Acronis

Report 2022

# Acronis Cyber Protection Operation Centers Report:

Cyberbedrohungen in der zweiten Jahreshälfte 2022 – Daten im Visier

# Acronis
# Cyber Protection Operation Centers Report

## Inhaltsverzeichnis




**Autoren:**

**Alexander Ivanyuk**
Senior Director für den Bereich Produkt- und Technologie-positionierung bei Acronis

**Candid Wuest**
Vice President für den Bereich Cyber Protection Research bei Acronis

**Irina Artioli**
Cyber Protection Evangelist bei Acronis

# Einführung und Zusammenfassung

Acronis hat als erstes Unternehmen einen vollständig integrierten Cyber Protection-Ansatz zum Schutz aller Daten, Applikationen und Systeme implementiert. Cyber Protection erfordert eine aktive Untersuchung und Überwachung von Bedrohungen, um die Verlässlichkeit (Safety), Verfügbarkeit (Accessibility), Vertraulichkeit (Privacy), Authentizität (Authenticity) und Sicherheit (Security) aller entsprechenden Daten zu gewährleisten. Diese wichtigen fünf Vektoren der Cyber Protection sind unter dem Schlagwort „SAPAS“ bekannt. Als Teil dieser Strategie haben wir weltweit insgesamt vier Cyber Protection Operation Center eingerichtet, um Cyberbedrohungen rund um die Uhr überwachen und untersuchen zu können.

Wir haben außerdem unsere aktuellen Flaggschiff-Produkte weiterentwickelt: Acronis Cyber Protect Cloud, eine in die Acronis Cyber Cloud-Plattform integrierte Cloud-Lösung, sowie Acronis Cyber Protect 15, eine reine On-Premise-Lösung. Auch vor diesen Veröffentlichungen war Acronis schon mit seiner innovativen Acronis Active Protection Antiransomware-Technologie führend auf dem Data Protection-Markt. Diese Technologie wurde im Laufe der Zeit kontinuierlich weiterentwickelt, um die einzigartige Kompetenz des Unternehmens bei der Abwehr von Daten gefährdenden Bedrohungen zu demonstrieren. Insbesondere die 2016 von Acronis eingeführten Erkennungstechnologien, die mit künstlicher Intelligenz (KI) und heuristischer Verhaltensanalyse arbeiten, wurden so erweitert, dass sie mittlerweile alle Arten von Malware sowie andere potenzielle Bedrohungen abdecken.

Dieser Bericht behandelt die Bedrohungslandschaft, die unsere Sensoren und Analysten in der zweiten Jahreshälfte 2022 ermittelt haben. Die in diesem Bericht vorgestellten allgemeinen Malware-Daten wurden von Juli bis November diesen Jahres gesammelt und spiegeln diejenigen Bedrohungen wider, die wir in diesen Monaten auf entsprechenden Endgeräten beobachtet haben.

Dieser Bericht bietet einen globalen Ausblick und basiert auf den Daten von mehr als 750.000 individuellen Endpunkten, die über die ganze Welt verteilt sind. Die meisten besprochenen Statistiken konzentrieren sich auf Bedrohungen für Windows-Betriebssysteme, da diese (im Vergleich zu macOS und Linux) am stärksten verbreitet sind.

## Die fünf wichtigsten Kennzahlen in diesem Bericht:

- In Bezug auf „Malware pro Nutzer“ waren Südkorea, Jordanien und China die Länder mit den meisten Angriffen im dritten Quartal 2022.
- Acronis konnte im Zeitraum von Juli bis November 2022 rund 40 Millionen URLs auf geschützten Endpunkten blockieren, wobei es in den letzten beiden Monaten einen deutlichen Anstieg gegenüber den Sommermonaten gab.
- 30,6% aller empfangenen E-Mails waren Spam und rund 1,6% davon enthielten Phishing-Links oder Malware.
- Es wird erwartet, dass die durchschnittlichen Kosten für eine Datenschutzverletzung im Jahr 2023 auf voraussichtlich 5 Millionen Dollar steigen werden.
- Im dritten Quartal 2022 haben durchschnittlich 7,7% aller Endgeräte versucht, auf schädliche URLs zuzugreifen. Gegenüber dem Vorquartal (mit dort 8,3%) entspricht dies einem leichten Rückgang.

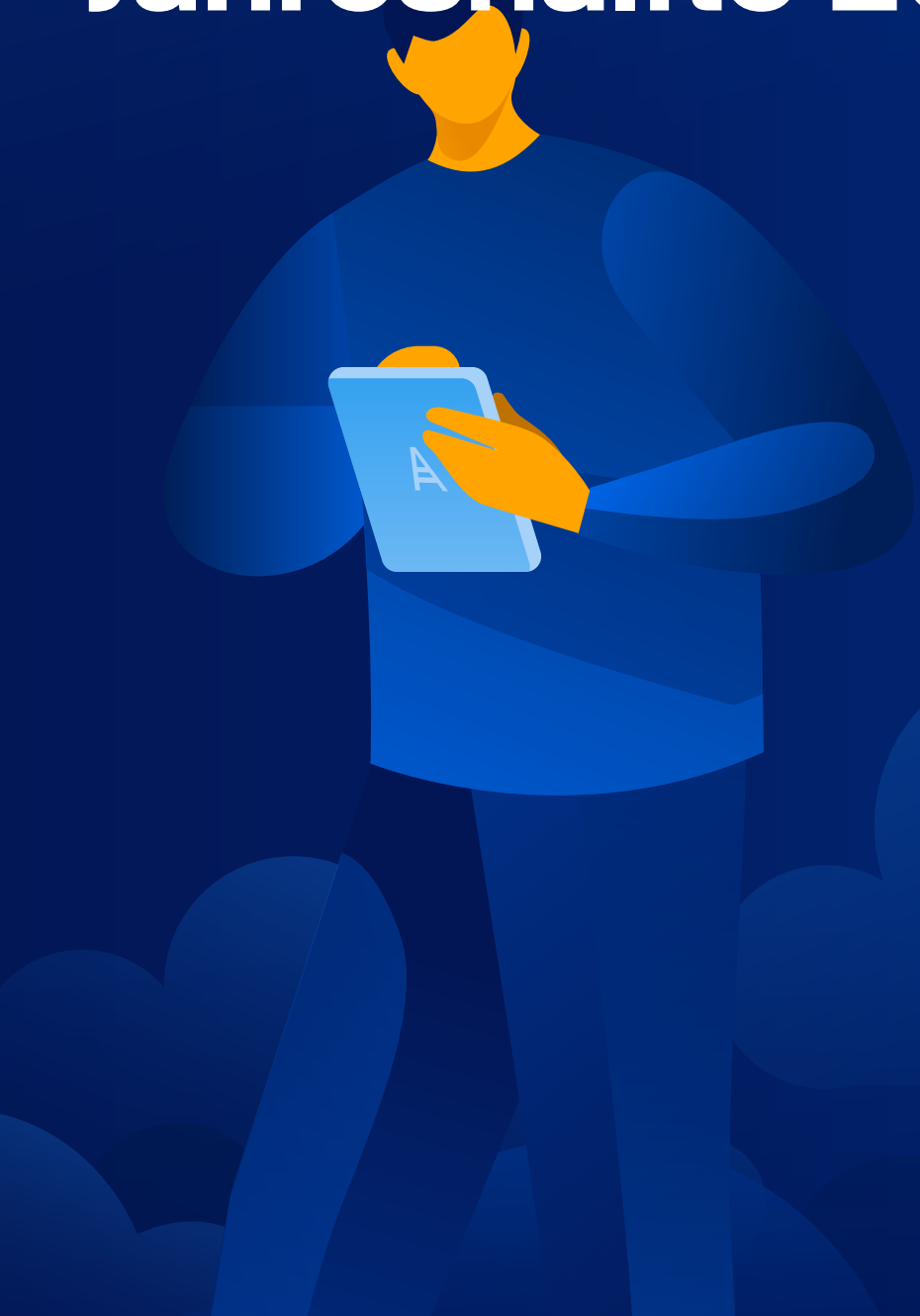
## Einige der Cyber Security-Trends, die wir in der zweiten Jahreshälfte 2022 beobachtet haben:

