falle eines Angriffs mit Doppelerpressung stehlen Angreifer im nächsten Schritt vertrauliche Daten als zusätzliches Druckmittel, damit sie ein höheres Lösegeld fordern können. Dadurch verringert sich der Handlungsspielraum der Opfer deutlich: Selbst wenn sie die verschlüsselten Daten aus Backups wiederherstellen können, müssen sie sich immer noch mit der Drohung der Angreifer auseinandersetzen, die gestohlenen Daten offenzulegen.

4. **Ausführung der Ransomware:** Als Nächstes implementieren Angreifer die Ransomware und führen sie aus, wodurch die Zieldateien auf allen Systemen, die mit dem Netzwerk verbunden sind, verschlüsselt werden. Im Regelfall beendet die Ransomware laufende Prozesse im Zusammenhang mit Sicherheitssoftware und Datenbanken, damit eine möglichst hohe Anzahl von Dateien verschlüsselt werden kann. Um die Wiederherstellung der Dateien zu behindern, werden Schattenkopien zumeist ebenfalls aus dem System gelöscht. Einige Ransomware-Familien starten das kompromittierte System auch im abgesicherten Modus von Windows neu, um Software zur Endgerätesicherheit vor der Dateiverschlüsselung zu umgehen. Nach der Dateiverschlüsselung erhalten die Opfer eine Lösegeldforderung, die Anweisungen zur Zahlung des Lösegelds und zur Entschlüsselung der Dateien enthält.

5. **DDoS:** Wenn das Opfer nicht verhandlungsbereit ist, verstärken manche Hackergruppen den Druck durch DDoS-Angriffe auf das Netzwerk oder die Website des Opfers, um den Geschäftsbetrieb noch stärker zu beeinträchtigen.

In Abbildung 1 wird die typische Abfolge von Angriffsphasen eines Ransomware-Angriffs mit Doppelerpressung dargestellt.

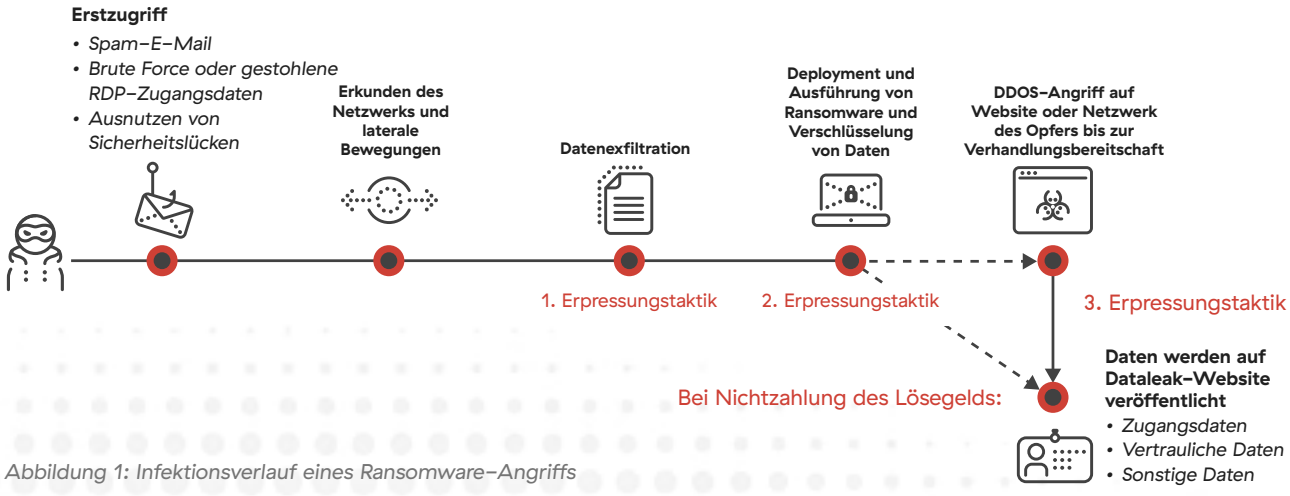


Abbildung 1: Infektionsverlauf eines Ransomware-Angriffs

Statistiken zu Ransomware-Angriffen in den Jahren 2021—2022

Die große Menge an Transaktionsdaten auf der Zero Trust Exchange verschafft einzigartige Einblicke in die Taktiken und Opfer der Cyberkriminellen. Von Februar 2021 bis März 2022 beobachtete ThreatLabz eine Zunahme der Ransomware-Payloads um 80 % im Vergleich zum Vorjahr. Darüber hinaus wurde anhand der Daten, die Cyberkriminelle auf ihren Dataleak-Websites veröffentlichen, festgestellt, dass die Anzahl der Opfer von Ransomware mit Doppelerpressung um 117 % gestiegen ist.

Von Ransomware betroffene Branchen

Das verarbeitende Gewerbe war bereits im Jahr 2020 die am häufigsten angegriffene Branche, auf die zwischen November 2019 und Januar 2021 12,7 % der Ransomware-Angriffe mit Doppelerpressung entfielen. In diesem Jahr stieg der Anteil der Angriffe auf Fertigungsunternehmen sogar noch weiter auf 19,5 %, gefolgt von Dienstleistungen (9,7 %), Bauwesen (8,1 %), Einzel- und Großhandel (7,5 %) sowie Hightech (6,7 %).

Ransomware-Infektionen nach Branche

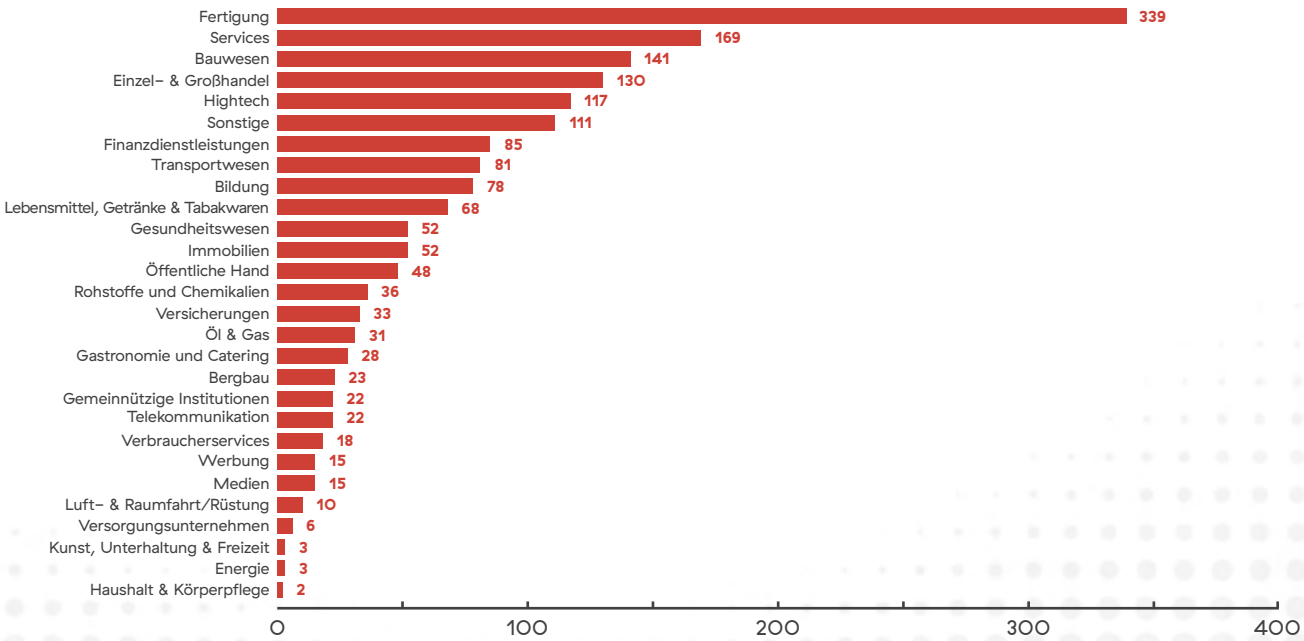


Abbildung 2: Ransomware-Infektionen nach Branche

Die Zunahme der Ransomware-Angriffe mit Doppelerpressung war je nach Branche sehr unterschiedlich. Im Report des letzten Jahres wurde festgestellt, dass die Zahl der Angriffe auf Einrichtungen des Gesundheitswesens besonders niedrig war. Grund dafür war die verstärkte Kontrolle durch Strafverfolgungsbehörden sowie die Zusicherung mehrerer bekannter Ransomware-Gruppen, das Gesundheitswesen während der COVID-19-Pandemie nicht ins Visier zu nehmen.

Die diesjährigen Daten sprechen jedoch eine andere Sprache. Im Jahr 2021 kam es zu 643 % mehr Angriffen auf Einrichtungen des Gesundheitswesens, obwohl die Gesamtzahl solcher Angriffe im Jahr 2020 noch sehr gering war. Mehrere weitere Branchen mit höheren Ausgangswerten verzeichneten ebenfalls eine Zunahme der Angriffe im dreistelligen Bereich, darunter das Bildungswesen (225 %), das verarbeitende Gewerbe (190 %), das Bauwesen (161 %), Finanzdienstleister (130 %) und Dienstleister (109 %).

Prozentuale Veränderung der Häufigkeit von Angriffen mit Doppelerpressung zwischen 2020 und 2021

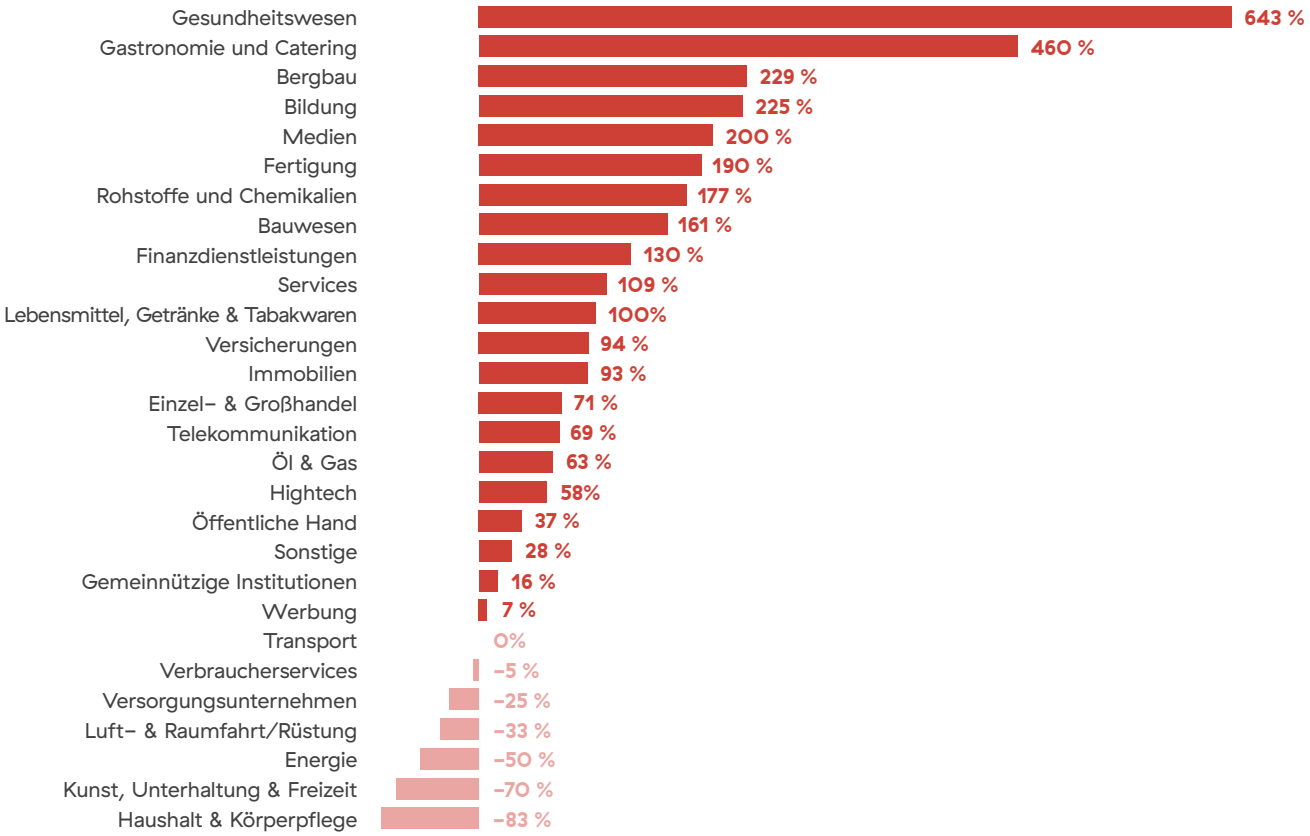


Abbildung 3: Prozentuale Veränderung der Häufigkeit von Angriffen mit Doppelerpressung nach Branche

Die aktivsten Ransomware-Gruppen

Conti und LockBit waren im Jahr 2021 die Ransomware-Gruppen, denen die meisten Angriffe mit Doppelerpressung zuzuschreiben waren. Allerdings gesellte sich im Laufe des Jahres eine Reihe von Neueinsteigern dazu.

In Abbildung 4 ist dargestellt, wann die aktivsten Ransomware-Gruppen der letzten Jahre erstmals in Erscheinung traten und damit begannen, Daten auf Dataleak-Websites oder in Hackerforen zu veröffentlichen.

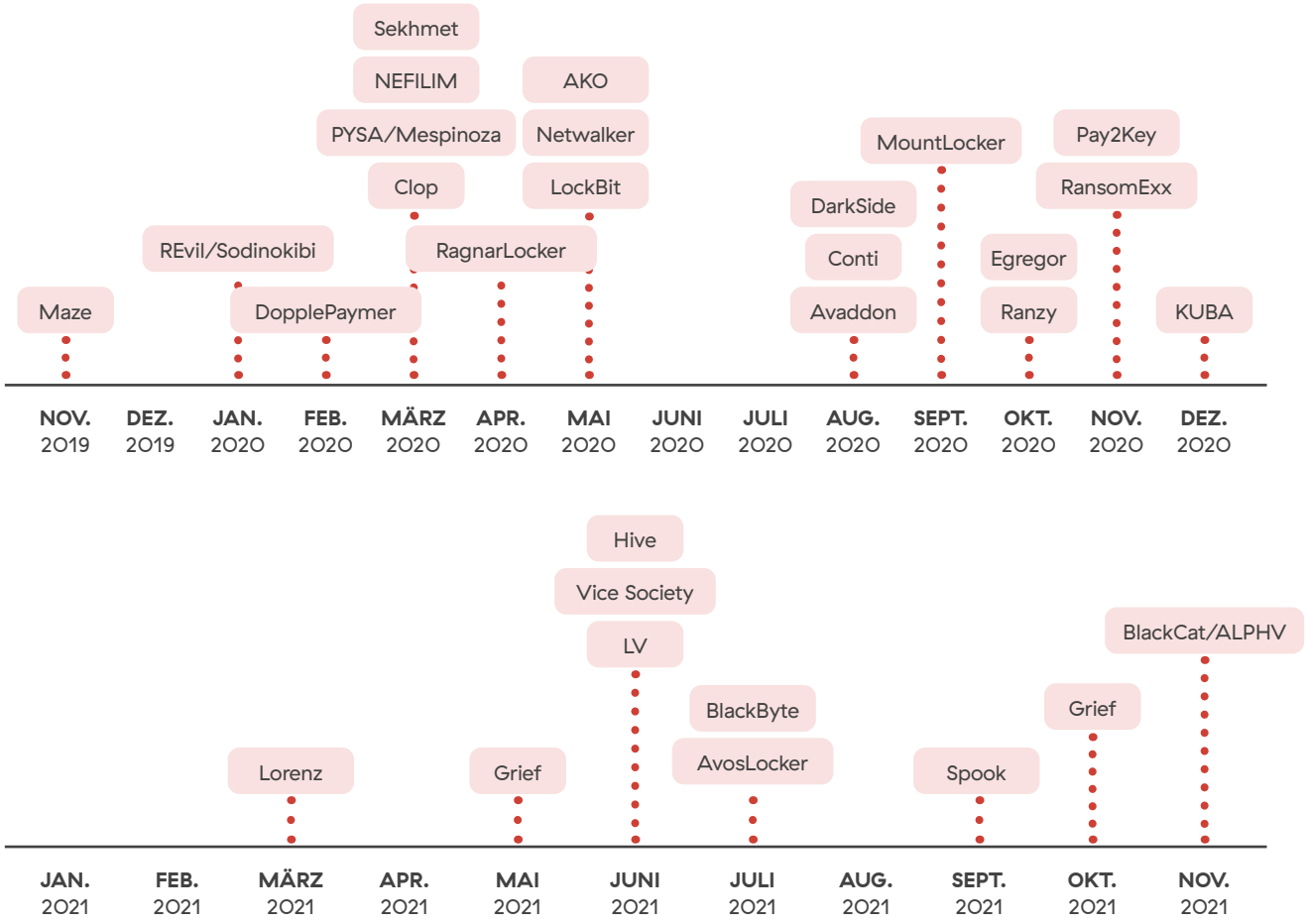


Abbildung 4: Zeitleiste der Veröffentlichung gestohlener Daten auf Dataleak-Websites oder in Hackerforen

Viele der aktiven Ransomware-Gruppen in den Jahren 2021—2022 nutzen RaaS-Modelle (Ransomware-as-a-Service) und steigern so die Verbreitung über Affiliate-Netzwerke. Im Jahr 2021 haben sich außerdem mehrere etablierte Ransomware-Gruppen umbenannt, so wurde z. B. DoppelPaymer zu Grief, DarkSide zu BlackMatter und Avaddon erst zu Haron, dann zu Midas (die beiden letzteren verwenden den Ransomware-Builder von Thanos).

Conti war innerhalb der letzten zwei Jahre die aktivste Ransomware-Gruppe — und die kostspieligste aller Zeiten: Das FBI schätzt, dass bis Januar 2022 mehr als 1.000 Unternehmen Angriffen im Zusammenhang mit Conti-Ransomware zum Opfer fielen. Dabei beliefen sich die Gesamtkosten für die Opfer auf mehr als 150 Millionen US-Dollar (ohne die damit verbundenen Schäden oder Kosten für deren Behebung).
Zu den Opfern von Conti gehören einige Anbieter kritischer Dienstleistungen aus der Finanz-, IT- und Energiebranche sowie aus dem Regierungssektor, darunter der staatliche Gesundheitsdienst Irlands und die Regierung von Costa Rica. Im Mai 2022 setzte das Außenministerium der USA eine Belohnung in Höhe von 10 Millionen US-Dollar für Informationen über die Anführer der Gruppe aus.

LockBit, früher bekannt als ABCD-Ransomware, greift in der Regel Unternehmen des kleinen und mittleren Größensegments an und entgeht so größtenteils der öffentlichen Aufmerksamkeit — mit Ausnahme des Angriffs auf Accenture im August 2021. LockBit ist eine weit verbreitete RaaS, die aufgrund ihrer Geschwindigkeit und Leistung für Angreifer besonders interessant ist.

In Abbildung 5 sind die Ransomware-Gruppen aufgeführt, die zwischen Februar 2021 und März 2022 die meisten Unternehmen mit Angriffen mit Doppelerpressung geschädigt haben, basierend auf Informationen von Dataleak-Websites.