- Ransomware ist nach wie vor die stärkste Bedrohung für mittlere und große Unternehmen (ebenso für Behörden, das Gesundheitswesen und weitere systemkritische Branchen).
- Unautorisiert weitergegebene oder gestohlene Anmeldedaten waren im ersten Halbjahr 2022 für fast die Hälfte aller gemeldeten Sicherheitsverletzungen verantwortlich. Gestohlene Anmeldedaten sind nach wie vor eine der Hauptursachen für Datenschutzverstöße, denn mit ihnen wird es für Angreifer leichter, erfolgreiche Phishing- und Ransomware-Kampagnen durchzuführen.
- Von 12.985 Schwachstellen, die in den ersten sechs Monaten diesen Jahres gemeldet wurden, wurden 475 aktiv ausgenutzt.
- Von Juli bis Oktober 2022 nahm die Zahl der Phishing-Angriffe um den Faktor 1,3 zu und macht nun 76% aller Angriffe aus (gegenüber 58% im ersten Halbjahr 2022).

# Was Sie im Bericht finden können:

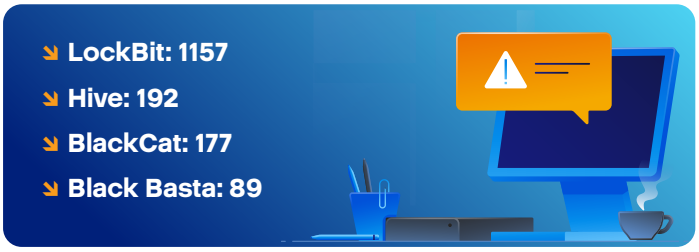
- Die wichtigsten Sicherheits- und Bedrohungstrends im zweiten Halbjahr 2022
- Warum wir immer mehr Datenschutzverletzungen sehen
- Allgemeine Malware-Statistiken und eine Betrachtung der wichtigsten Bedrohungsfamilien
- Ransomware-Statistiken mit einer tiefergehenden Analyse einiger der gefährlichsten Bedrohungen
- Welche Schwachstellen wesentlich dazu beitragen, dass Angriffe erfolgreich sind
- Unsere Sicherheitsempfehlungen
- Unsere Sicherheitsvorhersagen für 2023

# Die wichtigsten Cyberbedrohungen und Trends in der zweiten Jahreshälfte 2022



# 1. Die Anzahl der Ransomware-Angriffe geht zurück, aber die Bedrohung ist größer denn je

Bedauerlicherweise nimmt die Bedrohung durch Ransomware weiter zu. Obwohl die Zahl der Angriffe, Varianten und neuen Familien zurückgeht, sind die von den Cyberkriminellen bisher eingesetzten Familien sehr erfolgreich. Im zweiten Halbjahr diesen Jahres konnten die Ransomware-Gangs jeden Monat 200-300 neue Opfer auf ihre Erfolgsliste setzen. Diese vier Hauptbetreiber konnten bis Ende des dritten Quartals folgende Zahlen an kompromittierten Zielen für sich verbuchen:




Während einige Familien (die man auch getrost als „Ransomware-Marken" bezeichnen könnte) die Szene verlassen haben – wie z.B. Egregor, REvil, BlackMatter und DoppelPaymer – haben sich die entsprechenden Akteure einfach umbenannt und neue Operationen gestartet. Durch diese Taktik können sie den Strafverfolgungsbehörden aus dem Weg gehen (oder zumindest deren Fortschritte ausbremsen) und sich weitere Monate, wenn nicht Jahre, erfolgreicher krimineller Aktivitäten verschaffen.

Das gab es auch früher schon einmal: WastedLocker tauchte als die Ransomware Hades oder Cryptolocker wieder auf und wurde im Herbst zu PayloadBin und Macaw. Die Ransomware DarkSide wurde zuerst in DarkSide 2.0 und später dann wieder in BlackMatter umbenannt. Zu Beginn diesen Jahres hat die Ransomware-Bande BlackCat bestätigt, dass sie ehemalige Mitglieder der DarkSide-/BlackMatter-Gruppe sind.

Obwohl die Strafverfolgungsbehörden in 2022 einige große Erfolge im Kampf gegen Ransomware-Akteure verzeichnen konnten, sind die Cyberkriminellen weiterhin auf der Gewinnerseite. Die niederländische Polizei (in Zusammenarbeit mit der Cyber Security-Firma Responders.NU) konnte die Ransomware-Bande DeadBolt zur Herausgabe von 155 Dechiffrierungsschlüsseln überlisten, indem sie Lösegeldzahlungen vortäuschte. Leider hat die DeadBolt-Bande, nachdem sie erkannt hat, dass sie ausgetrickst und nicht bezahlt wurde, ihre Taktik geändert: Sie verlangen nun vor der Herausgabe von Dechiffrierungsschlüsseln eine doppelte Bestätigung.

Ein große Erfolg auf der positiven Seite war die kürzliche Verhaftung eines russischen LockBit-Mitglieds in Kanada, welches für die Einforderung von Erpressungszahlungen verantwortlich war. Laut Europol dürfte es sich bei der Person jedoch eher um ein Mitglied als um den Leiter der gesamten Cybercrime-Operation handeln. Die Hauptakteure sind immer noch draußen und richten Schaden an.

**Die vier Großen in der Ransomware-Welt in 2022**

Wie bereits erwähnt, wird der Markt der Ransomware-Akteure tatsächlich von lediglich 4-5 Spielern dominiert. Die vier aktivsten im Jahr 2022 waren LockBit, Black Basta, Hive und BlackCat.

Natürlich gibt es auch noch andere Spieler, aber diese richten viel weniger Schaden an. Gruppen wie STOP, Inlock, Dharma, Xorist, Venus, Cuba, Pendragon, Chaos, Killnet, Zeppelin und weitere veröffentlichen weiterhin aktiv neue Varianten und infizieren damit auch Anwender.

Werfen wir einen Blick auf einige Fälle, die von den wichtigsten Bedrohungsakteuren in der Welt der Ransomware verursacht wurden:

**LockBit 3.0**

LockBit ist eine der modernsten Ransomware-Familien, die es gibt. Es verwendet starke Anti-Debugging- und Anti-Erkennungsmechanismen, kann Windows Defender deaktivieren und Backups löschen. Im September 2022 wurde dann ein geleakter LockBit 3.0-Builder auf Twitter veröffentlicht. Der Sprecher der Gruppe „LockBitSupp" behauptete jedoch, dass die Bande nicht gehackt wurde und machte stattdessen einen ehemaligen Entwickler für den Leak verantwortlich. Es ist jedenfalls zu erwarten, dass dieser Vorfall noch Folgen haben wird, wenn sich nämlich andere Gruppen den durchgesickerten Code zur Verstärkung ihrer Angriffstechniken zunutze machen werden.

Gleichzeitig muss man leider konstatieren, dass die LockBit-Betreiber ihre Sache sehr gut machen. Sie führen den Markt bei weitem an, denn nach Schätzungen verschiedener Experten liegt ihr Anteil bei 40-50%. Und sie erweitern ihre Erfolgsliste mit immer mehr hochkarätigen Opfern.

Im Juli hat LockBit bei der FAAC-Gruppe (Fabbrica Automatismi Apertura Cancelli) zugeschlagen, die mit 53 Unternehmen auf fünf Kontinenten einen konsolidierten Umsatz von über 600 Millionen Euro erzielt und weltweit über 3.600 Mitarbeiter beschäftigt. Darauf folgte ein Angriff auf das Unternehmen La Poste Mobile, das mit 2.740 Mitarbeitern einen Jahresumsatz von über 513 Millionen Dollar erwirtschaftet.

Anschließend setzte LockBit seine Aktivitäten bei der kanadischen Stadt St. Marys (in Ontario) mit 7.500 Einwohnern und der Stadt Frederick (in Colorado) mit 15.000 Einwohnern fort. Die Gruppe forderte ein Lösegeld von 200.000 Dollar, damit die gestohlenen Daten nicht veröffentlicht werden.

Auch die IHG, die derzeit 6.028 Hotels in mehr als 100 Ländern betreibt, wurde Opfer eines entsprechenden Cyberangriffs. Die genauen Hintermänner dieses Angriffs sind zwar unbekannt, aber vor kurzem hat die Ransomware-Bande Lockbit einen Angriff auf das Hotel Holiday Inn Istanbul Kadıköy gemeldet.

Das japanische Technologie-Unternehmen Oomiya wurde ebenfalls getroffen. Oomiya erzielt einen Jahresumsatz von 50 Millionen Dollar und beschäftigt rund 500 Mitarbeiter. Das Unternehmen ist auf die Entwicklung und Herstellung von mikroelektronischen Geräten und Anlagensystemen spezialisiert. Dieser Vorfall könnte beträchtliche Auswirkungen auf Drittanbieter haben, weil Oomiya weltweit in der Lieferkette großer Unternehmen aus verschiedenen Branchen (wie der Fertigungs-, Halbleiter-, Automobil-, Kommunikations- und Gesundheitsbranche) vertreten ist.

Von der Bank von Brasilia (BRB) wurden rund 50 Bitcoins verlangt, damit die Öffentlichkeit nicht erfährt, worauf die Angreifer Zugriff hatten. Von der Pendragon Group, die in Großbritannien über 200 Autohäuser betreibt und einen Jahresumsatz von mehr als 3,9 Milliarden Dollar erzielt, wurden 60 Millionen Dollar für die Dechiffrierung von Dateien sowie deren Geheimhaltung verlangt. Pendragon hat die britischen Behörden über den Vorfall informiert und einen entsprechenden Bericht an die Strafverfolgungsbehörden zur Untersuchung weitergeleitet. Interessanterweise griff auch LockBit die Firma an, als das schwedische Unternehmen Hedin Mobility Group über 450 Millionen Dollar für die Übernahme von Pendragon geboten hat.

**Black Basta**

Die Gruppe „Black Basta“ tauchte (wie schon mal berichtet) erstmals im April 2022 auf und wurde offenbar von ehemaligen Mitgliedern der Ransomware-Gangs Conti und REvil gegründet, mit denen sie ähnliche Taktiken, Techniken und Prozeduren teilt. Erst kürzlich haben Sicherheitsforscher von SentinelLabs Belege dafür gefunden, dass die Ransomware-Bande Black Basta mit der finanzorientierten Hackergruppe FIN7 (die auch als „Carbanak“ bekannt ist) verbunden ist. Man wird sehen, wie sich das entwickelt. Bisher konnte Black Basta allerdings schon einige große Hits landen.

Die Knauf-Gruppe, mit einem Jahresumsatz von über 11 Milliarden Dollar, ist eines der ersten Opfer von Black Basta. Knauf ist ein führender Hersteller von Baumaterialien, der weltweit über 35.000 Mitarbeiter an 150 Produktionsstandorten beschäftigt.