Ransomware-Angriffe nach Gruppe

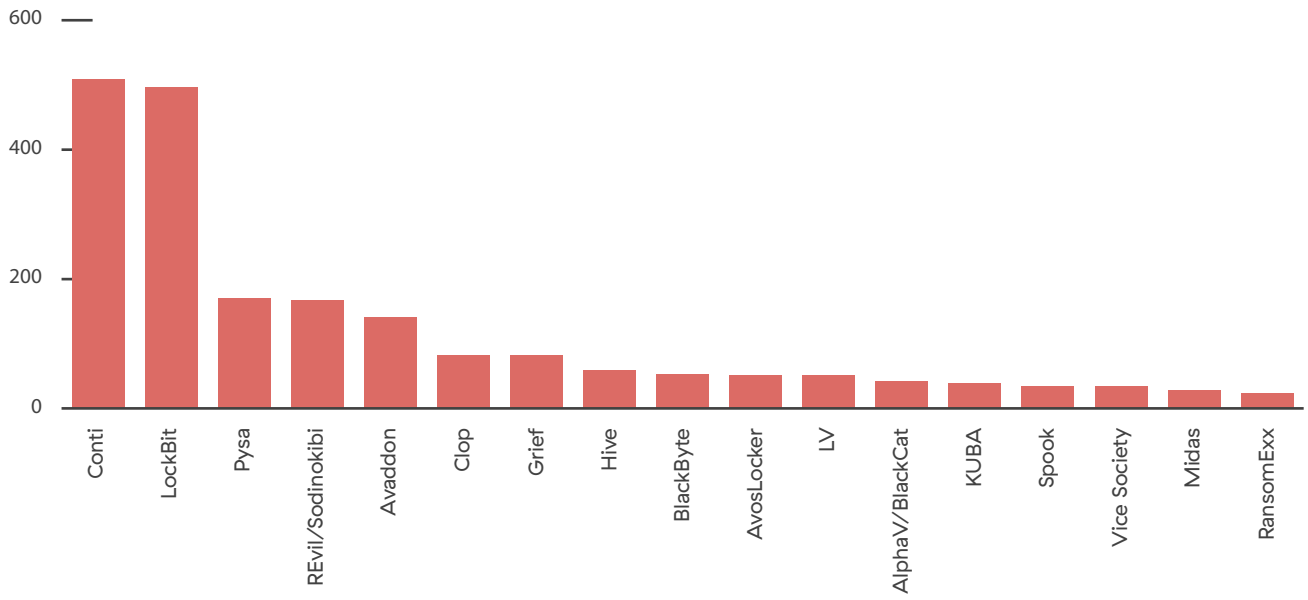


Abbildung 5: Ransomware-Angriffe nach Gruppe, Februar 2021—März 2022

Prognosen für 2022–2023

Ransomware as a Service wird sich weiter durchsetzen

RaaS hat sich für alle beteiligten Parteien als nützlich erwiesen. Neue Ransomware-Entwickler und Partner werden dieses Modell verstärkt verwenden, um immer neue Angriffe auf anfällige Organisationen durchzuführen.

Veränderte Ransomware-Modelle führen zu neuen Zielen

Da Ransomware-Builder und Unternehmensinformationen im Dark Web zum Verkauf stehen, haben Angreifer den Vorteil, dass sie Unternehmensprofile nach bestimmten Schwachstellen, Gewinnen und der potenziell wirkungsvollsten Ransomware filtern können, um die idealen Ziele zu finden. Infolgedessen ist eine Verlagerung hin zu leichteren Zielen zu erwarten, einschließlich Unternehmen des kleinen und mittleren Größensegments mit weniger Sicherheitskontrollen. Ein weiteres Ziel könnten Organisationen sein, deren Zugangsdaten im Rahmen eines Phishing-Angriffs gestohlen wurden und die zudem Anwendungen nutzen, die im Internet sichtbar sind sowie bekannte Sicherheitsrisiken aufweisen.

Die einzelnen Phasen eines Ransomware-Angriffs werden noch schneller ablaufen

Jetzt, da Cyberkriminelle über das Dark Web einfachen und günstigen Zugriff auf Unternehmensprofile und kompromittierte Zugangsdaten haben, sind die Zeiten vorbei, in denen Angreifer monate- oder sogar jahrelang ihr Ziel beobachteten und analysierten, bevor sie einen Angriff starten. Immer mehr öffentliche Berichte über Ransomware-Angreifer, die die Zeit zwischen den einzelnen Phasen auf nur wenige Tage verkürzen, zeigen, dass die Kriminellen mit optimierten Technologien zur Ransomware-Erkennung vertraut sind und wissen, dass es von entscheidender Bedeutung ist, einen Angriff so schnell wie möglich abzuwickeln. Daher müssen Sicherheitsteams Lücken schließen und die Erkennung beschleunigen — auf Tage, Stunden oder sogar nur Minuten —, um die schlimmsten Sicherheitsverletzungen im Jahr 2022 und darüber hinaus zu verhindern.

Supply-Chain-Angriffe werden häufiger auftreten, da Angreifer die Ökosysteme von Partnern und Lieferanten kompromittieren

Die weltweit führenden Unternehmen verfügen oft über die besten Sicherheitsvorkehrungen, aber das gilt möglicherweise nicht für ihre Lieferanten und Partner, die ebenfalls auf deren Netzwerke, Systeme und Informationen zugreifen können. Dies zeigte sich erst kürzlich, als Lapsus$ Okta hackte und Apple von der Hackergruppe REvil erpresst wurde, die über Quanta Computer, einem Fertiger von Apple-Produkten, an Firmengeheimnisse gelangt war. Diese und viele andere Gruppen nutzten Supply-Chain-Angriffe, um mittels des Zugangs von Zulieferern auf vertrauliche Informationen zuzugreifen, ohne die strengen Sicherheitsmaßnahmen ihrer eigentlichen Ziele überwinden zu müssen.

Ransomware könnte als oder in Verbindung mit Wiper-Malware verwendet werden, um Daten zu vernichten

Anfang 2022 wurden Wiper-Angriffe auf die Ukraine bekannt, darunter HermeticWiper und eine Decoy-Ransomware namens PartyTicket. Dies ist nicht das erste Mal, dass Ransomware bei geopolitischen Angriffen eingesetzt wird: 2017 wurden beispielsweise NotPetya und Bad Rabbit genutzt, um ukrainische Organisationen zu schädigen. Geopolitische Spannungen führen oft zum Einsatz von Ransomware, Wiper-Malware und ähnlichen Methoden. Die Vorteile für die Angreifer liegen auf der Hand: Anonymität und die Möglichkeit, jegliche Beteiligung zu dementieren.

Alte (und neue) Sicherheitsrisiken werden weiterhin Schäden verursachen

Im vergangenen Jahr wurden unter anderem mit Log4j, PrintNightmare, ProxyShell/ProxyLogon einige schwerwiegende Sicherheitsrisiken bekannt, mit denen sich Unternehmen auch in den kommenden Jahren auseinandersetzen müssen. Angreifer werden weiterhin nach ungepatchter und veralteter Software sowie entsprechenden Servern Ausschau halten und diese ausnutzen, um Sicherheitskontrollen zu umgehen.

Ransomware-Gruppen werden immer wieder unter neuem Namen auftreten

Schon im Jahr 2021 konnte man diesen Kreislauf beobachten: Eine Ransomware-Gruppe führt einen umfassenden Angriff durch, erregt Aufmerksamkeit und wird von Strafverfolgungsbehörden sanktioniert. In der Folge verschwindet sie von der Bildfläche und kehrt später unter neuem Namen zurück. Da die Strafverfolgungsbehörden diese Gruppen sehr genau beobachten, wird sich dieses Muster auch im Jahr 2022 fortsetzen.

Unternehmen müssen ihre Sicherheitsmaßnahmen auch über den Endgeräteschutz hinaus erhöhen Ransomware-Gruppen werden vermehrt Taktiken anwenden, um Antivirenprogramme und andere Sicherheitskontrollen für Endgeräte zu umgehen. Daher werden Unternehmen einen noch größeren Bedarf an Defense-in-Depth-Lösungen haben, um Eindringlinge entdecken und abwehren zu können.

Ransomware-Entwickler werden ihre Malware noch besser verschleiern

Malware-Autoren implementieren Techniken zur Malware-Verschleierung, um Reverse Engineering zu verhindern und die Erkennung statischer Signaturen zu umgehen. Die Komplexität der Malware-Verschleierung wird dank fortschrittlicher Techniken wie Control Flow Flattening, polymorpher String-Verschleierung und der Verwendung VM-basierter Packer weiter zunehmen.

Offengelegter Ransomware-Quellcode wird zu Abspaltungen führen

Im vergangenen Jahr wurden mehrere Quellcodes für Ransomware öffentlich gemacht, darunter zwei Versionen von Conti und Babuk. Zscaler ThreatLabz stellte bereits fest, dass der Quellcode beider Ransomware-Gruppen von Dritten übernommen und in Angriffen verwendet wurde. Die Veröffentlichung von Quellcode wird zweifellos zu einem Missbrauch durch andere kriminelle Gruppen führen, die nicht über das Fachwissen verfügen, um eigene Ransomware zu entwickeln.

Empfehlungen zum Schutz vor Angriffen

Das Zero-Trust-Konzept ist gleichermaßen wirksam gegen einfache Ransomware-Angriffe und Angriffe mit mehrfacher Erpressung, eigenständig agierende Gruppen und groß angelegte RaaS-Angriffe unter Mitwirkung von Affiliate-Netzwerken. Es empfiehlt sich als Strategie, die in sämtlichen Angriffsphasen – von der Reduzierung von Sicherheitsrisiken im Vorfeld über die Prävention und Erkennung versuchter Angriffe bis hin zur Schadensbegrenzung nach einem erfolgreichen Erstzugriff – zur Minimierung der potenziellen Folgewirkungen eingesetzt werden kann. Zur effektiven Abwehr von Ransomware-Angriffen haben sich insbesondere folgende Maßnahmen bewährt:

1 **Verkleinern der externen Angriffsfläche:** Im Vorfeld von Ransomware-Angriffen führen die Akteure zumeist Reconnaissance-Maßnahmen zur Erkundung der IT-Umgebung ihrer potenziellen Opfer durch. Dabei halten sie insbesondere Ausschau nach Sicherheitslücken sowie nach Möglichkeiten zur gezielten Kalibrierung des Angriffs. Je mehr Anwendungen im Internet exponiert sind, desto anfälliger ist eine Organisation für Angriffe. Eine Zero-Trust-Architektur schützt interne Anwendungen wirksam, indem sie sie für Angreifer unsichtbar macht.

2 **Durchsetzung einheitlicher Sicherheitsrichtlinien zur Verhinderung des Erstzugriffs:** Für Organisationen mit dezentralen Belegschaften ist die Implementierung einer SSE-Architektur (Security Service Edge) ein unverzichtbares Muss. Nur so lassen sich einheitliche Sicherheitsrichtlinien für sämtliche User innerhalb und außerhalb des Unternehmensnetzwerks durchsetzen.

3 **Sandboxing zum Erkennen unbekannter Payloads:** Angesichts der rapiden Entwicklung neuer Ransomware-Varianten und Payloads gewährt die signaturbasierte Erkennung keinen ausreichenden Schutz. Eine KI-gestützte Inline-Sandbox, die in der Lage ist, das Verhalten von Dateien zu analysieren, erkennt auch Ausweichmanöver und bislang unbekannte Varianten.

4 **Implementierung einer ZTNA-Architektur (Zero Trust Network Access):** Durch granulare User-to-Application- und Application-to-Application-Segmentierung und minimale Rechtevergabe über dynamische Zugriffskontrollen kann die laterale Bewegungsfreiheit innerhalb der IT-Umgebung radikal eingeschränkt werden. Dadurch lässt sich der Schaden begrenzen, der im Fall eines erfolgreichen Angriffs durch Verschlüsselung bzw. Diebstahl von Daten entstehen kann.

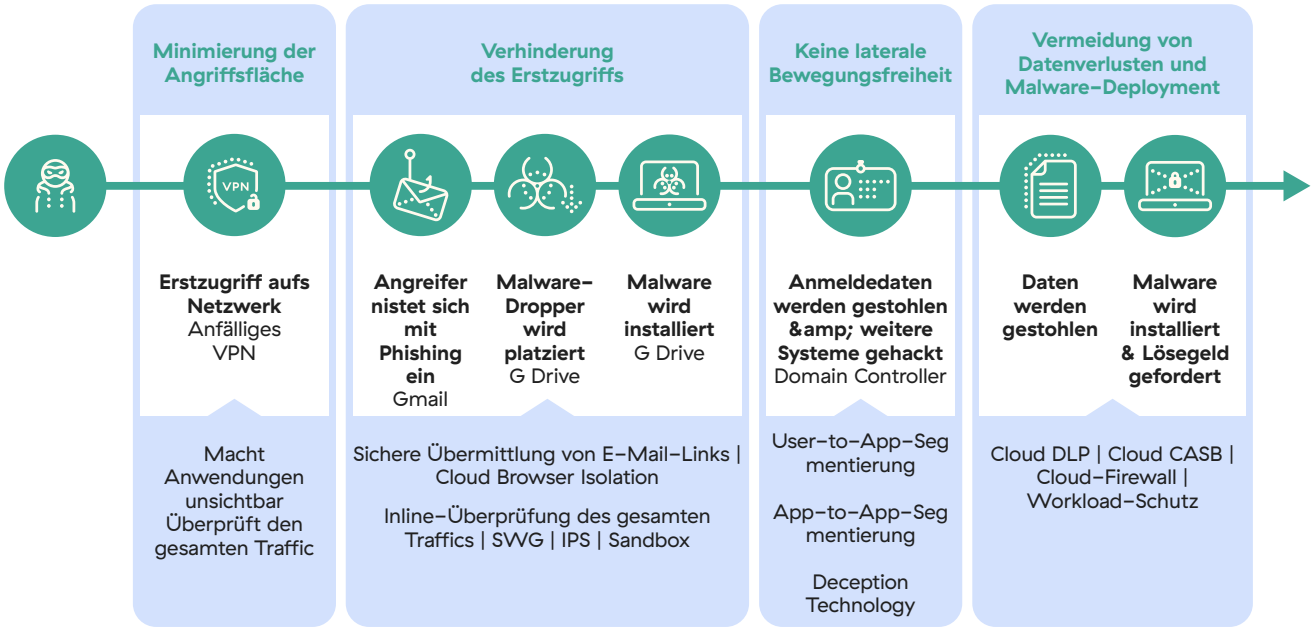
5 **Einsatz von Inline Data Loss Prevention:** Um Doppelerpressungsversuche zu vereiteln, kann die Exfiltration vertraulicher Daten durch Einsatz geeigneter DLP-Tools und -Richtlinien (Data Loss Prevention) verhindert werden.

6 **Regelmäßige Software-Aktualisierung und Mitarbeiterschulungen:** Durch umgehendes Installieren von Sicherheitspatches und regelmäßige Mitarbeiterschulungen lassen sich Sicherheitslücken schließen, die Cyberkriminelle ansonsten geschickt auszunutzen wissen.

7 **Notfallplanung:** Mit einer Cyber-Versicherung, einem Plan für die Datenwiederherstellung und einem Notfallplan im Rahmen des unternehmensweiten BCDR-Konzepts (Business Continuity and Disaster Recovery) sind potenzielle Opfer von Ransomware-Angriffen für den Ernstfall gewappnet.

Eine effektive Strategie zum Schutz vor Ransomware-Angriffen beinhaltet mehrschichtige Maßnahmen, die sämtliche Phasen des Angriffszyklus abdecken — von Reconnaissance und Erstzugriff über laterale Ausbreitung und Datendiebstahl bis hin zur Ausführung der eigentlichen Ransomware.

Vorteile von Zero Trust zur Abwehr von Ransomware



Fakten und Zahlen zur Entwicklung der Ransomware-Lage

Supply-Chain-Angriffe

Was ist unter dem Begriff zu verstehen?
Supply-Chain-Angriffe — auch bekannt als Angriffe auf die Wertschöpfungskette oder Angriffe über Dritte — sind Angriffe auf die Zulieferer einer Organisation mit dem Ziel, sich unbefugten Zugriff auf die IT-Umgebung der betreffenden Organisation zu verschaffen. Große Organisationen verfügen in der Regel über robuste Sicherheitskontrollen, die sie vor direkten Infiltrationen schützen. Supply-Chain-Angriffe werden als Möglichkeit ausgenutzt, diese Sicherheitskontrollen zu umgehen bzw. zu unterlaufen.

Bei Supply-Chain-Angriffen wird das Vertrauensverhältnis zwischen legitimen Organisationen ausgenutzt, das die Grundlage für gute Geschäftsbeziehungen bildet. Die Angreifer platzieren eine Backdoor zu einem Produkt, mit dem das intendierte Opfer regelmäßig arbeitet, und verschaffen sich dann durch diese „Hintertür" über automatische Patches oder sogenannte trojanisierte Software-Updates Zugang zur IT-Umgebung der betreffenden Organisation. Die dort gespeicherten bzw. gehosteten Ressourcen werden dann ausspioniert, Daten gestohlen, weitere Malware implantiert und Betriebsabläufe gestört.

Diese Angriffe erfordern ein hohes Maß an Planung und Raffinesse und können über das ursprüngliche Opfer hinaus zahlreiche weitere Organisationen in Mitleidenschaft ziehen.

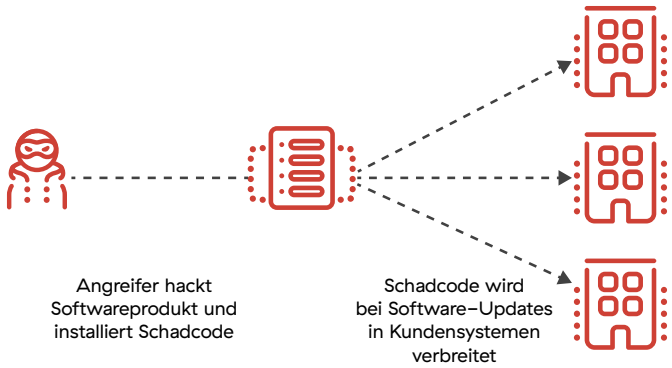


Abb. 6: Supply-Chain-Angriff

Supply-Chain-Angriff auf Kaseya
Am 2. Juli 2021 meldete der Software-Anbieter Kaseya einen Sicherheitsvorfall, der die lokale Version der Plattform Kaseya VSA betraf. Die Plattform wird von Managed Service Providers (MSPs) für Patch-Management, Backups und Client-Monitoring im Auftrag von Kunden eingesetzt. Die Zahl der MSPs, die bei dem Angriff Sicherheitsverletzungen erlitten, wird auf rund 70 geschätzt; von den Auswirkungen waren bis zu 1.500 KMUs betroffen.

Ermöglicht wurde der Angriff durch eine Zero-Day-Sicherheitslücke im Kaseya-VSA-Server, über die ein schädliches Skript an alle von diesem Server verwalteten Clients versendet werden konnte. Das Skript wurde dann wiederum zur Auslieferung von REvil/Sodinokibi-Ransomware ausgenutzt, die Dateien in den infizierten Systemen verschlüsselte.

Supply-Chain-Angriff auf Quanta Computer
Im April 2021 wurde Quanta Computer, der weltweit größte Hersteller von Laptops und ein wichtiger Lieferant von Apple-Produkten, Opfer eines Ransomware-Angriffs mit REvil. Quanta weigerte sich, das geforderte Lösegeld in Höhe von 50 Mio. USD zu zahlen, woraufhin die Angreifer stattdessen Apple und andere Quanta-Kunden ins Visier nahmen: Sie veröffentlichten 21 Screenshots von Schaltplänen für MacBooks und drohten mit der Offenlegung weiterer Daten, bis Apple und Quanta der Lösegeldforderung nachkamen.

Log4j-Ransomware

Im Dezember 2021 veröffentlichte die Apache Software Foundation eine Sicherheitswarnung zu einer Zero-Day-Sicherheitslücke (CVE-2021-44228) in der populären Log4j-Protokollbibliothek, die es Angreifern ermöglicht, schädliche Payloads herunterzuladen und auszuführen. Ein Angreifer, der die Kontrolle über Protokollnachrichten oder Protokollnachrichtenparameter hat, kann einen beliebigen Code ausführen, der von LDAP-Servern geladen wird, wenn die Message-Lookup-Substitution aktiviert ist. Das Log4j-Dienstprogramm ist als Komponente für Protokollierungsanfragen in zahlreiche Websites, Anwendungen und Frameworks integriert — entsprechend verheerend waren die Auswirkungen der Sicherheitslücke, die bereits für mehrere erfolgreiche Ransomware-Angriffe ausgenutzt wurde:

NightSky
Am 4. Januar 2021 nutzten Angreifer die Log4j-Sicherheitslücke in einem über das Internet zugänglichen System, auf dem VMware Horizon ausgeführt wurde, zur Verbreitung von NightSky-Ransomware.

Khonsari
Bei mehreren Angriffen wurde Khonsari-Ransomware über Log4j-Exploits in Windows-Systemen verbreitet.

Conti
Die Conti-Gruppe hat die Log4j-Sicherheitslücke ebenfalls zur Ausführung von Ransomware-Angriffen ausgenutzt. Nach Beobachtungen von AdvIntel scannte die Gruppe anfällige Versionen von Log4j in VMware vCenter und nutzte bestehende Cobalt-Strike-Sitzungen zur lateralen Ausbreitung ihrer Ransomware in den Netzwerken europäischer und US-amerikanischer Opfer aus.

TellYouThePass
Angreifer nutzten die Log4j-Sicherheitslücke zur Verbreitung und Ausführung von TellYouThePass-Ransomware in Windows- und Linux-Systemen aus.

Ransomware-as-a-Service (RaaS)

Das Dark Web hat sich längst als Marktplatz für kriminelle Machenschaften etabliert, auf dem auch Schadcode-Entwickler ihre Produkte anbieten. Diese Entwicklung betrifft unterschiedliche Angriffsarten und wird u. a. im ThreatLabz-Report „State of Phishing 2022“ dokumentiert.

RaaS erfreut sich mittlerweile ungeheurer Beliebtheit und war bei der Mehrzahl der im Berichtzeitraum beobachteten Ransomware-Angriffe im Spiel. Sage und schreibe acht der elf aktivsten Ransomware-Gruppen nutzten RaaS-Ökosysteme zur Ausführung von Angriffen.

Das RaaS-Modell basiert auf einer Arbeitsteilung zwischen zwei Partnern: Ransomware-Betreibern und Affiliates. Bei den Betreibern handelt es sich um die Gruppen, die die Ransomware entwickeln. Alles Weitere — Auskundschaften potenzieller Opfer, Ausführung der Ransomware und Verhandlungen über Lösegeldforderungen — übernehmen die Affiliates.

Die Betreiber stellen über das Dark Web den Kontakt zu geeigneten Affiliates her, denen sie dann die Ransomware sowie die erforderlichen Tools zu ihrer Ausführung bereitstellen. Affiliates erhalten außerdem Zugriff auf eine Dataleak-Website und ggf. Unterstützung bei den Lösegeldverhandlungen. Im Gegenzug zahlen sie 70 bis 80 % ihrer Gewinne an die Betreiber.

Von diesem Modell profitieren beide Seiten. Den Affiliates werden alle notwendigen Ressourcen zur Ausführung hochgradig effektiver Ransomware-Angriffe zur Verfügung gestellt, ohne dass sie den Schadcode selbst programmieren müssen. Diese Option ist sowohl für kompetente Hacker attraktiv, die dadurch Entwicklungszeit und Ressourcen sparen, als auch für Cyberkriminelle ohne Entwicklerkompetenzen, die sonst nicht in der Lage wären, einen derartigen Angriff auszuführen. Ransomware-Betreiber wiederum können dadurch die Reichweite ihrer Aktivitäten beträchtlich vergrößern und entsprechend höhere Gewinne einstreichen.

Die Verbreitung von RaaS hat zu einer Zunahme sowohl der Angriffshäufigkeit als auch der Schadenshöhe geführt:

- **Höhere Angriffshäufigkeit:** Bedingt durch den Wegfall von Einstiegshürden wie Zeitaufwand und Entwicklerkompetenz beteiligen sich immer mehr Cyberkriminelle als Affiliates an der Ausführung von Ransomware-Angriffen.
- **Höhere Lösegelder aufgrund von Doppelerpressung:** Doppelerpressung ist als Komponente im RaaS-Modell inbegriffen, d. h. die Angreifer stehlen Daten und drohen bei Verweigerung der Lösegeldzahlung mit ihrer Veröffentlichung auf einer Dataleak-Website. Dadurch steigen sowohl die Lösegeldforderungen als auch die Erfolgsquote bei Ransomware-Angriffen.

Angriffe mit geopolitischem Hintergrund

Sicherheitsexperten weltweit rechnen mit einer Zunahme von Ransomware-Angriffen infolge des Konflikts in der Ukraine.

Im März 2022 warnte US-Präsident Joe Biden in einer offiziellen Erklärung vor dem erhöhten Risiko von Cyberangriffen auf US-amerikanische Ziele infolge der Wirtschaftssanktionen gegen Russland. Organisationen im öffentlichen wie im privaten Sektor wurden dringend zur Verstärkung ihrer Cybersicherheit aufgefordert.

Acht der elf aktivsten Ransomware-Gruppen nutzten 2021 RaaS-Ökosysteme zur Ausführung von Angriffen.

Bei Redaktionsschluss dieses Reports lagen Informationen über mehrere Ransomware-Angriffe gegen ukrainische Ziele und/oder im Zusammenhang mit diesem Konflikt vor:

1. **PartyTicket:** Diese Go-basierte Ransomware kam bei Angriffen auf ukrainische Unternehmen in Kombination mit der HermeticWiper-Malware zum Einsatz. PartyTicket ist nicht ausgereift und enthält u. a. fehlerhafte Verschlüsselung, die entschlüsselt und rückgängig gemacht werden kann. Daher liegt die Vermutung nahe, dass sie als Decoy entwickelt wurde, das von HermeticWiper ablenken soll.
2. **Conti:** Die Cybersecurity and Infrastructure Security Agency (CISA), das Federal Bureau of Investigation (FBI), die National Security Agency (NSA) und der United States Secret Service haben erneut eine Sicherheitswarnung zu Conti veröffentlicht, einer Ransomware-Gruppe mit Verbindungen nach Russland. Darin heißt es: „Die Cyberbedrohungsakteure von Conti sind weiterhin aktiv, und es wurden bereits über 1.000 Angriffe mit Conti-Ransomware gegen US-amerikanische und internationale Organisationen gemeldet." Ende Februar veröffentlichte die Conti-Gruppe zwei Erklärungen auf ihrer Dataleak-Website, in denen sie als Reaktion auf „westliche Kriegstreiberei und amerikanische Drohungen gegen die Bürger der Russischen Föderation" der russischen Regierung ihre Unterstützung zusagte.

Ransomware im Visier der Strafverfolgungsbehörden

Strafverfolgungsbehörden auf der ganzen Welt gehen zunehmend gegen Ransomware-Gruppen vor, insbesondere solche, die weitreichende Schäden verursachen. Im Berichtzeitraum wurden mehrere erfolgreiche Polizeiaktionen gegen prominente Ransomware-Gruppen durchgeführt.

REvil

REvil zählt zu den aktivsten und gefährlichsten Ransomware-Gruppen der letzten zwei Jahre und machte insbesondere mit groß angelegten Angriffen auf Kaseya und JSB von sich reden. Eine geplante FBI-Aktion zur Stilllegung der REvil-Server nach dem Kaseya-Angriff verlief im Sande, nachdem die Gruppe im Juli 2021 den Betrieb einstellte und die beteiligten Hacker untertauchten. Dies war allerdings nur von kurzer Dauer, denn bereits im September 2021 war REvil wieder aktiv.

Im Januar 2022 ging die russische Regierung offenbar auf Ersuchen der USA gegen die REvil-Hacking-Gruppe vor. Der russische Geheimdienst (FSB) durchsuchte 25 Adressen, nahm 14 Mitglieder der REvil-Gruppe fest und beschlagnahmte 426 Mio. Rubel, 600.000 USD, 500.000 Euro, 20 Luxusautos und Computerausrüstung. REvil tauchte jedoch bereits im April 2022 wieder auf und griff Organisationen mit einer aktualisierten Ransomware-Version an.

DarkSide

Am 6. Mai 2021 führte die Ransomware-Gruppe DarkSide einen aufsehenerregenden Angriff auf Colonial Pipeline, die größte Öl-Pipeline in den USA, durch. Die Behörden griffen gegen die Gruppe durch, und innerhalb von zwei Wochen nach dem Angriff meldete ein Bedrohungsakteur namens UNKN die Einstellung von DarkSide. In der Erklärung hieß es, die Gruppe habe den Zugriff auf ihre Server verloren und ihre Kryptowährung sei auf ein unbekanntes Konto übertragen worden. Nach Angaben des US-Justizministeriums wurden bei der Aktion 63,7 Bitcoin mit einem Gesamtwert von rund 2,3 Mio. USD beschlagnahmt.

Egregor

Am 9. Februar 2021 gingen ukrainische, französische und US-amerikanische Strafverfolgungsorgane im Rahmen einer gemeinsamen Aktion erfolgreich gegen die Ransomware-Gruppe Egregor — ehemals unter dem Namen „Maze" bekannt — vor. Neben der Stilllegung der Dataleak-Website wurden Gruppenmitglieder verhaftet und Computer beschlagnahmt, die bei Ransomware-Angriffen involviert waren. Egregor hatte insgesamt rund 80 Mio. USD von mehr als 150 Erpressungsopfern erbeutet.

Umbenennungen prominenter Ransomware-Varianten

Im vergangenen Jahr war ein auffälliger Trend zum Rebranding zahlreicher bekannter Ransomware-Varianten zu beobachten. Auslöser für die Umbenennung war zumeist unerwünschte Aufmerksamkeit seitens Strafverfolgungsbehörden und Medien. Teilweise wurden auch Sanktionen gegen einzelne Gruppen verhängt, die deren Fähigkeit zum Einziehen von Lösegeldern beeinträchtigten.

Aus DoppelPaymer wurde Grief

Anfang Mai 2021 war ein deutlicher Rückgang der Aktivität der DoppelPaymer-Ransomware zu beobachten. Die betreffende Dataleak-Website war zwar weiterhin online, jedoch wurde der letzte Neueintrag am 6. Mai 2021 veröffentlicht und ab Ende Juni auch keine Aktualisierungen bestehender Einträge mehr vorgenommen. Diese Funkstille wurde zunächst als Folge des Ransomware-Angriffs gegen Colonial Pipeline am 7. Mai 2021 interpretiert. Dahinter verbarg sich jedoch die Umbenennung der DoppelPaymer-Ransomware, die nun unter dem neuen Namen Grief aktiv ist. Beide Varianten nutzen den gleichen Schadcode, und auch die Dataleak-Websites sind sehr ähnlich angelegt. Gewisse Unterschiede gibt es im Aufbau der Zahlungsportale zur Entrichtung des Lösegelds. Auffällig ist hier insbesondere, dass Lösegelder nicht mehr in Bitcoin (BTC), sondern in der Kryptowährung Monero (XMR) gefordert werde. Experten sehen darin eine Reaktion auf die Sicherstellung der digitalen Wallet mit 63,7 der 75 von Colonial Pipeline erbeuteten Bitcoin durch das FBI.

Durch Umbenennung gelingt es Ransomware-Gruppen, Sanktionen zu umgehen und sich der Aufmerksamkeit der Strafverfolgungsbehörden zu entziehen.

Aus DarkSide wurde BlackMatter

Nach der erfolgreichen Aktion gegen DarkSide im Mai 2021 trat Ende Juli erstmals eine Ransomware-Gruppe namens BlackMatter in Erscheinung. Die in der Ransomware eingesetzte Verschlüsselungsroutine sowie bestimmte Formulierungen auf der Dataleak-Website ließen vermuten, dass es sich dabei um eine Neuauflage von DarkSide unter anderem Namen handelt.

BlackMatter stellte im November 2021 den Betrieb ein. In einer entsprechenden Erklärung, die im RaaS-Portal der Gruppe veröffentlicht wurde, hieß es: „Aufgrund bestimmter unlösbarer Umstände, die mit dem Druck seitens der Behörden zu tun haben (ein Teil des Teams ist den aktuellen Nachrichten zufolge nicht mehr verfügbar), ist das Projekt hiermit beendet."

Umbenennung Thanos-basierter Varianten

Thanos-Ransomware wird im Dark Web als RaaS angeboten und wurde erstmals im Februar 2020 identifiziert. Nach der geleakten Veröffentlichung des Ransomware-Builders wurden verschiedene neue Varianten entwickelt, u. a. die im Februar 2021 erstmals identifizierte Prometheus-Ransomware, die im September 2021 in „Spook" umbenannt wurde. Ähnlichkeiten sind insbesondere bei den Lösegeldforderungen und Dataleak-Websites zu erkennen; zudem ist jeweils der charakteristische Key Identifier von Thanos integriert.

Im Juli 2021 wurde eine weitere von Thanos abgeleitete Ransomware namens Haron entdeckt, die starke Ähnlichkeiten mit Avaddon-Ransomware aufweist. Diese betreffen insbesondere das Format der Lösegeldforderungen sowie der Verhandlungs- und Dataleak-Websites. Im Oktober 2021 wurde eine weitere Variante namens Midas entdeckt, bei der es sich um eine umbenannte Version der Haron-Ransomware handelt.

Umbenennung von Evil Corp
Evil Corp (auch unter dem Namen „Indrik Spider“ bekannt) ist eine kriminelle Organisation, die in verschiedenen Bereichen agiert. Sie hat u. a. den Banktrojaner Didrex entwickelt und zur Verbreitung ihrer BitPaymer-Ransomware ausgenutzt.

Das Office of Foreign Assets Control (OFAC) des US-Finanzministeriums verhängte Sanktionen gegen Mitglieder von Evil Corp für Schäden in Höhe von über 100 Mio. USD in über 40 Ländern, die durch ihre Dridex-Malware verursacht wurden. Aus Angst vor Geldbußen oder rechtlichen Schritten des US-Finanzministeriums weigerten sich die auf Ransomware-Verhandlungen spezialisierten Anbieter infolgedessen, Lösegeldzahlungen für Evil Corp abzuwickeln. Zur Umgehung der Sanktionen wurde die Ransomware mehrfach umbenannt.

Evil Corp verbreitete im Juni 2020 WastedLocker-Ransomware, im Dezember 2020 Hades-Ransomware und im März 2021 Phoenix-Ransomware. Im Mai 2021 erfolgte eine weitere Umbenennung in PayloadBin, um die wahre Identität der Bedrohungsakteure zu verschleiern.

Umbenennung von Rook
Rook-Ransomware wurde erstmals im November 2021 identifiziert und basiert auf geleaktem Source Code von Babuk-Ransomware. Im Dezember 2021 erfolgte die Umbenennung einer Rook-Variante in Night Sky. Diese Variante wurde von der chinesischen Gruppe DEV-0401 bei Ransomware-Angriffen mit Doppelerpressung unter Ausnutzung der Log4Shell-Sicherheitslücke eingesetzt. Im Januar 2022 stellten Rook und Night Sky beide den Betrieb ein. Noch im selben Monat wurde die Pandora-Ransomware beobachtet, bei der es sich offensichtlich ebenfalls um eine Rook-Variante mit neuem Namen handelt. Darauf lassen jedenfalls Ähnlichkeiten zwischen den jeweiligen Codes schließen.

Ransomware-Angriffe unter Ausnutzung kritischer Sicherheitslücken

ProxyLogon-Sicherheitslücken BlackKingdom und DearCry nutzten eine Kombination aus vier verschiedenen ProxyLogon-Sicherheitslücken aus, um sich Zugriff auf die Netzwerke von Angriffsopfern zu verschaffen und diese zu verschlüsseln. Diese Taktik kam zum Einsatz, um auf Microsoft-Exchange-Server zuzugreifen, E-Mail-Daten zu stehlen und weitere Backdoors zu implementieren. Zu den ProxyLogon-Sicherheitslücken zählen CVE-2021-26855 (Server-Side Request Forgery [SSRF] Vulnerability in Exchange), CVE-2021-26857 (Insecure Deserialization Vulnerability im Unified Messaging Service), CVE-2021-26858 (Post-Authentication Arbitrary File Write Vulnerability in Exchange) und CVE-2021-27065 (Post-Authentication Arbitrary File Write Vulnerability in Exchange). Microsoft hat diese Sicherheitslücken im März 2021 gepatcht.

Ein typischer Verlauf eines Angriffs, bei dem Remote-Code über den exponierten Port 443 ausgeführt wird, sieht folgendermaßen aus: Angreifer nutzen die Sicherheitslücke CVE-2021-26855 zur Umgehung der Authentifizierung bei Microsoft Exchange und können sich als User ausgeben. Der Angreifer sendet eine modifizierte POST-Anfrage für eine beliebige Datei im Verzeichnis, die ohne Authentifizierung lesbar ist und nicht im Verzeichnis benötigt wird. Der Angreifer authentifiziert sich über die Sicherheitslücke CVE-2021-26858 oder CVE-2021-27065 im Exchange Control Panel (ECP) und überschreibt beliebige Dateien im Zielsystem. Anschließend kann der Angreifer mittels einer Webshell Remote-Code auf dem Exchange-Server ausführen.

ProxyShell-Exchange-Sicherheitslücke
Conti-Ransomware nutzt die ProxyShell-Sicherheitslücke im Microsoft Exchange Server aus, um auf das Netzwerk des Angriffsopfers zuzugreifen. Dabei handelt es sich um eine Kombination aus CVE-2021-34473 (Microsoft Exchange Server Remote

Code Execution Vulnerability), CVE-2021-34523 (Microsoft Exchange Server Elevation of Privilege Vulnerability) und CVE-2021-31207 (Microsoft Exchange Server Security Feature Bypass Vulnerability). Microsoft stellte vomApril bis Mai 2021 Patches für diese Sicherheitslücken bereit. Conti nutzt jedoch weiterhin ungepatchte Server für Angriffe mit Remote-Code-Ausführung aus. Der Infektionsverlauf wird in diesem Report in den Abschnitten zu den Ransomware-Gruppen BlackByte, AvosLocker und Hive beschrieben. LockFile nutzt diese Sicherheitslücken ebenfalls zur Implementierung von Ransomware aus.

PrintNightmare

Ransomware-Akteure nutzen die PrintNightmare-Sicherheitslücken CVE-2021-34527 und CVE-2021-34481 für Angriffe auf Windows-Systeme aus. Dabei handelt es sich um Sicherheitslücken im Druckspooler-Dienst von Windows, die unbefugten Usern die Remote-Code-Ausführung von Dateivorgängen mit Systemrechten ermöglichen.

Die Sicherheitslücke besteht in der Point-and-Print-Funktion auf Windows-Systemen und ermöglicht Usern ohne entsprechende Zugriffsberechtigungen, Remote-Drucker zu aktualisieren oder zu installieren. Microsoft veröffentlichte im Juli und August 2021 Updates zur Behebung der PrintNightmare-Sicherheitslücken.

Ransomware-Gruppen nutzten die PrintNightmare-Sicherheitslücken bei zwei verschiedenen Angriffen zur Verbreitung von Vice-Society-Ransomware bzw. Magniber-Ransomware aus.

SonicWall SMA 100

Im Januar 2021 meldete SonicWall eine SQL-Injection-Sicherheitslücke in der Secure Mobile Access SMA 100 Series, über die Angreifer mithilfe speziell formulierter, nicht authentifizierter Anfragen auf Anmeldedaten und Sitzungen zugreifen und anfällige Appliances hacken konnten. SonicWall patchte die Lücke im Februar 2021.

Entdeckt wurde die Lücke, nachdem die UNC2447-Gruppe sie zum Angriff auf ein Netzwerk und Implementieren der FIVEHANDS-Ransomware für Doppelerpressungen ausgenutzt hatte. Die Angreifer konnten über die Zero-Day-Sicherheitslücke auf das Netzwerk zugreifen und die SOMBRAT-Backdoor sowie weitere Tools implementieren, um sich im Netzwerk einzunisten, die Umgebung auszukundschaften und Daten zu exfiltrieren. Zum Einsatz kamen u. a. Cobalt-Strike-Beacons, Adfind, BloodHound, Mimikatz, PC Hunter und Rclone. In der finalen Angriffsphase wurde FIVEHANDS-Ransomware implementiert und ausgeführt, um die Daten im angegriffenen System zu verschlüsseln, und bei Nichtzahlung des Lösegelds drohte die UNC2447-Gruppe mit der Veröffentlichung der Daten in Hacker-Foren.

QNAP-NAS-Geräte

Eine neue Variante der eChOraix-Ransomware wurde für Angriffe auf QNAP-NAS-Geräte (Quality Network Appliance Provider Network-Attached Storage) sowie Synology-NAS-Geräte eingesetzt, wobei Angreifer die Sicherheitslücke CVE-2021-28799 in den betreffenden Geräten ausnutzten. Die Sicherheitslücke ermöglicht die unbefugte Remote-Anmeldung ohne ordnungsgemäße Autorisierung auf QNAP-NAS-Geräten, auf denen HB3 (Hybrid Backup Sync) ausgeführt wird.

Die 11 aktivsten Ransomware-Gruppen

Im Folgenden werden die 11 aktivsten Ransomware-Gruppen mit ihren jeweiligen Angriffsverläufen im Überblick dargestellt. Diese Ransomware-Gruppen waren 2021 und 2022 für die meisten erfolgreichen Angriffe verantwortlich und werden hier zur konkreten Veranschaulichung der aktuellen Bedrohungslage detailliert vorgestellt. Dies umfasst einen kurzen Abriss ihrer jeweiligen Entstehungs- und Entwicklungsgeschichte, eine Beschreibung ihrer Taktiken samt Zuordnung zu den in der MITRE ATT&CK Matrix dokumentierten Kategorien sowie Fakten und Zahlen zu den Opfern der Angriffe.

Conti

Ransomware der Conti-Gruppe wurde erstmals im Februar 2020 identifiziert. Conti wird manchmal als RaaS klassifiziert; jedoch handelt es sich bei den Affiliates eher um Mitarbeiter als um Affiliates im eigentlichen Sinn, die sich über ein Portal zur Verwaltung der jeweiligen Seite anmelden und einen bestimmten Prozentsatz der Gewinne erhalten. Ähnlichkeiten im Code deuten darauf hin, dass Conti vermutlich die Nachfolgeversion der Ryuk-Ransomware ist. Conti war 2021 die aktivste Ransomware-Variante.