An einem Wochenende im November wurde der kanadische Lebensmitteleinzelhandelsriese Sobeys angegriffen. Die Kette beschäftigt über 134.000 Mitarbeiter in 1.500 Lebensmittel- und Drogeriemärkten in allen 10 kanadischen Provinzen. Sobeys ist einer von lediglich zwei großen Lebensmitteldiscountern des Landes – und operiert unter den Markennamen Sobeys, Safeway, IGA, Foodland, FreshCo, Thrifty Foods und Lawtons Drugs. Die Ransomware Black Basta konnte die Computer von Sobeys verschlüsseln. Als dieser Bericht verfasst wurde, befanden sich die Angreifer noch in Verhandlungen mit dem Unternehmen.

**Hive**

Auch die Ransomware-Bande Hive konnte große Treffer landen. Zu den jüngsten Opfern gehörte beispielsweise Tata Power. Dies ist Indiens größtes Stromerzeugungsunternehmen, das über seine Vertriebshändler mehr als 12 Millionen Kunden bedient und dabei mehr als 5 Milliarden Dollar einnimmt. Die Betreiber von Hive stellten die gestohlenen Daten über ihre Leak-Website ins Netz. Dazu gehörten Verträge, Finanz- und Geschäftsdokumente, technische Projekte sowie personenbezogene Daten (wie z.B. Aadhaar-Kartennummern) der Mitarbeiter. Außerdem waren technische Zeichnungen, Finanz- und Bankdaten sowie Kundeninformationen in dem Datensatz enthalten.

Zuvor konnte Hive das Unternehmen Eurocell auf seine Opferliste setzen und 6 Millionen Dollar einfordern. Eurocell ist ein britischer Baustoffhändler mit einem Jahresumsatz von 420 Millionen Dollar.

Auch die Computer der Bell Canada-Tochter BTS (Bell Technical Solutions) wurden von der Ransomware Hive heimgesucht. BTS ist mit seinen mehr als 4.500 Mitarbeitern ein unabhängiges Tochterunternehmen, das auf die Bereitstellung von Bell-Dienstleistungen in den Provinzen Ontario und Québec spezialisiert ist.

Ebenfalls von einem Angriff betroffen waren 92 Filialen von Damart, einem französischen Bekleidungsunternehmen mit weltweit über 130 Filialen. Die Betreiber von Hive haben dabei eine Lösegeldforderung von 2 Millionen Dollar gestellt.

**BlackCat/ALPHV**

Die BlackCat-Gruppe ist für ihre dreifache Erpressungstaktik berüchtigt, weil den Opfern nach dem Diebstahl von Unternehmensdaten mit deren Veröffentlichung sowie mit DDoS-Angriffen (Distributed Denial of Service) gedroht wird, wenn die Forderungen nicht erfüllt werden. BlackCat hatte in der zweiten Hälfte von 2022 mehrere große Angriffsziele.

Sie behaupten, über 150 GB an Daten vom europäischen Gaspipeline-Betreiber Creos Luxembourg S.A. gestohlen zu haben. Das Unternehmen macht mit über 800 Mitarbeitern einen Jahresumsatz von 290 Millionen Euro.

Die berühmte japanische Videospielfirma Bandai Namco (bekannt für zahlreiche Videospiele wie Elden Ring, Pac-Man und Tekken) wurde ebenfalls Opfer eines Angriffs. Das Unternehmen erzielt einen Jahresumsatz von rund 7,3 Milliarden Dollar.

Die Ransomware BlackCat/ALPHV stand hinter einem Angriff auf das italienische Energiedienstleistungsunternehmen GSE (Gestore dei Servizi Energetici SpA). Die Cyberkriminellen konnten dabei etwa 700 GB Daten aus der IT-Infrastruktur des Unternehmens exfiltrieren.

Record TV, der zweitgrößte Fernsehsender Brasiliens, SBT und TV Cultura wurden unlängst ebenfalls Opfer eines Cyberangriffs. Es ist noch nicht geklärt, ob diese Aktionen koordiniert waren. Auf jeden Fall war Ransomware im Spiel - und es besteht der Verdacht, dass BlackCat dafür verantwortlich ist. Von diesem Vorfall wurden das interne Netzwerk, die Telefondienste, die Post sowie die Übertragung lokaler Fernsehkanäle betroffen. Die Sender haben keine öffentliche Stellungnahme abgegeben, mussten jedoch die Übertragung ihres Live-Programms aussetzen.

**Weitere bemerkenswerte Fälle**

Natürlich waren auch andere Gruppen im Einsatz, um große und mittelständische Unternehmen rund um den Globus zu kompromittieren.

Der deutsche Elektronikproduzent Semikron wurde von der Ransomware-Gruppe LV angegriffen. Semikron verfügt über 3.000 Mitarbeiter in 24 Niederlassungen weltweit und erzielt einen jährlichen Umsatz von 460 Millionen Dollar.

Die argentinische Justizbehörde von Córdoba wurde zum Opfer der Ransomware-Gruppe PLAY. Es ist noch unklar, wie genau PLAY in das Justiznetzwerk eindringen konnte. Allerdings wurde im März im Rahmen des sogenannten Lapsus$-Einbruchs bei Globant eine Liste der E-Mail-Adressen von Mitarbeitern veröffentlicht.

Die Ransomware-Gang Clop behauptet, 5 TB an Daten von South Staffs Water gestohlen zu haben. Dieses Unternehmen liefert täglich 330 Millionen Liter Trinkwasser an 1,6 Millionen Haushalte und hat einen Jahresumsatz von 335 Millionen Dollar.

Griechenlands größter Erdgasversorger DESFA (mit einem Jahresumsatz von 270 Millionen Euro) hat bestätigt, dass es nach einem Cyberangriff durch die Ransomware Ragnar Locker zu einem begrenzten Datenverlust und einem Ausfall des IT-Systems gekommen ist. Die Bande hinter Ragnar Locker hat sich auch zu einem Anschlag auf TAP Air Portugal bekannt. Die Bande hat ein neues Datenleck auf ihrer Website veröffentlicht, das personenbezogene Daten von mehr als 9.000 Kunden enthält.