Infektionsverlauf:
Conti hat bei verschiedenen Kampagnen unterschiedliche Mechanismen für den Erstzugriff eingesetzt:

1. Verbreitung über Spam-E-Mails mit schädlichen Anhängen oder Links, über die zusätzlich TrickBot, IcedID, BazarLoader oder Cobalt Strike heruntergeladen werden, damit die Angreifer Zugang zum System erhalten.
2. Erstzugriff durch Ausnutzen bekannter Sicherheitslücken wie Log4j oder ProxyShell bzw. schwachen RDP-Zugangsdaten (Remotedesktopprotokoll).

Nach dem erfolgreichen Erstzugriff kommen Post-Exploitation-Tools wie Cobalt Strike oder Mimikatz zum Einsatz, um Zugangsdaten zu stehlen und sich im Netzwerk einzunisten. Wir wissen, dass Conti-Bedrohungsakteure Metasploit, Netscan und andere Tools verwenden, die für Red-Team-Simulationen entwickelt wurden, um sich Zugriff auf Informationen zu Netzwerk- und Domaincontrollern zu verschaffen. Anschließend nutzen die Bedrohungsakteure AnyDesk, PsExec oder andere Remote-Dienstprogramme für die laterale Ausbreitung im Netzwerk. Im nächsten Schritt werden mithilfe von Rclone oder anderen Tools Daten exfiltriert. Erst danach erfolgt die eigentliche Implementierung und Ausführung der Conti-Ransomware zur Verschlüsselung von Daten (siehe Abb. 7 unten).

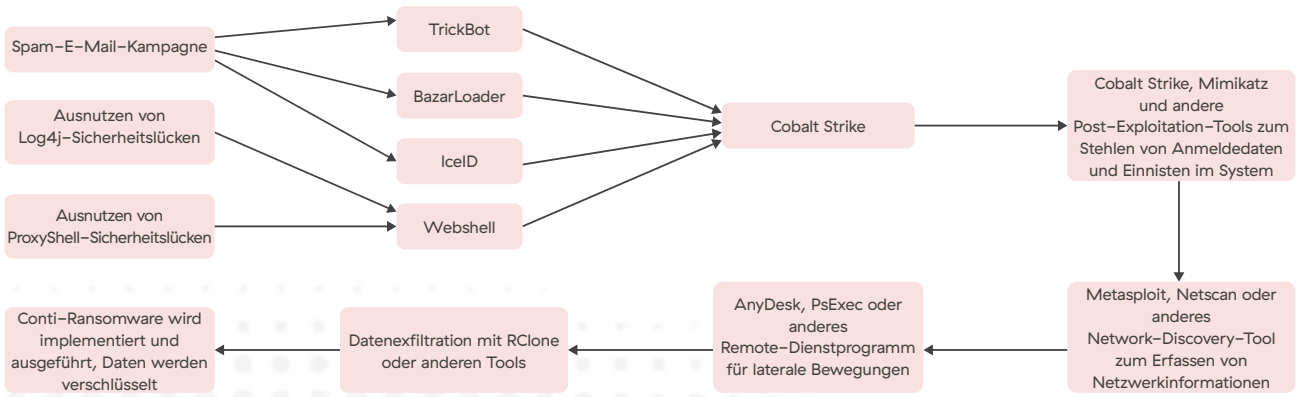


Abb. 7: Anatomie eines Ransomware-Angriffs mit Conti

Die ursprüngliche Version von Conti nutzte RSA- und AES-Algorithmen zur Verschlüsselung. Mittlerweile kommt ChaCha-Verschlüsselung statt AES zum Einsatz.

Ende Januar 2022 identifizierte ThreatLabz im Rahmen unseres weltweiten Engagements zur Verfolgung von Ransomware eine aktualisierte Version der Conti-Ransomware. Dieses Update war bereits im Umlauf, als ein ukrainischer Forscher am 27. Februar 2022 Conti-Quellcode und Chat-Logs im massiven Umfang veröffentlichte. In der neuen Version von Conti sind neue Befehlszeilenargumente inbegriffen, mit denen das System im abgesicherten Modus von Windows bei aktiviertem Netzwerk hochgefahren und dann die Verschlüsselung gestartet werden kann. Durch den Neustart im abgesicherten Modus kann Conti die Anzahl der verschlüsselten Dateien maximieren, da Datenbanken und andere Geschäftsanwendungen mit hoher Wahrscheinlichkeit nicht ausgeführt werden. Conti hat auch die Erweiterungen der verschlüsselten Dateien aktualisiert, sodass sie jetzt Groß- und Kleinbuchstaben sowie Zahlen enthalten. Zu guter Letzt wird auch noch das Desktop-Hintergrundbild eingerichtet, das dem Ransomware-Opfer nach der erfolgreichen Datenverschlüsselung angezeigt wird.

Abb. 8 zeigt, welche Branchen von Conti-Angriffen mit Doppelerpressung betroffen waren.

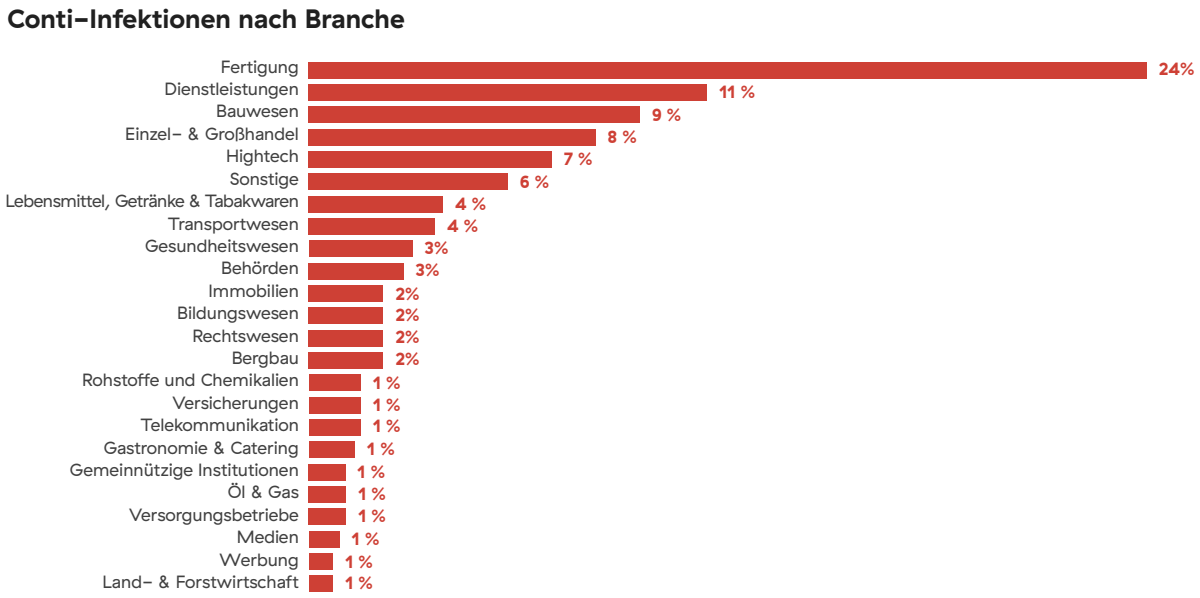


Abb. 8: Conti-Infektionen nach Branche

Seit August 2020 betreibt Conti eine eigene Dataleak-Website, auf der gestohlene Daten von Unternehmen veröffentlicht werden, die sich weigern, das geforderte Lösegeld zu zahlen.

Abb. 9: Dataleak-Website von Conti

Conti: MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Sammlung	Exfiltration	Auswirkung
Spearphishing-Link	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung	Manipulation von Zugriffstokens	Verschleierung/Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen der Netzwerkkonfiguration	Lateraler Tool-Transfer	Archivierung gesammelter Daten	Automatische Exfiltration	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch Modul-Load		Ausnutzung zur Rechteerhöhung	Beeinträchtigung der Verteidigung	Erkennen von Remote-Systemen	Remote-Services	Daten aus dem lokalen System	Exfiltration über Webservice	System-wiederherstellung wird behindert
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Geteilte Module			Process Injection	Erkennen von Dateien und Verzeichnissen				Herunterfahren/Neustart des Systems
Gültige Konten	Ausführung durch User				Erkennung von Sicherheitssoftware				Verunstaltung
Sicherheitslücken in der Lieferkette					Anfrage an die Registry				

LockBit

LockBit-Ransomware wurde erstmals im September 2019 identifiziert — damals nach ihrer Erweiterung .abcd als „ABCD-Ransomware“ benannt. Anfang 2020 erschien eine neue Version, die die Erweiterung .lockbit an verschlüsselte Dateien anhängt. 2020 schloss sich LockBit dem Maze-Kartell an und veröffentlichte seitdem die Daten von Angriffsopfern auf der Dataleak-Website von Maze. Seit Maze im September 2020 den Betrieb einstellte, betreibt LockBit eine eigene Dataleak-Website (siehe Abb. 10).

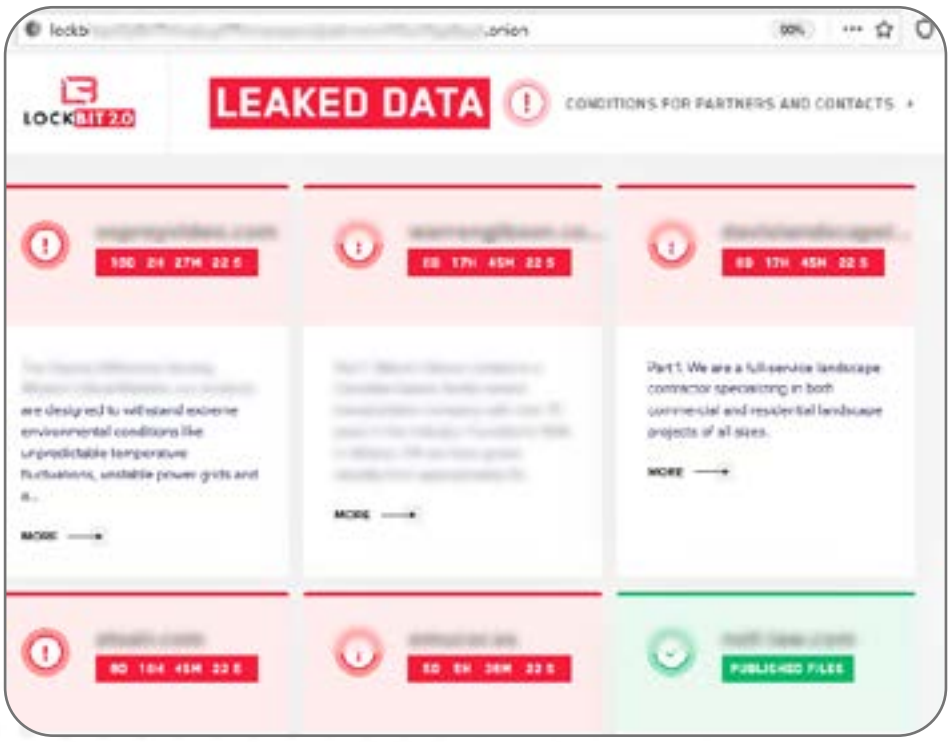


Abb. 10: Dataleak-Website von LockBit

Im Juni 2021 folgte die Veröffentlichung einer neuen Version namens LockBit 2.0. Seit Juli 2021 werden gestohlene Daten der Angriffsopfer auf der Dataleak-Website veröffentlicht. LockBit setzt das RaaS-Modell ein und konnte Mitarbeiter der angegriffenen Organisationen als Affiliates gewinnen, die legitimen Zugriff auf das jeweilige Netzwerk hatten. Verbreitet wird LockBit über Spam-E-Mail-Kampagnen, die schädliche Anhänge oder Links enthalten.

Teilweise erfolgte der Netzwerkzugriff auch mithilfe von RDP- oder VPN-Zugangsdaten, die im Brute-Force-Verfahren gehackt wurden, über infizierte RDP-Konten oder durch Ausnutzen der Sicherheitslücke CVE-2018-13379 im Fortinet VPN.

Infektionsverlauf:
Beim ersten dokumentierten LockBit-2.0-Angriff erfolgte der Zugriff auf das System des betroffenen Unternehmens über ein gehacktes RDP-Konto. Anschließend wurden mit einem Netzwerkscanner Informationen zum Netzwerk erfasst und die Domain-Controller lokalisiert. Neben weiteren Tools nutzten die Angreifer StealBit zur Datenexfiltration sowie Process Hacker und PC Hunter zur Beendung von Prozessen und Services in der Datenbank. Mithilfe einer Batch-Datei wurden Sicherheitsprodukte deinstalliert und Windows-Ereignisprotokolle sowie Funktionen von Windows Defender deaktiviert. Anschließend wurde die Ransomware LockBit 2.0 über Windows-Gruppenrichtlinien verbreitet und ausgeführt.

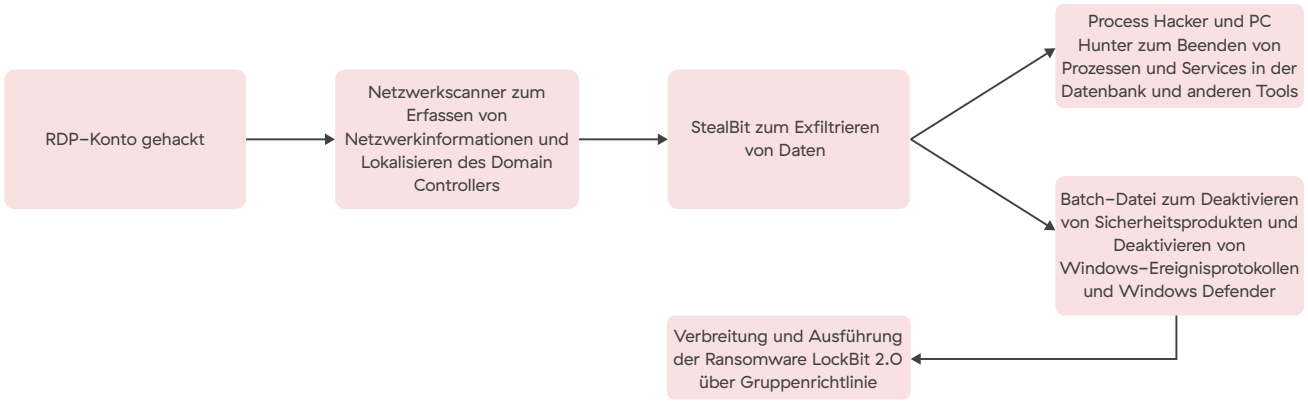


Abb. 11: Anatomie eines Ransomware-Angriffs mit LockBit

LockBit-Ransomware ist nicht zuletzt aufgrund ihrer Effizienz so beliebt: Mithilfe eines Multithreading-Verfahrens geht die Verschlüsselung schneller als bei jeder anderen Ransomware, zumal pro Datei nur 4 KB verschlüsselt werden. Zur Verschlüsselung wird eine Kombination aus RSA- und AES-Algorithmen verwendet. Im Oktober 2021 wurde eine LockBit-Variante für Linux und VMware ESXi veröffentlicht, die Daten mithilfe einer Kombination aus AES- (Advanced Encryption Standard) und ECC-Algorithmen (Elliptic-Curve Cryptography) verschlüsselt.

Abb. 12 zeigt, welche Branchen von LockBit-Angriffen mit Doppelerpressung betroffen waren.

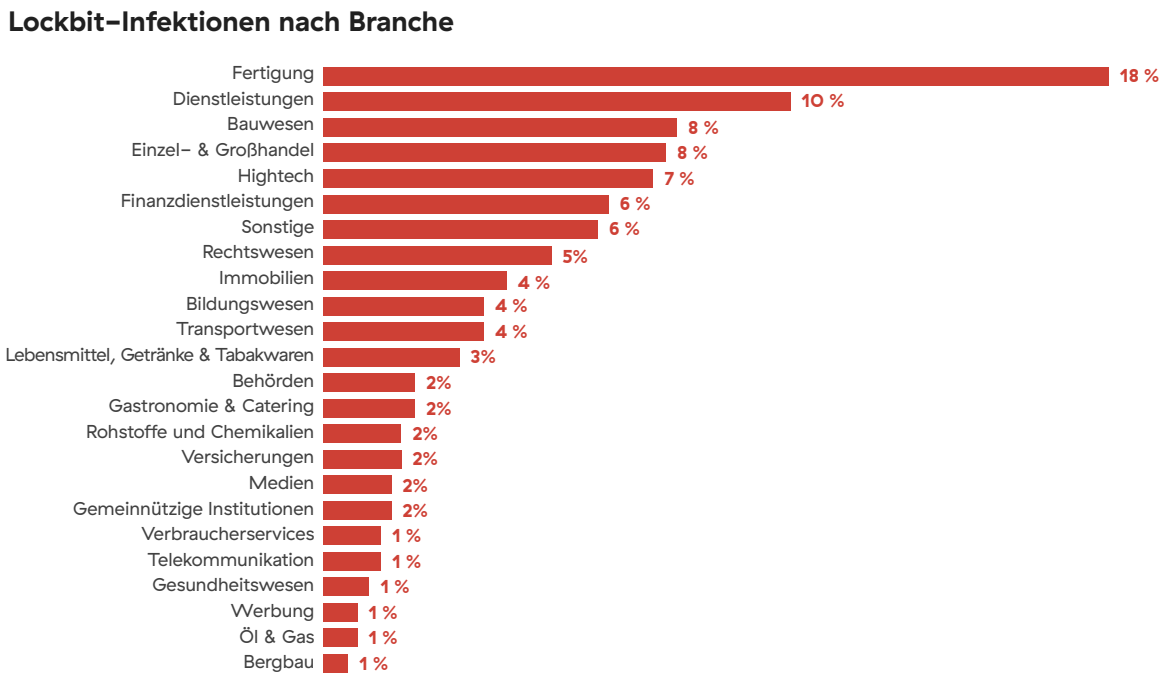


Abb. 12: LockBit-Infektionen nach Branche

LockBit: MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Sammlung	Exfiltration	Auswirkungen
Spearphishing-Link	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung	Missbrauch des Mechanismus zur Rechtevergabe: Umgehung der User Account Control	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen der Netzwerkkonfiguration	Lateraler Tool-Transfer	Archivierung gesammelter Daten	Exfiltration über Webservice	Daten werden verschlüsselt
Spearphishing-Anhang				Beeinträchtigung der Verteidigung: Deaktivierung oder Modifizierung von Tools	Erkennen von Remote-Systemen	Remote-Services	Daten aus dem lokalen System		Systemwiederherstellung wird behindert
Gültige Konten				Entfernen des Indikators beim Host: Löschen der Windows-Ereignisprotokolle	Erkennen von Dateien und Verzeichnissen				Verunstaltung
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt				Änderung der Domainrichtlinie: Änderung der Gruppenrichtlinie	Erkennung von Sicherheitssoftware				
Sicherheitslücken in der Lieferkette									

PYSA/Mespinoza

PYSA-Ransomware tritt auch unter dem Namen „Mespinoza“ auf und wurde erstmals im Oktober 2019 identifiziert. Die Gruppe nimmt Opfer aus unterschiedlichen Branchen und Ländern aufs Korn und machte insbesondere mit Attacken auf „weiche Ziele“ wie Bildungseinrichtungen und Krankenhäuser auf sich aufmerksam.

Infektionsverlauf

Der Erstzugriff erfolgt über Spam-E-Mails oder gehackte RDP-Anmeldedaten. Mit Scanning-Tools wie Port Scanner und dem Advanced IP Scanner von Famatech Corp werden dann Informationen zum Netzwerk erfasst. Im nächsten Schritt kommen Post-Exploitation-Tools wie Mimikatz, PowerShell Empire, Koadic und PsExec zum Einsatz, mit denen die Angreifer Anmeldedaten stehlen und sich laterale Bewegungsfreiheit verschaffen. Teilweise wurde zur Exfiltration von Daten aus den Systemen der Angriffsopfer auch das WinSCP-Tool verwendet. Ein PowerShell-Skript deaktiviert dann die Sicherheitssoftware und löscht Schattenkopien und Systemwiederherstellungspunkte, damit die Daten nicht aus der Backup-Sicherung wiederhergestellt werden können. Erst danach wird die eigentliche PYSA-Ransomware implementiert und ausgeführt, um die Daten des Opfers zu verschlüsseln.