Die Cybercrime-Gruppe RansomHouse gibt an, acht italienische Bezirke kompromittiert und sämtliche 2,1 TB an Daten veröffentlicht zu haben, die aus den IT-Infrastrukturen der Union der toskanischen Gemeinden in der Metropole Florenz extrahiert wurden. In ihrer Mitteilung gab die RansomHouse-Gruppe bekannt, dass sie bei den Angriffen auf die italienische Regierungsinfrastruktur von schwachen Kennwort-Praktiken (wie z.B. die Verwendung von Kennwörtern wie „12345678“) profitieren konnten, um die vermeintlich geschützte sensiblen Daten zu erbeuten.

Das französische CHSF (Center Hospitalier Sud Francilien), ein 28 km vom Pariser Stadtzentrum entferntes Krankenhaus mit rund 1000 Betten, wurde Opfer eines Cyberangriffs. Das medizinische Zentrum, welches ein Gebiet mit ca. 600.000 Einwohnern versorgt, musste aufgrund des Angriffs Patienten an andere Einrichtungen überweisen und Operationstermine verschieben. Die Angreifer haben ein Lösegeld von 10 Millionen Dollar für den Dechiffrierungsschlüssel gefordert.

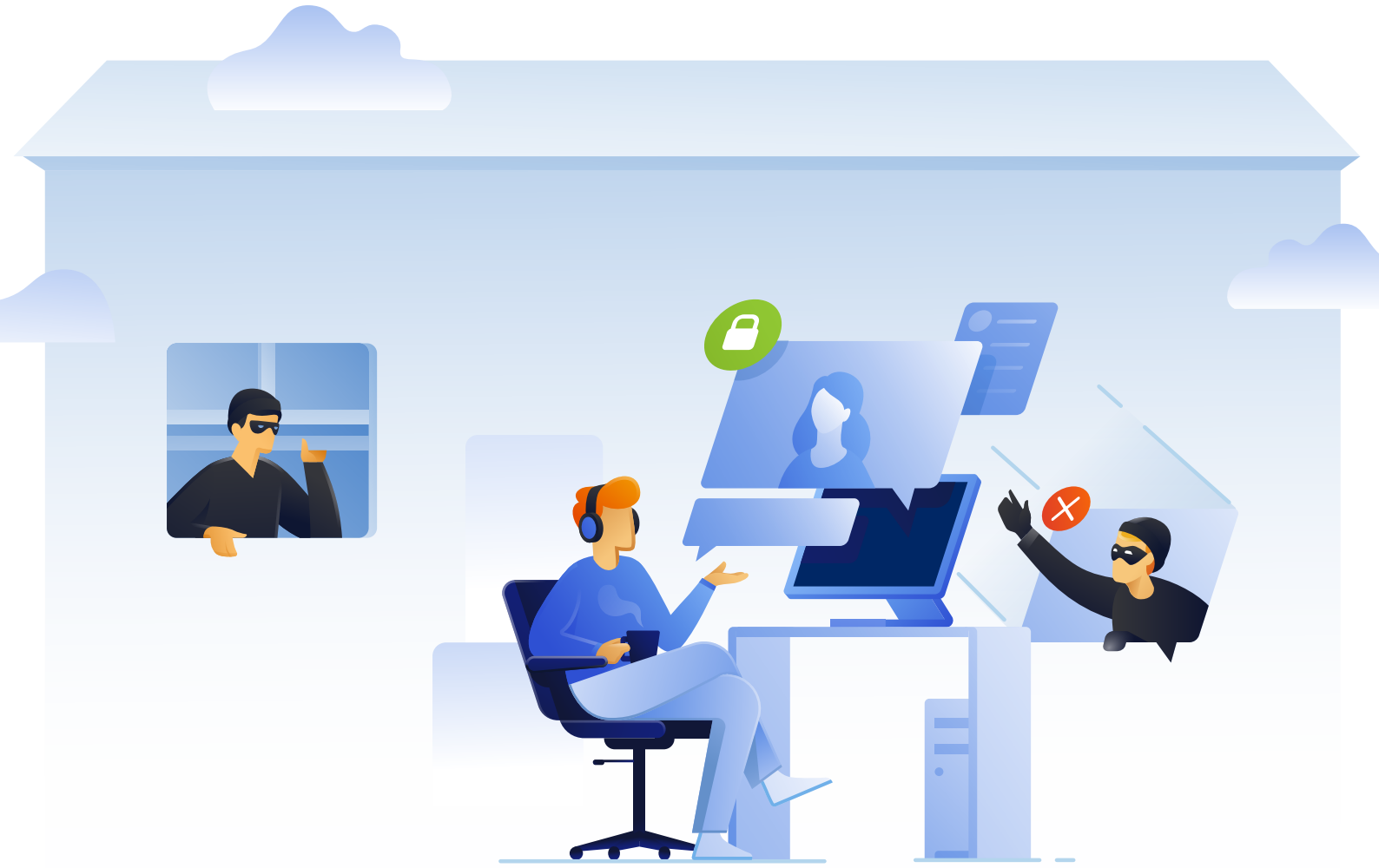
Wie das Unternehmen BRP (Bombardier Recreational Products) am 8. August 2022 mitteilte, hat sich eine Ransomware-Gang namens RansomEXX zu einem Cyberangriff auf das Unternehmen bekannt. BRP vertreibt verschiedene Produkte in mehr als 120 Ländern und beschäftigt über 20.000 Mitarbeiter bei einem Jahresumsatz von fast 6 Milliarden Dollar. RansomEXX hat BRP auf seiner Datenleak-Website aufgeführt, zusammen mit fast 30 GB an Dateien, die vorgeblich aus dem Unternehmen entwendet wurden. Zu diesen entwendeten Dateien gehören Vertraulichkeitsvereinbarungen, Ausweispapiere, Materiallieferverträge, Vertragsverlängerungen und vieles mehr. In seiner Erklärung präsentierte das Unternehmen erste Ergebnisse einer internen Untersuchung und erklärte, dass die Angreifer über einen Lieferkettenangriff in die entsprechenden Systeme eingedrungen sind.