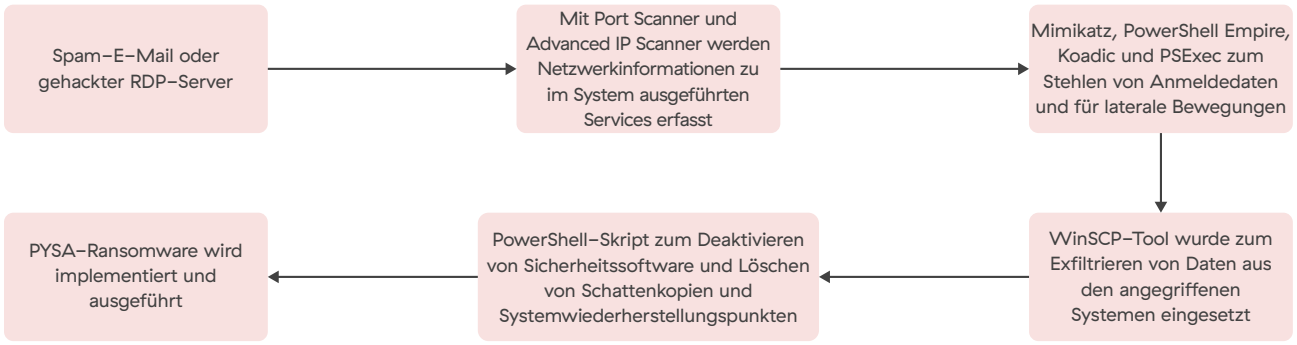


Abb. 13: Anatomie eines Ransomware-Angriffs mit PYSA

18 % der PYSA-Angriffe richteten sich gegen Bildungseinrichtungen.

PYSA verschlüsselt Dateien mit einer Kombination aus RSA- und AES-CBC-Algorithmen.

Abb. 14 zeigt, welche Branchen von PYSA/Mespinoza-Angriffen mit Doppelerpressung betroffen waren.

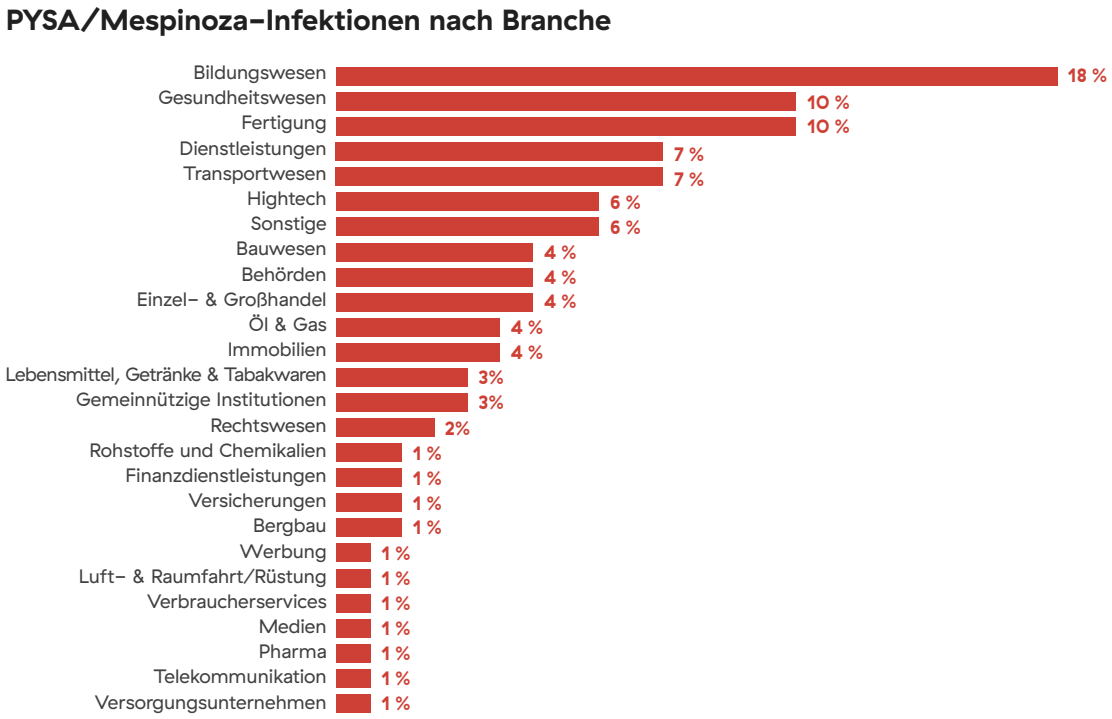


Abbildung 14: PYSA/Mespinoza-Angriffe nach Branche

Bei Verweigerung der Lösegeldzahlung werden gestohlene Daten auf der Dataleak-Website von PYSA veröffentlicht.

Abb. 15: Dataleak-Website von PYSA/Mespinoza

PYSA/Mespinoza: MITRE ATT&CK Taktiken & Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmecha-nismen	Erkennung	Laterale Bewegung	Sammlung	Exfiltration	Auswirkungen
Spearphishing-Link	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung	Manipulation von Zugriffstokens	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen der Netzwerkkonfi-guration	Lateraler Tool-Transfer	Erfasste Daten werden archiviert	Exfiltration über alternatives Protokoll	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch Modul-Load	Geplanter Task/Job		Schutzmecha-nismen werden beeinträchtigt	Erkennen von Remote-Systemen		Daten aus dem lokalen System	Exfiltration über Webservice	Systemwieder-herstellung wird behindert
Gültige Konten	Ausführung durch User			Änderung der Domainrichtlinie: Änderung der Gruppenrichtlinie	Erkennen von Dateien und Verzeichnissen				
					Erkennung von Sicherheitssoft-ware				
					Anfrage an die Registry				

REvil/Sodinokibi

REvil ist auch unter dem Namen „Sodinokibi“ bekannt, wurde erstmals im April 2019 identifiziert und zählt zu den aktivsten Ransomware-Gruppen der vergangenen Jahre. REVil wird ebenfalls über ein RaaS-Ökosystem verbreitet. Die erste Doppelerpressung mit einer REvil-Ransomware wurde im Januar 2020 dokumentiert, wobei die gestohlenen Daten zunächst in einem Hacker-Forum veröffentlicht wurden. Seit Februar 2020 betreiben die REvil/Sodinokibi-Angreifer eine eigene Dataleak-Website (siehe Abb. 16).

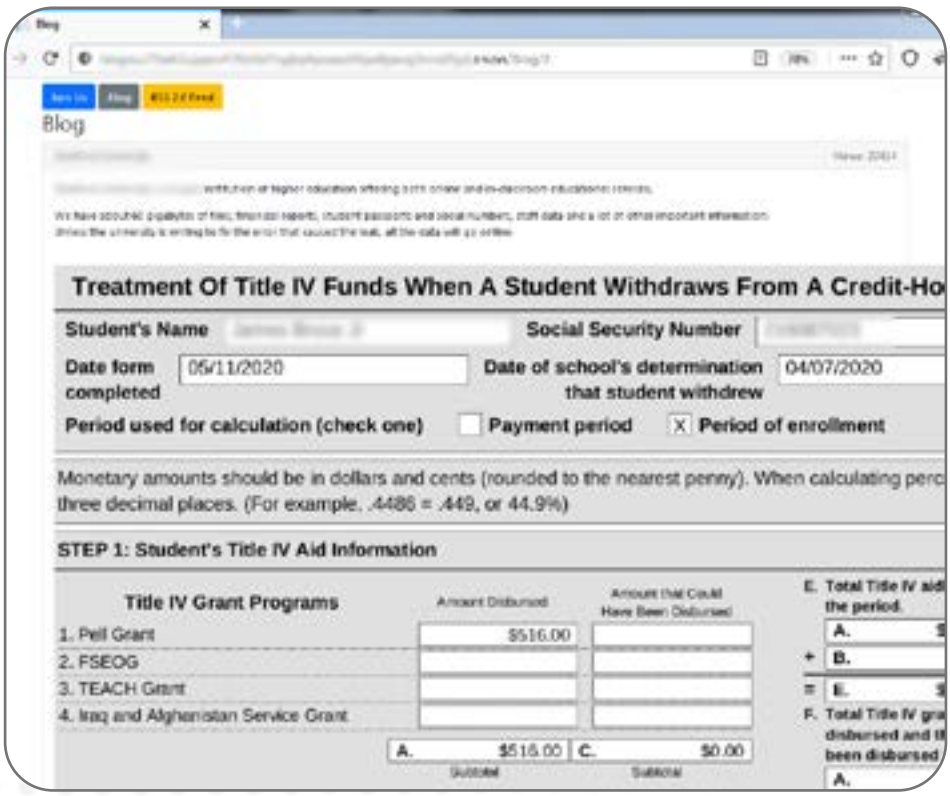


Abb. 16: Dataleak-Website von REvil/Sodinokibi

Das Experiment, gestohlene Daten über ihre Dataleak-Website zu versteigern, erwies sich als erfolglos und wurde wieder eingestellt.

Mediales Aufsehen erregte die REvil-Gruppe insbesondere durch Ausnutzen einer Zero-Day-Schwachstelle im Kaseya-VSA-Server im Juli 2021, über die dann schädliche Skripte an sämtliche von dem gehackten VSA-Server verwalteten Clients verschickt wurden.

Wie bereits erwähnt, wurden Mitglieder von REvil im Januar 2022 angeblich von den russischen Strafverfolgungsbehörden verhaftet. Im April 2022 wurde die Ransomware jedoch aktualisiert und die Infrastruktur wieder online gestellt. Seitdem werden neue REvil-Angriffe verzeichnet.

Infektionsverlauf

REvil-Affiliates nutzen unterschiedliche Mechanismen für den Erstzugriff, u. a. Spam-E-Mails, Exploit-Kits, gehackte RDP-Konten und Sicherheitslücken. Eine typische Angriffskampagne beginnt mit einer Spam-E-Mail mit schädlichem Anhang. Beim Öffnen des Anhangs wird ein Trojaner wie z. B. IcedID heruntergeladen, der als Vektor für laterale Bewegungen fungiert. REvil-Affiliates setzen eine Reihe unterschiedlicher Post-Exploitation-Tools (u. a. Cobalt Strike, SharpSploit und Mimikatz) ein, um Anmeldedaten zu stehlen (siehe Abb. 17). Zum Erfassen von Netzwerkinformationen werden Network-Discovery-Tools wie Netscan, BloodHound, AdFind usw. eingesetzt. Die Angreifer nutzen den Zugriff auf PsExec oder RDP aus, um sich ungehindert lateral durchs Netzwerk zu bewegen. Daten werden mit FileZilla, Rclone, MEGAsync oder FreeFileSync exfiltriert. Vor der Implementierung der eigentlichen Ransomware setzen REvil-Affiliates PC Hunter, Process Hacker, KillAV und/oder weitere Skripte ein, um sicherheitsbezogene Prozesse und Services zu beenden. Im letzten Schritt wird die REvil-Ransomware zur Verschlüsselung von Daten implementiert.

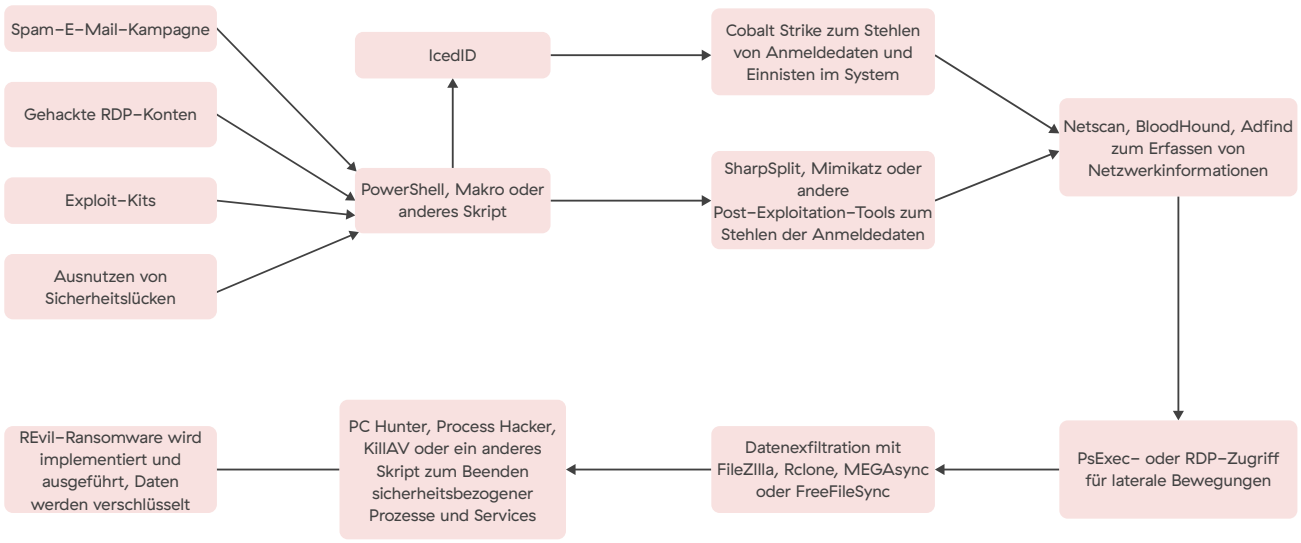


Abb. 17: Verlauf eines REvil/Sodinokibi-Angriffs

REvil verschlüsselt Dateien mit ECC-Algorithmen. Konkret kommt eine Kombination aus Curve25519 und Salsa20 zum Einsatz.

Abb. 18 zeigt, welche Branchen von REvil-Angriffen mit Doppelerpressung betroffen waren.

REvil/Sodinokibi-Infektionen nach Branche

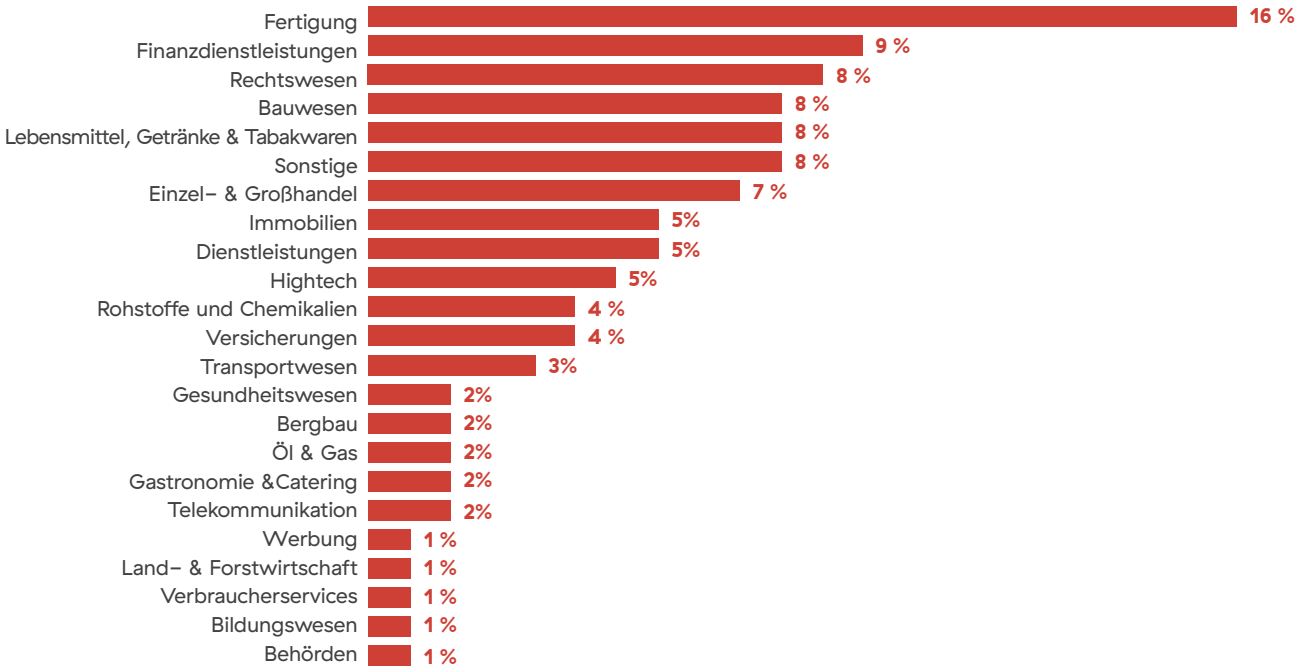


Abb. 18: REvil/Sodinokibii-Infektionen nach Branche

REvil/Sodinokibi: MITRE ATT&CK Taktiken & Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrme-chanismen	Erkennung	Laterale Bewegung	Datenerfas-sung	Exfiltration	Auswirkung
Spearphishing-Link	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung	Manipulation von Zugriffstokens	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen der Netzwerk-konfiguration	Lateraler Tool-Transfer	Erfasste Daten werden archiviert	Automatische Exfiltration	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch Modul-Load	Pfadunterbre-chungen durch Erstellung ausführbarer Programm-dateien	Pfadunterbrechun-gen durch Erstellung ausführbarer Programmdateien	Schutzmecha-nismen werden beeinträchtigt	Erkennen von Remote-Systemen	Remote-Services	Daten aus dem lokalen System	Exfiltration über Webservice	Systemwieder-herstellung wird behindert
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Geteilte Module		Ausnutzung zur Rechteerhöhung		Erkennen von Dateien und Verzeichnissen				Herunterfahren/ Neustart des Systems
Drive-by Compromise	Ausführung durch User				Erkennung von Sicher-heitssoftware				Verunstaltung
Gültige Konten					Anfrage an die Registry				
Sicherheits-lücken in der Lieferkette									

Avaddon

Avaddon-Ransomware wurde erstmals im Juni 2020 identifiziert und war zu diesem Zeitpunkt sehr aktiv. Die Avaddon-Gruppe nutzte ebenfalls ein RaaS-Ökosystem zur Verbreitung ihrer Ransomware. Seit Januar 2021 setzt Avaddon zusätzlich DDoS-Taktiken zur Durchführung von Dreifacherpressungen ein. Durch DDoS-Angriffe auf die Website oder das Netzwerk des Opfers sollten die betroffenen Organisationen zu Verhandlungen mit den Betreibern bewegt und höhere Lösegeldzahlungen erzwungen werden.

Infektionsverlauf
Avaddon-Ransomware wurde von verschiedenen Affiliates verbreitet, wobei der Erstzugriff über eine Reihe unterschiedlicher Vektoren erfolgte. In den meisten Fällen kamen Spam-Kampagnen und Exploit-Kits zum Einsatz, teils verschafften sich die Affiliates aber auch durch Brute-Force-Angriffe oder gehackte RDP- und VPN-Anmeldedaten Zugang zu den jeweiligen Netzwerken.

Bei einem typischen Angriffsverlauf verschaffte Avaddon sich zunächst Zugriff zu einem Broker, der mithilfe gehackter Anmeldedaten infiziert wurde. Dann kam spezifisch angepasste Malware (u. a. Webshells wie BlackCrow and DarkRaven) zum Einsatz, mit der die Angreifer sich im System einnisteten. Avaddon verschaffte sich über SystemBC Zugriff auf infizierte Hosts und setzte dann Mimikatz und SharpDump zum Diebstahl von Anmeldedaten ein. Als Post-Exploitation-Tools kamen SoftPerfect Network Scanner, PowerSploit und Empire zum Scannen des Netzwerks zum Einsatz. Die Avaddon-Affiliates nutzten RDP für laterale Bewegungen und den Taskplaner von Windows, um unerkannt im System zu verbleiben. Vor Implementierung und Ausführung der eigentlichen Avaddon-Payload zur Verschlüsselung der betroffenen Systeme wurden Daten mit MEGAsync exfiltriert und sicherheitsbezogene Prozesse und Services beendet.

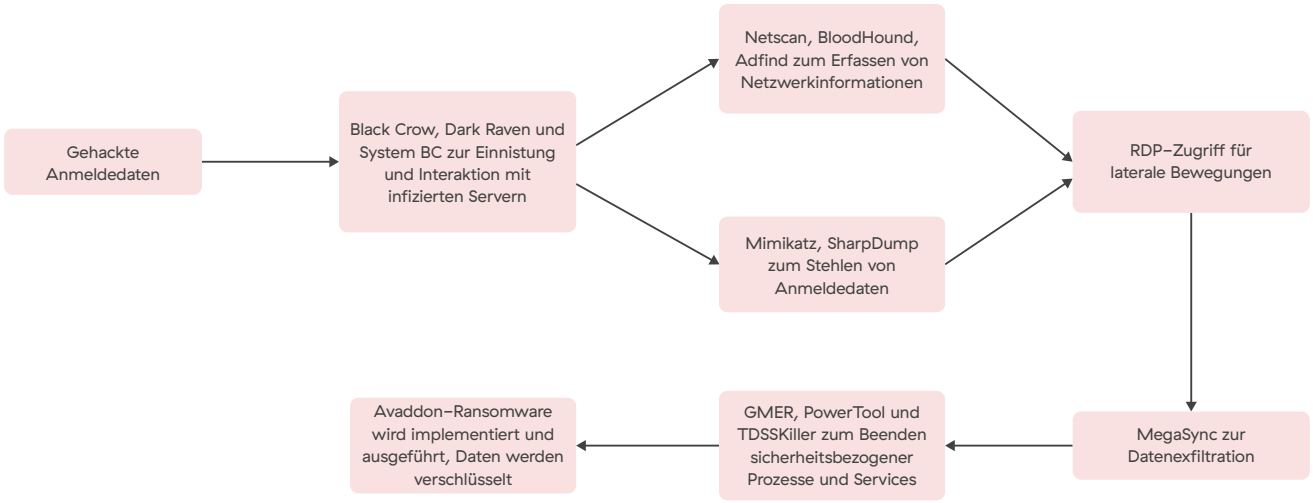


Abb. 19. Anatomie eines Ransomware-Angriffs mit Avaddon

Avaddon verschlüsselte Dateien mit einer Kombination aus RSA- und AES-Algorithmen. Im Februar 2021 veröffentlichte ein Bedrohungsforscher ein kostenloses Entschlüsselungstool, woraufhin Avaddon den zugrundeliegenden Fehler in der Ransomware behob. Im Juni 2021 stellte Avaddon den Betrieb ein und gab den Code zur Entschlüsselung der Daten betroffener Unternehmen frei. Daraufhin entwickelte Emsisoft einen Decrypter zur Entschlüsselung von Avaddon-Ransomware.

Ähnlich wie die anderen bereits erwähnten Ransomware-Familien erstellte Avaddon im August 2019 eine eigene Dataleak-Website (siehe Abb. 20).

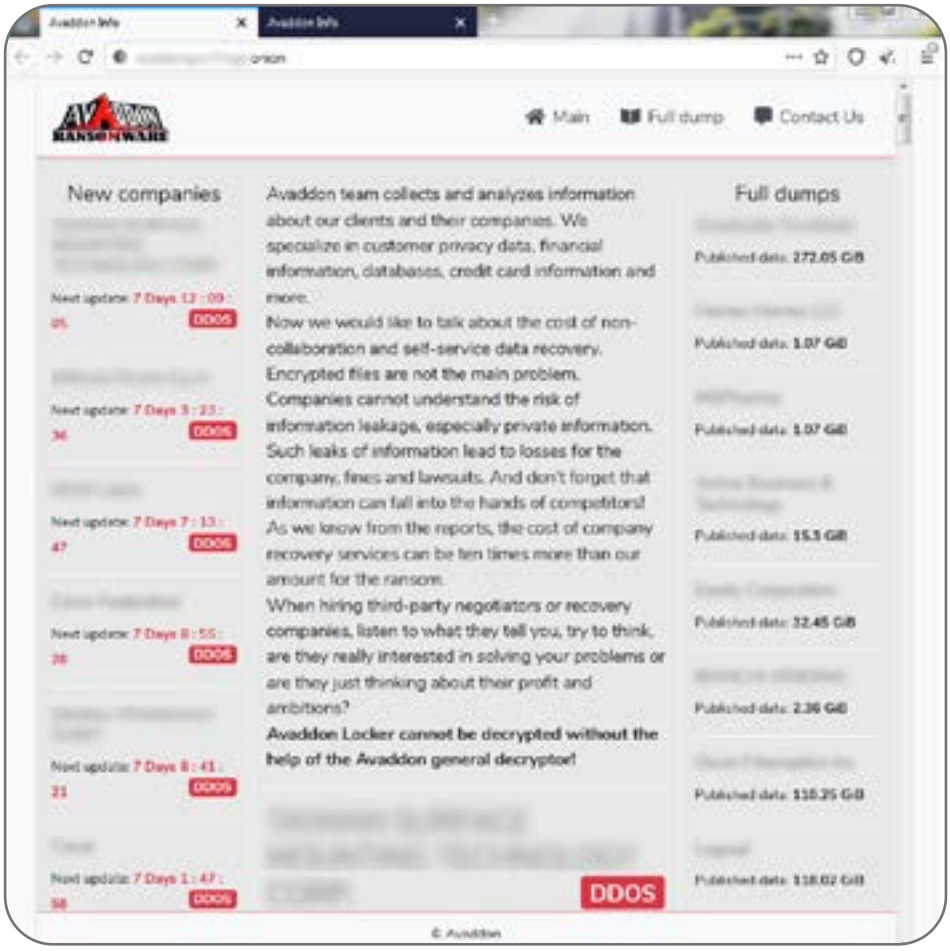


Abb. 20: Dataleak-Website von Avaddon

Im Anschluss an die Einstellung von Avaddon nutzte die gleiche Gruppe den Ransomware-Builder von Thanos, um erneut Angriffe zu starten. Avaddon wurde zunächst in „Haron“ und im Oktober 2021 in „Midas“ umbenannt.

Abb. 21 zeigt, welche Branchen von Avaddon–Angriffen mit Doppelerpressung betroffen waren.

Avaddon–Infektionen nach Branche

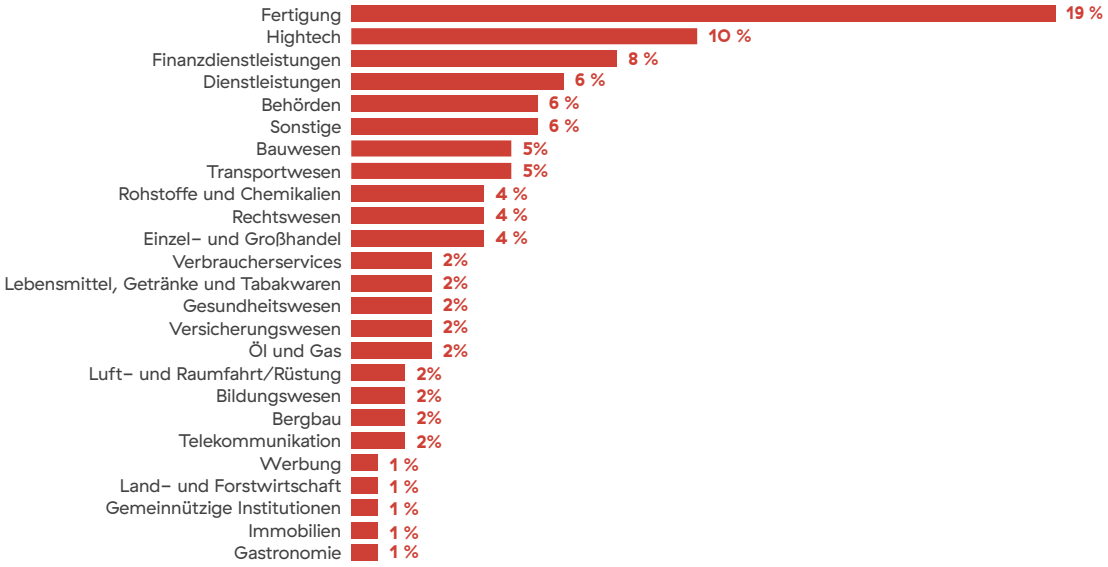


Abb. 21: Avaddon–Infektionen nach Branche

Avaddon — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechte–erhöhung	Umgehen von Abwehrme–chanismen	Erkennung	Laterale Bewegung	Daten–erfassung	Exfiltration	Auswir–kung
Spearphishing–Link	Command–Line Interface	Boot– oder Logon–Autostart–Ausführung	Gültige Konten	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen der Netzwerk–konfiguration	Lateraler Tool–Transfer	Erfasste Daten werden archiviert	Exfiltration über alternatives Protokoll	Daten werden verschlüsselt
Spearphishing–Anhang	Geplanter Task/Job	Gültige Konten		Schutzmecha–nismen werden beeinträchtigt	Erkennen von Remote–Systemen	Remote Services:	Daten aus dem lokalen System		System–wiederher–stellung wird behindert
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Ausführung durch User			Process Injection	Erkennen von Dateien und				
Drive–by Compromise				Entfernen des Indikators beim Host	Erkennung von				
Gültige Konten				Entfernen des Indikators beim Host	Erkennung von				

Clop

Ransomware der Clop-Familie trat erstmals im Februar 2019 in Erscheinung. Im März 2020 begann Clop mit Doppelerpressungen, bei der gestohlene Daten von kompromittierten Organisationen weitergegeben wurden, wenn sie kein Lösegeld an ihre Dataleak-Websites zahlten (siehe Abbildung 22).

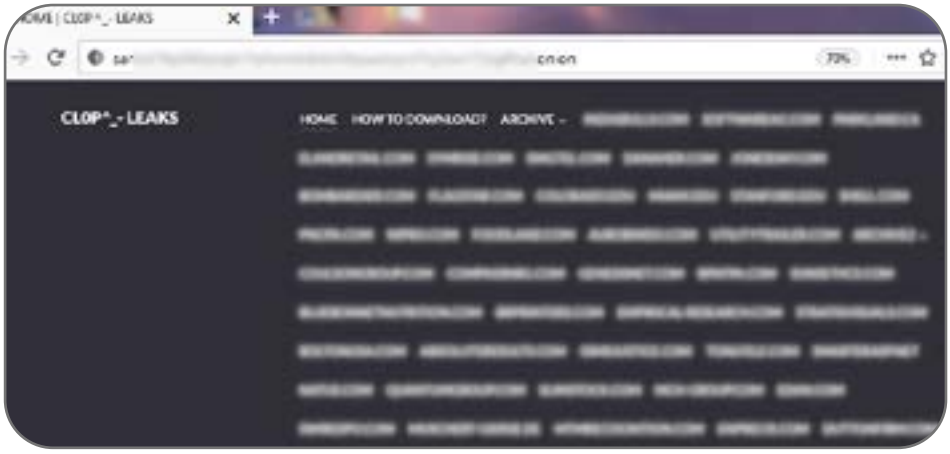


Abb. 22: Dataleak-Website von Clop

Die Clop-Ransomware zielt hauptsächlich auf große Organisationen ab. Wie ThreatLabz beobachten konnte, fordert die Clop-Ransomware-Gruppe achtstellige Lösegeldbeträge und lehnte sogar Lösegeld-Angebote in Höhe von mehreren Millionen US-Dollar ab.

Clop-Ransomware wurde ursprünglich durch die Bedrohungsgruppen TA505 und FIN11 eingesetzt und fand durch Spam-Kampagnen des Bedrohungsakteurs TA505 weite Verbreitung. ThreatLabz hat mehrere Clop-Angriffe beobachtet, bei denen die Schwachstelle SolarWinds Serv-U CVE-2021-35211 ausgenutzt wurde. Dadurch war die Remote-Codeausführung mit zusätzlichen Rechten möglich, um Erstzugriff zu erlangen. Die Bedrohungsgruppe FIN11 nutzt mehrere Sicherheitslücken in der Accellion File Transfer Appliance (FTA) aus, und zwar CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 und CVE-2021-27104. Anschließend legt FIN11 die DEWMODE-Webshell zur Datenexfiltration ab, gefolgt von der Clop-Ransomware, die dann ausgeführt wird.

Clop nimmt prominente Angriffsziele ins Visier und hat bereits Schäden in Höhe von 500 Mio. USD verursacht (Schätzwert; Stand: Nov. 2021).

Infektionskette

Bei einem Angriff gelang TA505 die Kompromittierung über eine Spam-E-Mail mit einem HTML-Anhang. Der Anhang leitete den User zu einer XLS-Dokumentdatei weiter, die den Get2-Loader ablegte. Der Loader lud weitere Payloads wie SdBot, FlawedAmmy, FlawedGrace und Cobalt Strike herunter. Nachdem man im Netzwerk Fuß gefasst und Daten gestohlen und exfiltriert hatte, setzte die Bedrohungsgruppe die Clop-Ransomware ein und führte sie wie in Abbildung 23 dargestellt aus.

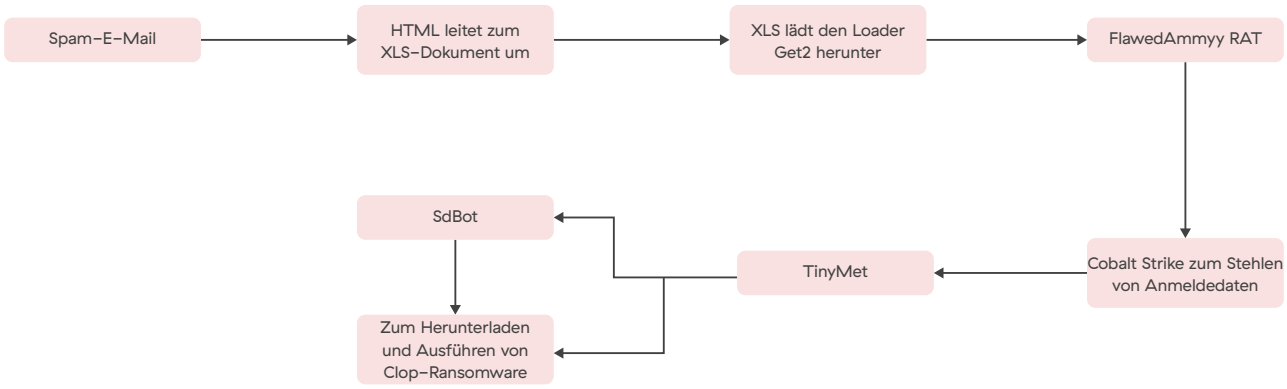


Abb. 23: Anatomie eines Ransomware-Angriffs mit Clop

Clop verschlüsselt Dateien mit einer Kombination aus RSA- und AES-Algorithmen.

Abb. 24 zeigt, welche Branchen von Clop-Angriffen mit Doppelerpressung betroffen waren.

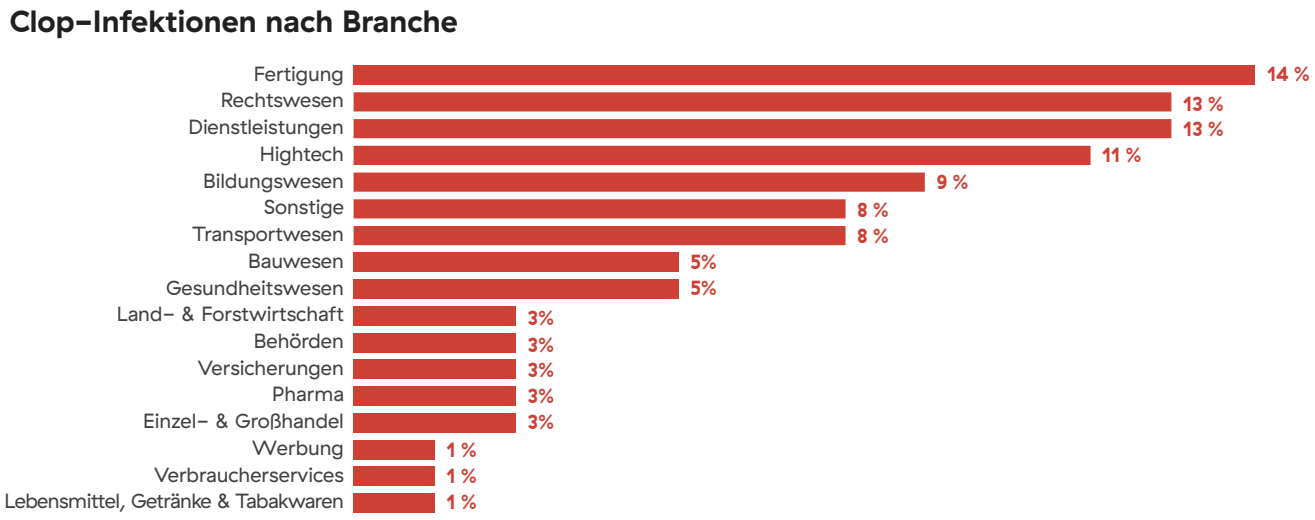


Abb. 24: Clop-Infektionen nach Branche

Clop — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkung
Gültige Konten	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung	Manipulation von Zugriffstokens	Masquerading: Ungültige Code-Signatur	Erkennen der Netzwerkkonfiguration	Lateraler Tool-Transfer	Automatische Exfiltration	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch User	Systemprozess wird erstellt oder modifiziert: Windows-Service	User Account Control wird umgangen	Schutzmechanismen werden beeinträchtigt: Tools werden deaktiviert oder modifiziert	Erkennen von Remote-Systemen	Remote-Services	Exfiltration über Webservice	Systemwiederherstellung wird behindert
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Native API		Ausnutzung zur Rechteerhöhung	Verschleierung/Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Dateien und Verzeichnissen			
Sicherheitslücken in der Lieferkette				Process Injection: DLL-Injection	Anfrage an die Registry			
				Indirekte Ausführung von Befehlen	Erkennung von Sicherheitssoftware			

Grief

Grief-Ransomware ist eine Abwandlung von DoppelPaymer, deren Aktivität im Mai 2021 nach dem Angriff auf die Colonial Pipeline erheblich zurückging. Grief-Ransomware hat viele Ähnlichkeiten mit DoppelPaymer, etwa einen gemeinsam genutzten Ransomware-Code und Dataleak-Websites. Einen Beispiel-Screenshot der Dataleak-Website von Grief zeigt Abbildung 25.

Abb. 25: Dataleak-Website von Grief

Das Lösegeldportal von Grief weist einige Unterschiede zum Portal von DoppelPaymer auf. Ein Hauptunterschied ist, dass die Lösegeldzahlung in Monero anstatt Bitcoin abgewickelt wird. Dieser Umstieg zu einer anderen Kryptowährung könnte eine Reaktion darauf sein, dass dem FBI die Wiedererlangung eines Teils der Lösegeldzahlung von Colonial Pipeline gelang, die in Bitcoin vorgenommen wurde.

Infektionskette

Grief-Ransomware wurde auf Systemen eingesetzt, die zuvor mit Dridex infiziert wurden. Dies nutzen die Angreifer, bevor sie Cobalt Strike verwenden und den Grief-Ransomware-Payload einsetzen und ausführen. Grief verschlüsselt Dateien mit einer Kombination aus 2048-Bit-RSA- und 256-Bit-AES-Algorithmen.

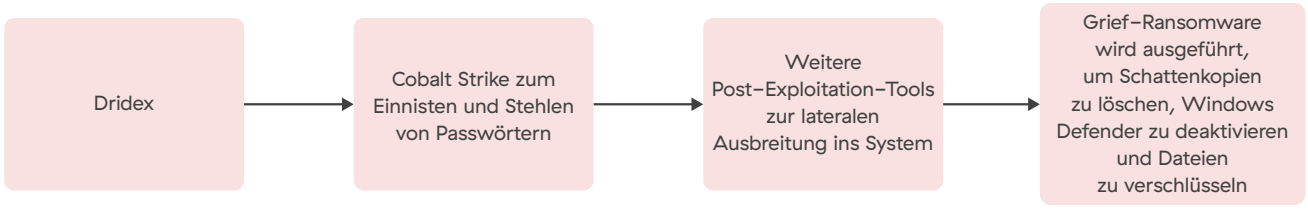


Abb. 26: Anatomie eines Ransomware-Angriffs mit Grief

Abb. 27 zeigt, welche Branchen von Grief-Angriffen mit Doppelerpressung betroffen waren.