Das spanische Unternehmen CSI (Consorci Sanitari Integral) ist ein weiteres Opfer der RansomEXX-Gruppe. Der Vorfall betraf alle Gesundheitszentren des Unternehmens in Barcelona und dem Landkreis Baix Llobregat, wodurch die entsprechenden Mitarbeiter nicht mehr auf Patientendaten oder Prozeduren zugreifen konnten. Die CSI ist eine öffentliche Einrichtung mit rund 3.500 Mitarbeitern. Sie wird vom Gesundheitsministerium, den Gemeinden Sant Joan Despí und l'Hospitalet de Llobregat, dem Consell Comarcal del Baix Llobregat sowie der Creu Roja getragen. Die Organisation umfasst 13 Gesundheitszentren, die Patienten in öffentlichen Gesundheitseinrichtungen, in der Primärversorgung, in Krankenhäusern und in sozialen Gesundheitszentren (zwei Häuser) betreuen. Die CSI verwaltet außerdem Dienste zur Beurteilung von Abhängigkeit und Behinderung in Barcelona und L'Hospitalet. Zwar hat das Management des Gesundheitsversorgers keine weiteren Einzelheiten bekannt gegeben, aber die wirtschaftlichen Auswirkungen dieses Vorfalls dürften größer sein als die Folgen des Drogenhandels.

Die Ransomware-Gang Vice Society behauptet, mehr als 500 GB der LAUSD (dem vereinigten Schulbezirk von Los Angeles, USA) gestohlen zu haben. In dem Bezirk sind mehr als 640.000 Schüler angemeldet.

Die Ransomware-Gruppe Everest behauptet, Zugriff auf alle Server des öffentlichen Versorgungsunternehmens Eskom Hld SOC Ltd. in Südafrika erhalten zu haben. Die Angreifer haben 200.000 Dollar (zahlbar in Bitcoin oder Monero) für ein Paket gefordert, das Administrator-, Root- und Sysadmin-Kennwörtern für Linux- und Windows-Server enthält. Eskom ist ein staatliches Elektrizitätsunternehmen, das mehr als 90% aller Kunden in Südafrika und in der Entwicklungsgemeinschaft des südlichen Afrika (SADC) mit Energie versorgt. Die Betreiber von Everest hatten bereits im März 2022 den Kauf des „Root-Zugriffs auf die südafrikanische Elektrizitätsgesellschaft“ für 125.000 Dollar gemeldet. Zu diesem Zeitpunkt hatte Eskom jedoch noch bestritten, dass es zu einer Sicherheitsverletzung gekommen wäre. Als die Everest-Gruppe unlängst über eine erneute Sicherheitsverletzung bei Eskom berichtete, wurde von Sicherheitsexperten darauf hingewiesen, dass der Energieversorger mit einigen Server-Problemen zu kämpfen hatte.

Und damit kommen wir zum „Elefanten im Raum“: auch das Unternehmen Cisco gab kürzlich bekannt, dass seine Infrastruktur von der Ransomware-Bande Yanluowang angegriffen wurde. Laut der anschließenden Untersuchung sollen aber weder Daten gestohlen noch veröffentlicht worden sein.



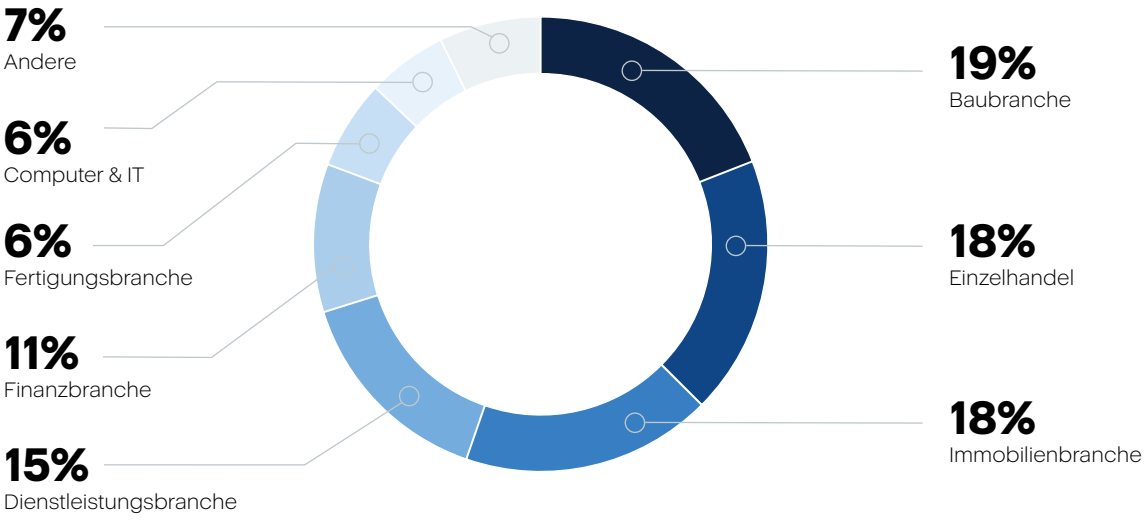
# 2. Angriffe über Phishing und andere betrügerische E-Mails sind nach wie vor der Haupteinfallsvektor

Die nachfolgenden E-Mail- und Phishing-Statistiken wurden über das Add-on-Paket „Advanced Email Security“ für Acronis Cyber Protect Cloud erhoben, das von Perception Point entwickelt wurde. Acronis und Perception Point arbeiten zusammen, um Unternehmen kontinuierlich vor E-Mail-basierten Bedrohungen zu schützen. Die Daten wurden in der zweiten Jahreshälfte 2022 erhoben und mit weiteren Telemetriedaten von Acronis zu Malware- und URL-Blockierungen auf den geschützten Endgeräten kombiniert.

In dem fraglichen Zeitraum haben wir eine deutliche Zunahme an E-Mail-basierten Bedrohungen festgestellt. Die Rate der gefährlichen E-Mail-Nachrichten ist in nur 4 Monaten um 0,6 Punkte (60%) gestiegen. Die Spam-Raten sind im selben Zeitraum um über 15% gestiegen und machen jetzt 30,6% des gesamten eingehenden Datenverkehrs aus. Es ist auch erwähnenswert, dass Acronis Kunden anfälliger für Spam-Attacken zu sein scheinen als andere Kunden (bei denen Perception Point eine Spam-Rate von 19,3% ermittelte). Dies ist jedoch noch nicht das Ende: wir erwarten für den Dezember (aufgrund der Weihnachtszeit) einen weiteren Anstieg.