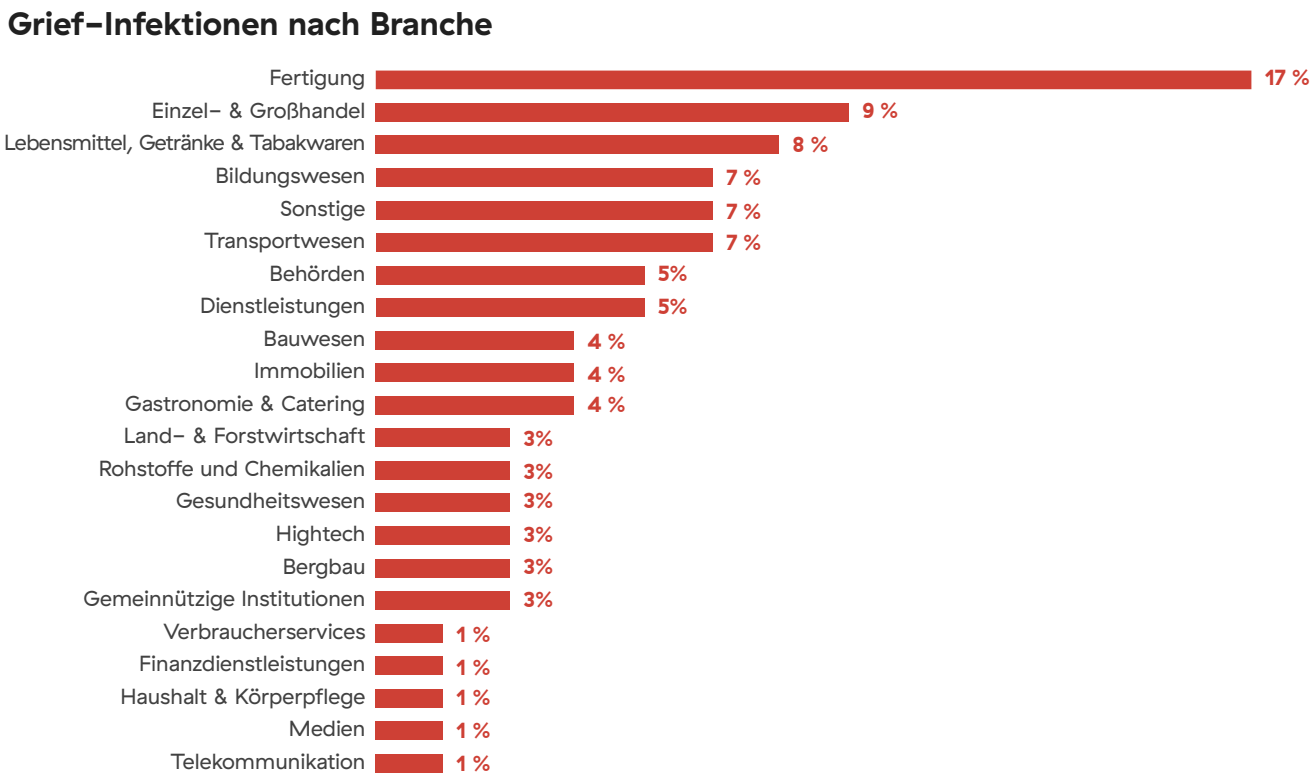


Abb. 27: Grief-Infektionen nach Branche

Grief — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkung
Gültige Konten	Command-Line Interface	Boot- oder Logon-Autostart-Ausführung: Registry-Schlüssel „Run“/Start-Ordner	Process Injection	Pfadunterbrechungen: Missbrauch der DLL-Suchreihenfolge	Erkennen der Netzwerkkonfiguration	Lateraler Tool-Transfer	Geplante Übertragung	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch User	Geplanter Task/Job		Verschleierung/Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Remote-Systemen			Systemwiederherstellung wird behindert
	Gemeinsam verwendete Module			Schutzmechanismen werden beeinträchtigt: Tools werden deaktiviert oder modifiziert	Erkennen von Dateien und Verzeichnissen			Herunterfahren/Neustart des Systems
				Masquerading: Gültiger Name oder Standort wird repliziert	Erkennung von Sicherheitssoftware			

Hive

Hive-Ransomware wurde erstmals im Juni 2021 als Teil eines RaaS-Modells entdeckt. Sie nutzt mehrere Mechanismen für den Erstzugriff, darunter Spam-E-Mails, geleakte VPN-Anmeldeinformationen sowie Sicherheitslücken in extern ausgerichteten Ressourcen. Die Erstinfektion beginnt mit der Ausnutzung der ProxyShell-Sicherheitslücken in Microsoft Exchange Server. ProxyShell Exchange-Sicherheitslücken sind eine Kombination aus CVE-2021-34473 (Sicherheitslücke bei der Remotecodeausführung bei Microsoft Exchange Server), CVE-2021-34523 (Sicherheitslücke im Zusammenhang mit der Ausweitung von Berechtigungen bei Microsoft Exchange Server) und CVE-2021-31207 (Sicherheitslücke im Zusammenhang mit der Umgehung der Sicherheitsfunktionen bei Microsoft Exchange Server).

Infektionskette

Der Angreifer erstellt in einem Postfach einen E-Mail-Entwurf mit einem Anhang, der die codierte Webshell enthält. Anschließend exportiert der Angreifer das gesamte Postfach (einschließlich der böswilligen E-Mail-Entwürfe) in das PST-Dateiformat mit einer ASPX-Erweiterung. So können Angreifer Webshells auf anfälligen Servern ablegen. Die Webshell lädt das PowerShell-Skript herunter, das die codierte Cobalt Strike-Payload enthält. Sie lädt weitere Stager herunter und fasst im System des Opfers Fuß. Anschließend verwendet sie Mimikatz, um NTLM-Hashes zu stehlen und greift anhand einer Pass-the-Hash-Taktik auf das Domain-Controller-Konto zu. Hive bewegt sich mithilfe gestohlener Anmeldeinformationen weiter lateral über RDP. Es scannt das Netzwerk und ruft mithilfe des Network-Scanners SoftPerfect zusätzliche Informationen ab. Zum Schluss wird die Hive-Ransomware bereitgestellt und ausgeführt und die Daten verschlüsselt.

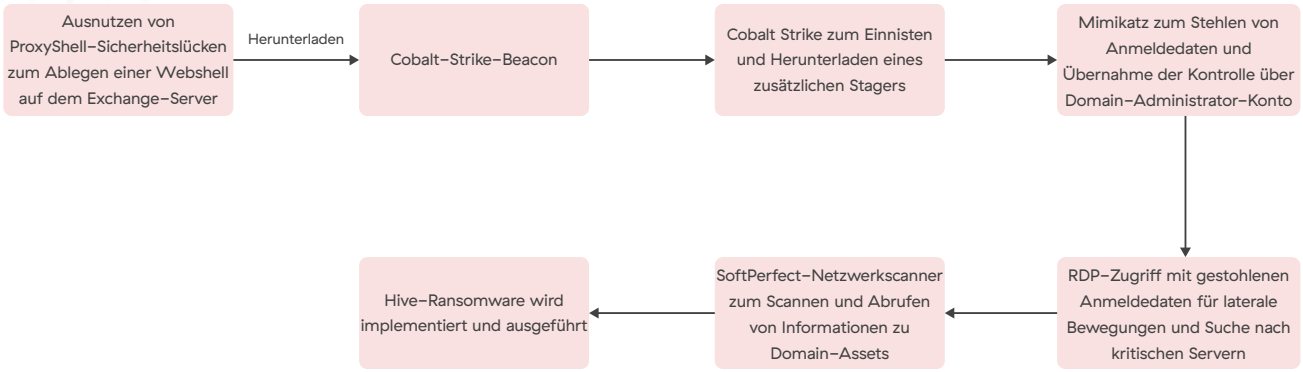


Abb. 28: Verlauf eines Hive-Angriffs

Frühere Versionen der Hive-Ransomware-Payload wurden in der Programmiersprache Go geschrieben und verwendeten zur Verschlüsselung der Dateien eine Kombination aus RSA- und AES-Algorithmen. Neuere Versionen von Hive sind in der Programmiersprache Rust geschrieben und verwenden Curve25519 und ChaCha20 für die Dateiverschlüsselung.

Hive-Affiliates exfiltrieren vor der Dateiverschlüsselung zudem Daten ihrer Opfer. Ein Screenshot der Dataleak-Website von Hive ist in Abbildung 29 zu sehen.

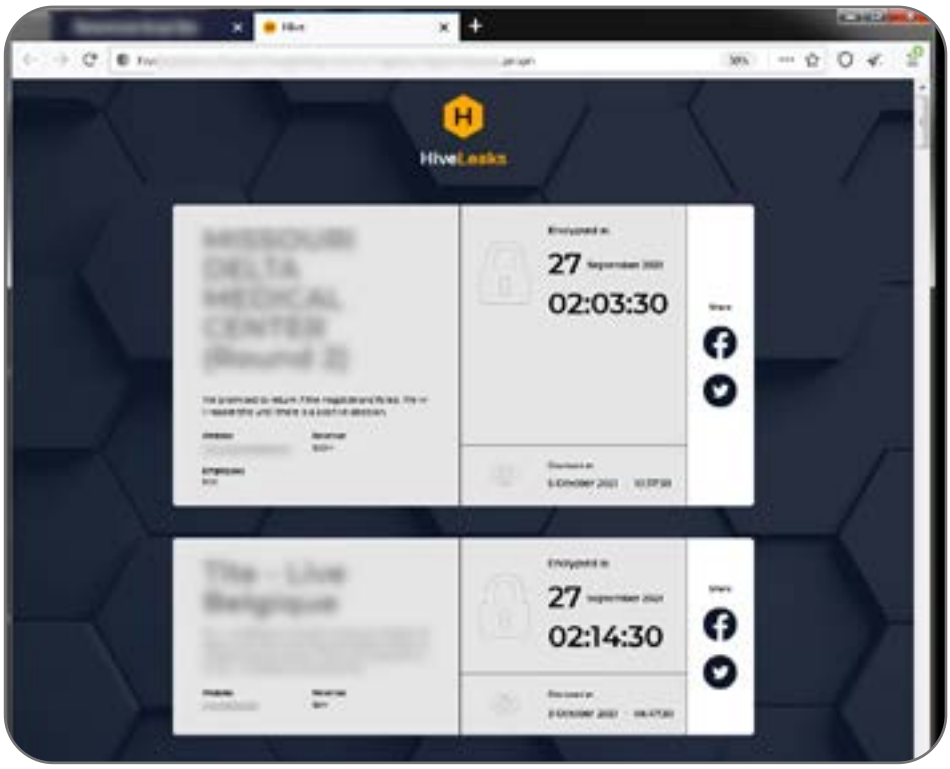


Abb. 29: Dataleak-Website von Hive

Abb. 30 zeigt, welche Branchen von Hive-Angriffen mit Doppelerpressung betroffen waren.

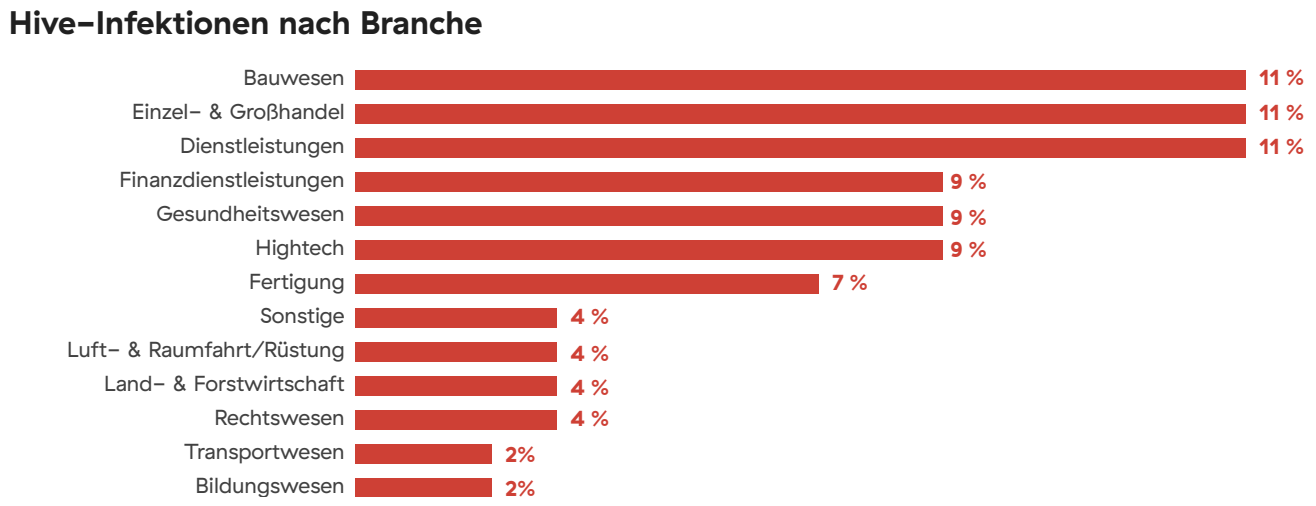


Abb. 30: Hive-Infektionen nach Branche

Hive — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkung
Externe Remote-Services	Command-Line Interface	Gültige Konten: Domain-Konten	Gültige Konten	Windows-Ereignisprotokolle werden gelöscht	Erkennen der Netzwerkkonfiguration	Remotedesktopprotokoll	Geplante Übertragung	Daten werden verschlüsselt
Spearphishing-Anhang	Ausführung durch User	Konto wird erstellt: Domain-Konto	Domain-Konten	Schutzmechanismen werden beeinträchtigt: Tools werden deaktiviert oder modifiziert	Erkennen von Remote-Systemen	Remote-Services		Systemwiederherstellung wird behindert
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt			Ausnutzung zur Rechteerhöhung	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Dateien und Verzeichnissen			
					Anfrage an die Registry			
					Erkennung von Sicherheitssoftware			

BlackByte

BlackByte ist eine weitere RaaS-Gruppe, die im Juli 2021 besonders in Erscheinung trat. Sie wurde ursprünglich in C# geschrieben und später, etwa im September 2021, in der Programmiersprache Go neu entwickelt. Die in Go verfasste Version weist zahlreiche Ähnlichkeiten mit der C#-Version auf, etwa die Befehle für laterale Verbreitung, Eskalation von Berechtigungen und Dateiverschlüsselung.

BlackByte-Kampagnen beginnen mit der Ausnutzung der ProxyShell-Sicherheitslücken im Microsoft Exchange Server.

Infektionskette
Der Angreifer erstellt einen E-Mail-Entwurf in einem Postfach. Die E-Mail hat einen Anhang, der die codierte Webshell enthält. Anschließend exportiert der Angreifer das gesamte Postfach (samt böswilliger E-Mail-Entwürfe) in das PST-Dateiformat mit einer ASPX-Erweiterung. Dadurch können Angreifer Webshells auf anfälligen Servern ablegen.

Als Nächstes wird die Webshell verwendet, um ein Cobalt Strike-Beacon auf dem anvisierten Exchange-Server abzulegen. Cobalt Strike und andere Post-Exploitation-Tools werden verwendet, um Anmeldeinformationen zu stehlen, Zugriff auf Dienstkonten zu erhalten und sich so im System zu etablieren. Darüber hinaus installiert BlackByte das RDP-Tool AnyDesk. AnyDesk wird für laterale Bewegungen und zum Ablegen von Cobalt Strike im infizierten Domänencontroller verwendet. Schließlich setzt Cobalt Strike die BlackByte-Ransomware ein und führt sie aus.

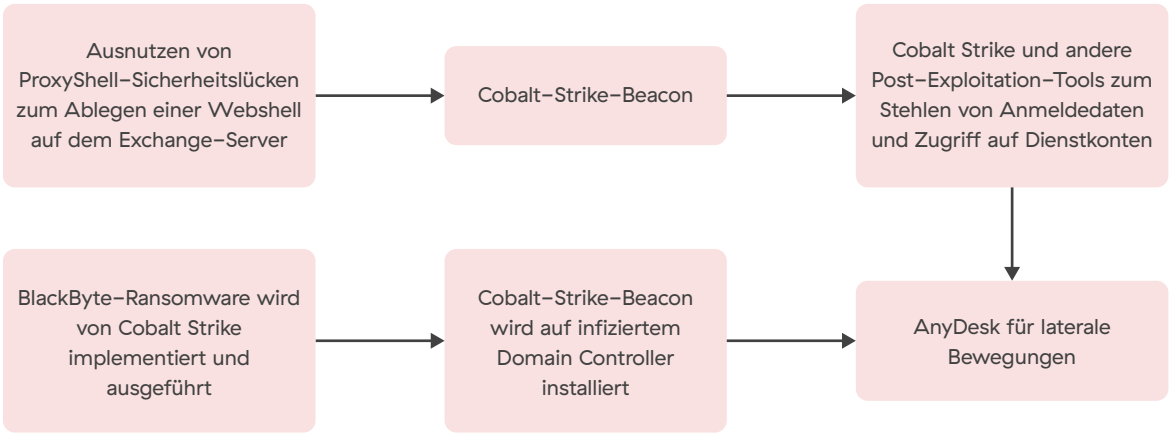


Abb. 31: Anatomie eines Ransomware-Angriffs mit BlackByte

Der Erstzugriff erfolgt durch Ausnutzen von ProxyShell-Sicherheitslücken, um das Ablegen einer Webshell auf dem Exchange-Server zu ermöglichen. Die Webshell lädt das Cobalt-Strike-Beacon herunter. Cobalt Strike stiehlt dann Anmeldeinformationen und installiert das RDP-Tool AnyDesk. AnyDesk wird für laterale Bewegungen und zum Ablegen von Cobalt Strike im infizierten Domänencontroller verwendet. Schließlich setzt Cobalt Strike die BlackByte-Ransomware ein und führt sie aus.

BlackByte verschlüsselt Dateien mit einer Kombination aus RSA- und AES-Algorithmen. Die neuesten BlackByte-Versionen verwenden Curve25519 ECC für asymmetrische Verschlüsselung und ChaCha20 für symmetrische Dateiverschlüsselung.

Die BlackByte-Akteure exfiltrieren vor der Dateiverschlüsselung zudem Daten ihrer Opfer. Ein Screenshot der Dataleak-Website von BlackByte ist in Abbildung 32 zu sehen.

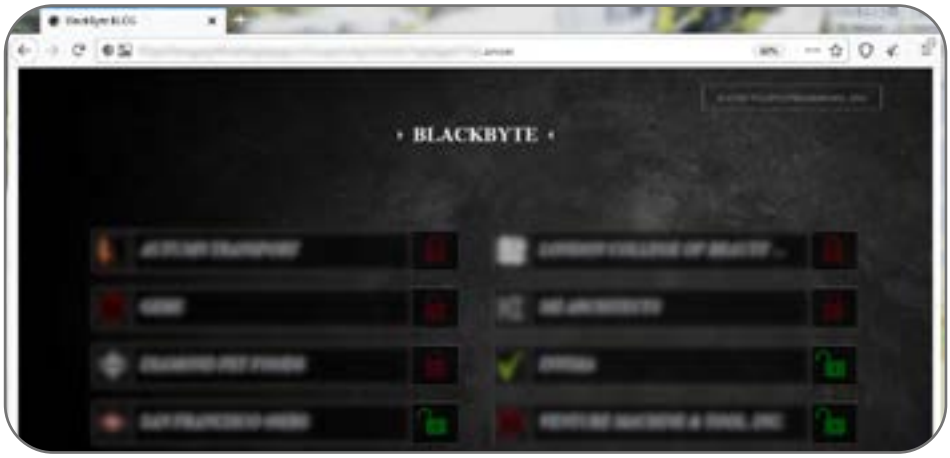


Abb. 32: Dataleak-Website von BlackByte

Abb. 33 zeigt, welche Branchen von BlackByte-Angriffen mit Doppelerpressung betroffen waren.

BlackByte-Infektionen nach Branche

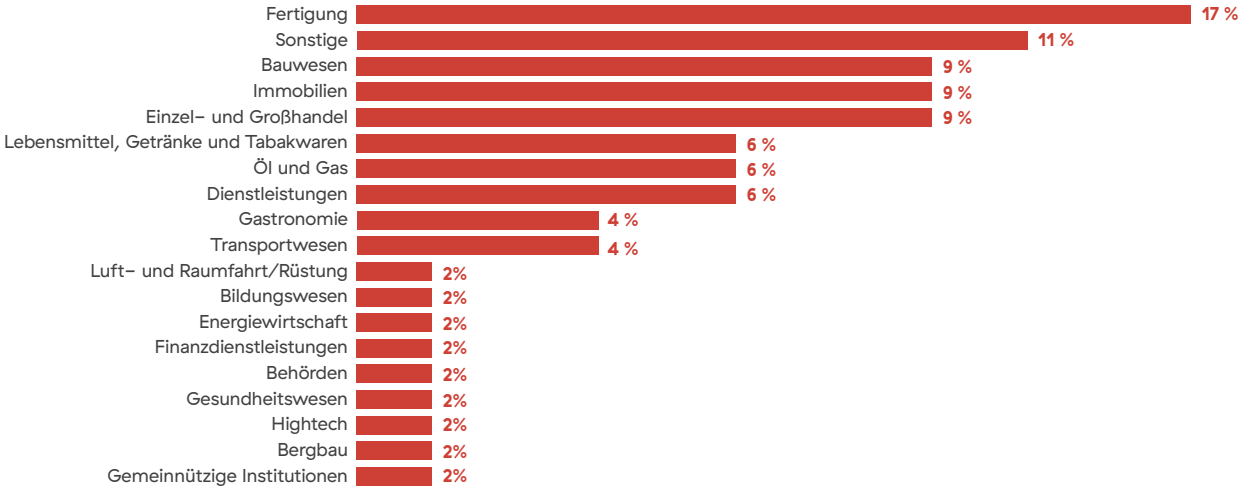


Abb. 33: BlackByte-Infektionen nach Branche

BlackByte — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrmechanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkung
Spearphishing-Anhang	Command- und Skript-Interpreter	Systemprozess wird erstellt oder modifiziert: Windows-Service	Domain-Konten	Schutzmechanismen werden beeinträchtigt: Tools werden deaktiviert oder modifiziert	Erkennen der Netzwerkkonfiguration	Lateraler Tool-Transfer	Geplante Übertragung	Daten werden verschlüsselt
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Native API		Ausnutzung zur Rechteerhöhung	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Remote-Systemen			Systemwiederherstellung wird behindert
	Ausführung durch User			Registry wird modifiziert	Erkennen von Dateien und Verzeichnissen			
					Anfrage an die Registry			
					Erkennung von Sicherheitssoftware			

AvosLocker

AvosLocker-Ransomware ist eine RaaS-Gruppe, die besonders im Juli 2021 in Erscheinung trat. Wie bei Hive und BlackByte beginnt die Erstinfektion mit der Ausnutzung der ProxyShell-Sicherheitslücken CVE-2021-34473, CVE-2021-34523 und CVE-2021-31207, die auf dem Microsoft Exchange-Server bestehen.

Infektionskette

Der Angreifer erstellt einen E-Mail-Entwurf in einem Postfach. Die E-Mail hat einen Anhang, der die codierte Webshell enthält. Anschließend exportiert der Angreifer das gesamte Postfach (samt böswilliger E-Mail-Entwürfe) in das PST-Dateiformat mit einer ASPX-Erweiterung. Dadurch können Angreifer Webshells auf anfälligen Servern ablegen.

Als Nächstes werden die Webshells verwendet, um Cobalt Strike auf dem infizierten Exchange-Server abzulegen. Cobalt Strike und Rclone stehlen Anmeldeinformationen und exfiltrieren Daten an Remote-Server.

Dabei wird das RDP-Tool AnyDesk unter lateraler Bewegung auf mehreren Systemen installiert. Es legt mehrere Batch-Skripts ab, um Registry-Schlüssel für Sicherheitssoftware ändern und löschen zu können. Außerdem werden Windows Update und Windows Defender deaktiviert.

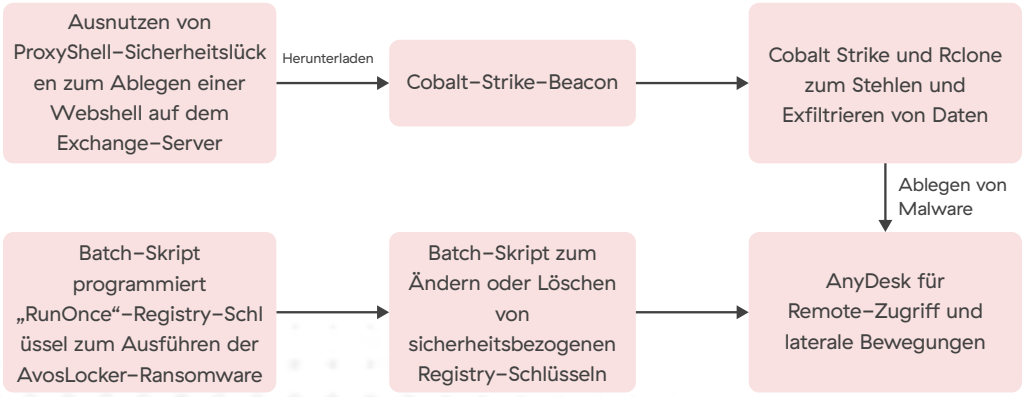


Abb. 34: Anatomie eines Ransomware-Angriffs mit AvosLocker

Schließlich startet AvosLocker das System im abgesicherten Modus von Windows neu, woraufhin die Ransomware mit der Dateiverschlüsselung beginnt. Durch das Booten im abgesicherten Modus kann AvosLocker möglichst viele Dateien verschlüsseln, da Geschäftsanwendungen wie Datenbanken wahrscheinlich nicht ausgeführt werden. So haben diese Anwendungen keine offenen Dateihandles, die die Dateiverschlüsselung verhindern könnten. Darüber hinaus werden viele Anwendungen für Sicherheitssoftware (z. B. Antivirenprogramme) standardmäßig nicht geladen, wenn das System im abgesicherten Modus ausgeführt wird. Auch andere Ransomware-Familien wie Conti, REvil und BlackMatter waren bereits in der Lage, Dateien im abgesicherten Modus von Windows zu verschlüsseln.

AvosLocker verwendet zur Dateiverschlüsselung eine Kombination aus RSA- und AES-Algorithmen. Von AvosLocker stammt eine Linux-Version der Ransomware, die auf VMware ESXi abzielt.

Nach dem Angriff droht der Angreifer, die Daten des Opfers auf einer Dataleak-Website zu veröffentlichen. In einigen Fällen droht er während der Verhandlungen mit einem DDoS-Angriff auf das Opfernetzwerk bzw. führt ihn direkt aus. Ein Screenshot der Dataleak-Website von AvosLocker ist in Abbildung 35 zu sehen.

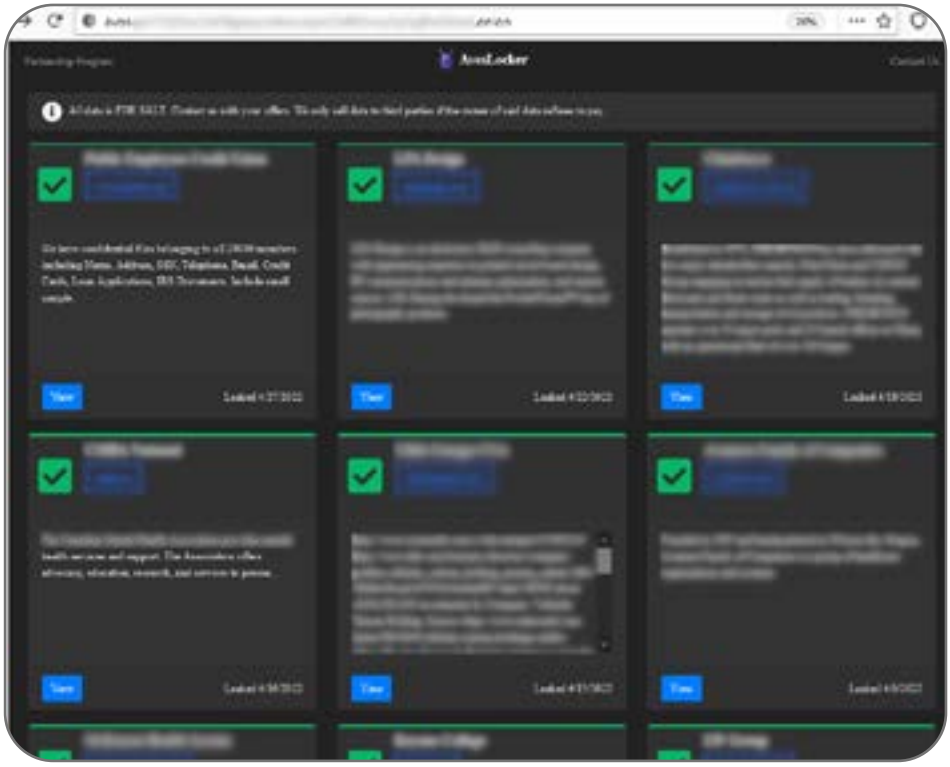


Abb. 35: Dataleak-Website von AvosLocker

Abb. 36 zeigt, welche Branchen von AvosLocker–Angriffen mit Doppelerpressung betroffen waren.

AvosLocker–Infektionen nach Branche

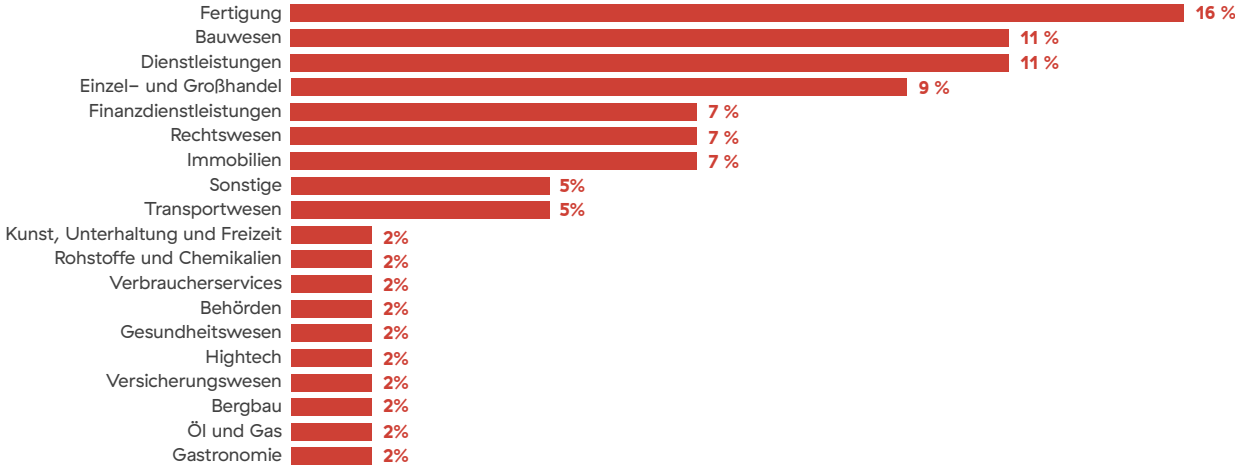


Abb. 36: AvosLocker–Infektionen nach Branche

AvosLocker — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehrme–chanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkungen
Spearphishing–Anhang	Command–Line Interface	Boot– oder Logon–Autostart–Ausführung: Registry–Schlüssel „Run“/ Start–Ordner	Domain–Konten	Schutzmecha–nismen werden beeinträchtigt: Tools werden deaktiviert oder modifiziert	Erkennen der Netzwerkkonfi–guration	Lateraler Tool–Transfer	Geplante Übertragung	Daten werden verschlüsselt
Öffentlich zugängliche Anwendungen werden als Einfallsvektor ausgenutzt	Ausführung durch User	Geplanter Task/Job	Ausnutzung zur Rechteerhöhung	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Remote–Systemen			Systemwieder–herstellung wird behindert
					Erkennen von Dateien und Verzeichnissen			Herunterfahren/ Neustart des Systems
					Erkennung von Sicherheitssoft–ware			

BlackCat/ALPHV

BlackCat, auch bekannt als ALPHV, ist eine RaaS-Operation, die erstmals im November 2021 auffällig wurde. BlackCat nutzt RUST als Programmiersprache, was die Performance verbessert und eine zuverlässige gleichzeitige Verarbeitung sicherstellt.

Infektionskette

Die Erstinfektion beginnt mit der Verwendung kompromittierter Anmeldeinformationen, um Zugriff auf die Netzwerksysteme der Opfer zu erhalten. Zunächst wird versucht, mit Cobalt Strike, PowerShell-Skripten und Batch-Skripts im Netzwerk des Opfers Fuß zu fassen. Sobald Zugriff besteht, werden Admin-Konten in Active Directory kompromittiert. Darüber hinaus kommen bösartige Group Policy Objects (GPOs) zum Einsatz, die Ransomware einschleusen und ausführen. Zudem werden Microsoft Sysinternals und andere Verwaltungstools bei dem Angriff genutzt.

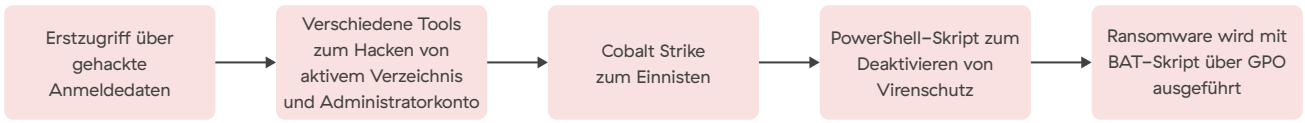


Abb. 37: Anatomie eines Ransomware-Angriffs mit BlackCat/ALPHV

BlackCat setzt mittlerweile zusätzlich DDoS-Taktiken ein. DDoS-Angriffe auf die Website oder das Netzwerk des Opfers dienen dazu, das betroffene Unternehmen zu Verhandlungen mit den Betreibern zu bewegen und höhere Lösegeldzahlungen zu erzwingen. Ein Screenshot der Dataleak-Website von BlackCat ist in Abbildung 38 zu sehen.

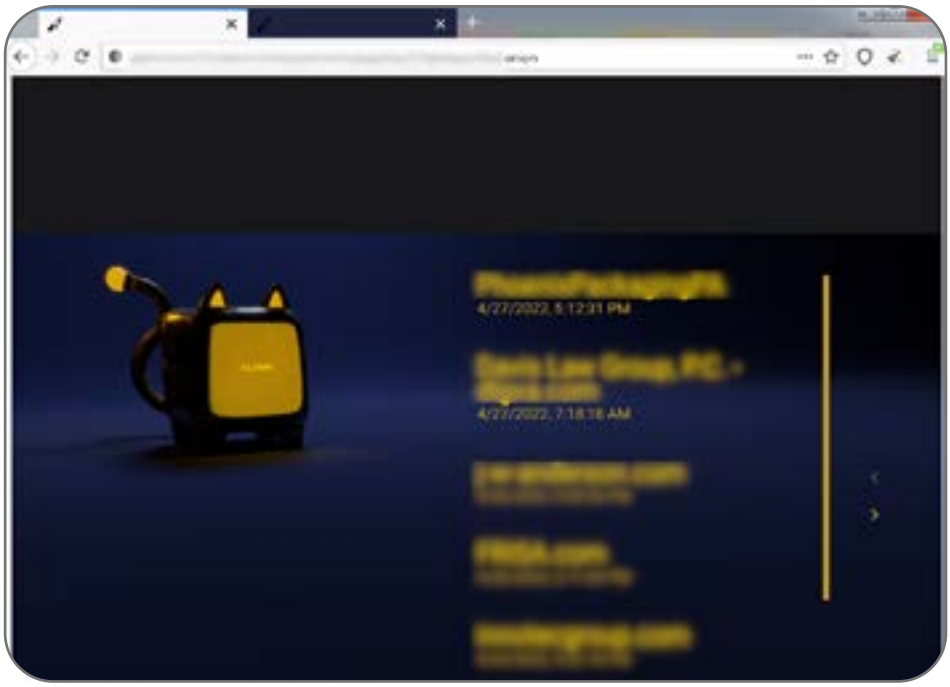


Abb. 38: Dataleak-Website von BlackCat/ALPHV

Abb. 39 zeigt, welche Branchen von BlackCat/ALPHV-Angriffen mit Doppelerpressung betroffen waren.

BlackCat/ALPHV-Infektionen nach Branche

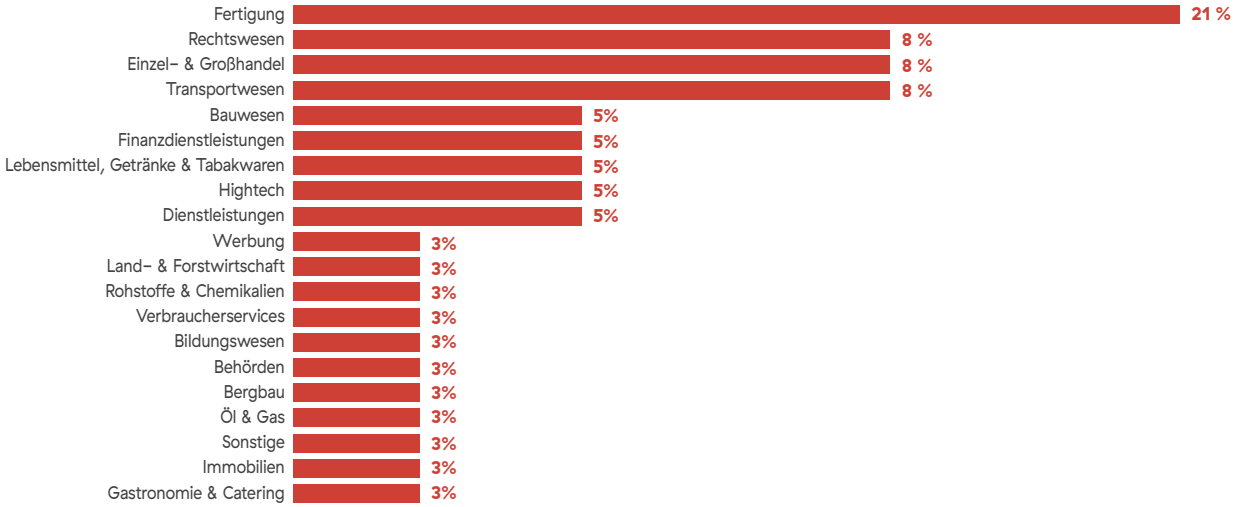


Abb. 39: BlackCat/ALPHV-Infektionen nach Branche

BlackCat — MITRE ATT&CK Taktiken und Techniken

Erstzugriff	Ausführung	Persistenz	Rechteerhöhung	Umgehen von Abwehr-mechanismen	Erkennung	Laterale Bewegung	Exfiltration	Auswirkungen
Gültige Konten	Command- und Skript-Interpreter	Boot- oder Logon-Autostart-Ausführung: Registry-Schlüssel „Run“/ Start-Ordner	Domain-Konten	Schutzmecha-nismen werden beein-trächtigt: Tools werden deaktiviert oder modifiziert	Erkennen der Netzwerkkonfi-guration	Lateraler Tool-Transfer	Geplante Übertragung	Daten werden verschlüsselt
	Ausführung durch User	Geplanter Task/Job	Ausnutzung zur Rechteerhöhung	Verschleierung/ Verschlüsselung von Dateien oder Daten wird aufgehoben	Erkennen von Remote-Systemen			Systemwieder-herstellung wird behindert
				Änderung der Domänenricht-linie: Änderung der Gruppen-richtlinie	Erkennen von Dateien und Verzeichnissen			
					Erkennung von Sicherheitssoft-ware			

Über ThreatLabz

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses erstklassige Team sorgt dafür, dass die Tausenden von Organisationen, die weltweit mit der globalen Zscaler-Plattform arbeiten, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware-Bedrohungen tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für Advanced Threat Protection auf der Zscaler-Plattform bei und führen regelmäßig interne Revisionen durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer Bedrohungen werden regelmäßig unter research.zscaler.de veröffentlicht.

Unser Newsletter informiert Organisationen über aktuelle Forschungsergebnisse der ThreatLabz-Experten.

Die von Gartner als führende SSE-Plattform benannte Zero Trust Exchange von Zscaler (Security Service Edge) bietet in sämtlichen Phasen des Angriffszyklus zuverlässigen Schutz vor Ransomware. Dadurch können Organisationen nicht nur das Angriffsrisiko beträchtlich senken, sondern reduzieren auch das Schadenspotenzial im Fall eines erfolgreichen Angriffs.

Mit der Zscaler-Lösung profitieren Organisationen von der nativen Integration marktführender Funktionen zur Abwehr und Bekämpfung von Ransomware-Angriffen durch:

Minimale Angriffsfläche

Die Cloud-native Proxy-basierte Architektur von Zscaler reduziert die Angriffsfläche, indem interne Anwendungen für das Internet unsichtbar gemacht werden, sodass sie nicht mehr als potenzielle Angriffsvektoren ausgenutzt werden können.

Schutz vor Kompromittierung

Zscaler ermöglicht die vollständige Überprüfung und Authentifizierung des gesamten verschlüsselten und unverschlüsselten Traffics, um unbefugte Zugriffe von Bedrohungsakteuren abzuwehren. Durch Browser Isolation und Inline-Sandboxing werden auch Ausweichmanöver und neuartige Bedrohungen zuverlässig erkannt.

Keine laterale Ausbreitung

Zscaler verbindet User und Entitäten direkt mit Anwendungen (statt mit Netzwerken), um ihre laterale Bewegungsfreiheit einzuschränken. Besonders geschäftskritische Anwendungen können durch realistische Decoys zusätzlich geschützt werden.

Schutz vor Datenverlusten

Durch Überprüfung des gesamten ausgehenden Traffics zu Cloud-Anwendungen werden Datenverluste bei der Übertragung verhindert. Zum Schutz von Daten im Ruhezustand kommen CASB-Funktionen (Cloud Access Security Broker) zum Einsatz, mit denen sich Sicherheitsrisiken zuverlässig erkennen und beheben lassen.

Interessenten finden auf unserer Website weitere Informationen zum Ransomware-Schutz von Zscaler.

zscaler™ | Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen veröffentlichen wir unter **zscaler.de** oder auf Twitter unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de