Niemand ist sicher – von E-Mail-basierten Angriffen sind praktisch alle Branchen betroffen. Eine Analyse der 50 am meisten angegriffenen Unternehmen zeigt jedoch, dass folgende Branchen besonders gefährdet sind:

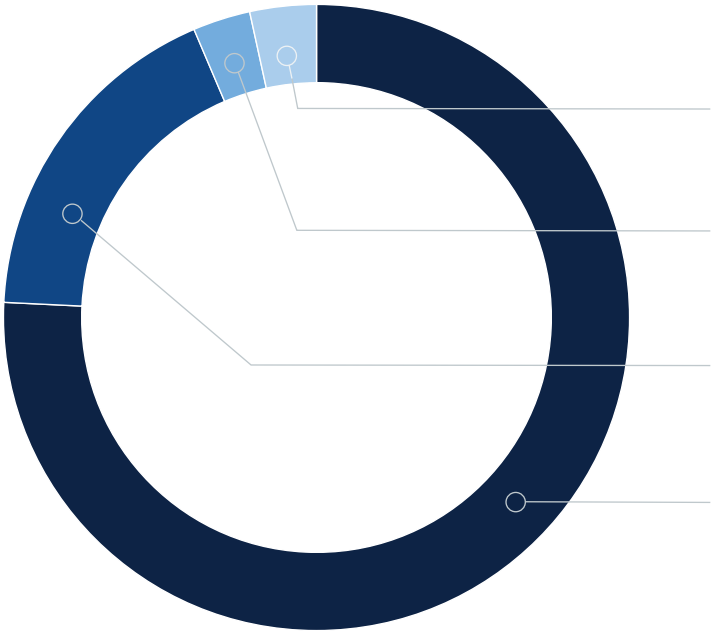
- **Baubranche**
- **Einzelhandel**
- **Immobilienbranche**
- **Professionelle Dienstleistungen (einschließlich IT)**
- **Finanzwesen**




**Die am meisten betroffenen Branchen von Juli bis November 2022**

Phishing – einschließlich spezieller Varianten wie Spear-Phishing- und Whaling-Angriffe – ist weiterhin die größte Bedrohung für Organisationen. Von Juli bis November 2022 nahm die Zahl der Phishing-Aktivitäten um 130% zu. Sie machen nun 76% aller E-Mail-basierten Angriffe aus (gegenüber 58% im ersten Halbjahr 2022). Entsprechend ist der Prozentsatz der Angriffe mit E-Mails, die Malware enthalten, gesunken. Auch Social Engineering-Angriffe haben in den letzten vier Monaten zugenommen und machen inzwischen 3% aller Angriffe aus (gegenüber 2% in unserem letzten Bericht).

Phishing – einschließlich spezieller Varianten wie Spear-Phishing- und Whaling-Angriffe – ist weiterhin die größte Bedrohung für Organisationen. Von Juli bis November 2022 nahm die Zahl der Phishing-Aktivitäten um 130% zu. Sie machen nun 76% aller E-Mail-basierten Angriffe aus (gegenüber 58% im ersten Halbjahr 2022). Entsprechend ist der Prozentsatz der Angriffe mit E-Mails, die Malware enthalten, gesunken. Auch Social Engineering-Angriffe haben in den letzten vier Monaten zugenommen und machen inzwischen 3% aller Angriffe aus (gegenüber 2% in unserem letzten Bericht).



**3%** Kompromittierung von Geschäfts-E-Mails

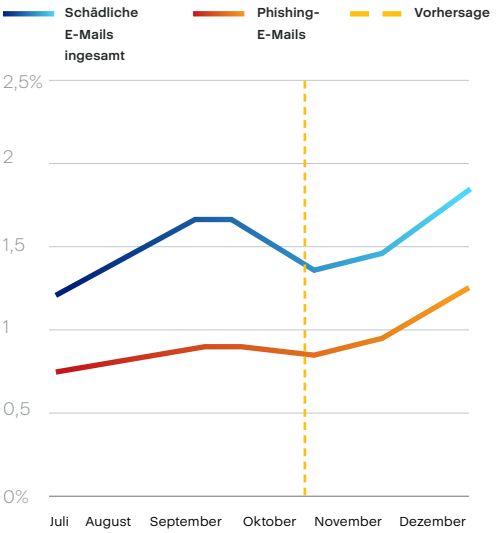
**3%** Fortschrittliche Angriffe

**18%** Malware

**76%** Phishing

| Monat in 2022 | Blockierte URLs |
|---|---|
| Januar | 5.786.801 |
| Februar | 5.288.611 |
| März | 8.075.799 |
| April | 9.306.368 |
| Mai | 4.903.640 |
| Juni | 6.940.702 |
| Juli | 5.619.052 |
| August | 7.096.120 |
| September | 4.785.525 |
| Oktober | 13.025.443 |
| November | 15.202.217 |

**Verhältnis von Phishing-E-Mails und E-Mails mit schädlichen Inhalten (ohne Spam)**



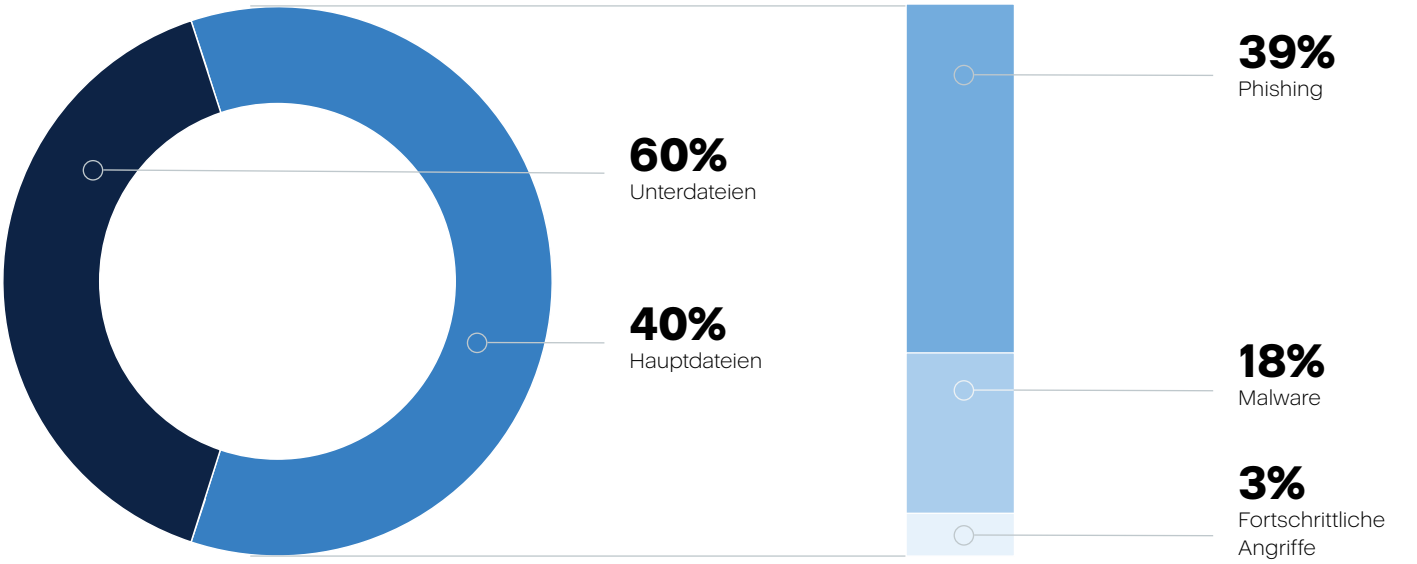

- 229.000 schädliche Ereignisse wurden im Oktober beobachtet
- 128.000 davon waren Phishing-Angriffe

Das sind 17% weniger als im 2. Quartal (mit damals 21.150.710) und 8% weniger als im 1. Quartal (mit 19.151.211).

Leider kommen viele E-Mails mit gefährlichen Inhalten (wie insbesondere URLs) immer noch durch einfache E-Mail-Filter und können so die Endpunkte der Anwender erreichen. Zudem umfassen schädliche E-Mail-Anhänge oft mehrere Ebenen – wie z.B. kennwortgeschützte ZIP-Archive, die LNK-Dateien enthalten, über die dann wiederum die finale Nutzlast heruntergeladen wird. Auch aus diesem Grund ist es wichtig, ebenfalls einen mehrschichtigen Verteidigungsansatz zu verfolgen.

Da Phishing einen Großteil der Angriffe ausmacht, verändert dies den Trend der Raten von schädlichen Ereignissen im Jahresverlauf. Basierend auf unserer Analyse und unter Berücksichtigung der Saisonalität (z.B. bevorstehende Feiertage) erwarten wir für den Dezember 2022 einen weiteren Anstieg der Angriffsraten – mit einem Jahresspitzenwert von über 2% am gesamten Datenverkehr.

Um Sicherheitsmaßnahmen zu umgehen, versuchen die Angreifer, ihre schädlichen Nutzlasten in den entsprechenden Dateien zu verstecken. Dank der Recursive Unpacker-Funktionalität (die Anti-Evasion-Schicht in der Plattform) konnten wir über 235.000 schädliche Ereignisse identifizieren, die in Unterdateien und URLs versteckt waren. Dies entspricht sechs von zehn Angriffen, die von der Plattform identifiziert wurden. Ein tieferer Blick auf die getarnten Angriffe zeigt, dass mit dieser Technik hauptsächlich Phishing-Bedrohungen (die 40% aller Angriffsversuche ausmachen) versteckt werden.




**Große Vorfälle und Phishing-Trends**

Phishing ist nach wie vor eines der beliebtesten Werkzeuge der Cyberkriminellen, um in fremde Systeme einzudringen. Werfen wir einen Blick auf einige große Vorfälle, die von Acronis und anderen Cyber Security-Forschern im Zeitraum Juli bis November 2022 entdeckt wurden.

Eine neue Angriffstechnik namens „GIFShell“ wird von den Angreifern verwendet, um Phishing-Angriffe über Microsoft Teams zu starten. Dabei werden Befehle ausgeführt, um Daten mithilfe von GIF-Dateien zu stehlen. Die zahlreichen Schwachstellen und Mängel in Microsoft Teams (mit seinen monatlich über 270 Millionen aktiven Anwendern) können für Befehlsausführungen, die Umgehung von Sicherheitsregeln, für Phishing-Angriffe oder für Datenexfiltrationen über GIF-Dateien miteinander verbunden werden. Mit GIFShell kann ein Angreifer eine Reverse Shell erstellen, die schädliche Befehle über base64-codierte GIFs in Microsoft Teams übermittelt. Die Ausgabe wird über GIF-Dateien exfiltriert, die von Microsofts eigener Infrastruktur abgerufen werden. Für GIFShell ist die Installation einer ausführbaren Datei erforderlich, die die Befehle ausführt, die über die GIF-Dateien empfangen werden. Alle eingehenden Nachrichten werden in diesen Protokollen gespeichert und sind für alle Windows-Benutzergruppen lesbar, sodass jede Malware auf dem Gerät auf diese Daten zugreifen kann.

Eine andere Phishing-Kampagne hatte es auf Microsoft-Benutzer abgesehen. Die Angreifer gaben sich als „das Microsoft-Team“ aus und wollten die Adressaten dazu verleiten, Erinnerungstexte in einem vermeintlichen Online-Gedenkboard zu Ehren von Königin Elizabeth II. einzutragen, nachdem diese im September verstorben war. Die Angreifer stahlen dabei Microsoft-Kontodaten und versuchten, die MFA-Codes (Multi-Faktor-Authentifizierung) ihrer Opfer abzugreifen, um deren Konten zu übernehmen. Die Phishing-Seite wurde mit dem EvilProxy-Phishing-Kit erstellt. Dies ist ein typisches Beispiel dafür, dass aufwühlende Nachrichten als Köder eingesetzt werden, was häufig funktioniert.

Bei einer weiteren umfassenden Phishing-Kampagne haben es die Angreifer auf die Anmeldedaten für den E-Mail-Dienst Microsoft 365 abgesehen. Sie richtet sich insbesondere gegen Unternehmen aus der FinTech-, Kredit-, Buchhaltungs- und Versicherungsbranche sowie gegen Kreditgenossenschaften aus den USA, Großbritannien, Neuseeland und Australien. Diese Kampagne ist insofern bemerkenswert, als dass die Bedrohungsakteure ein benutzerdefiniertes Proxy-basiertes Phishing-Kit verwenden, um Multi-Faktor-Authentifizierungen (MFA) zu umgehen. Das Kit kann legitime Anmeldeseiten, die den Anmeldeseiten der betreffenden Unternehmen nachempfunden sind, leicht anpassen und eigene Phishing-Elemente hinzufügen. Die Bedrohungsakteure verwenden Tools wie Evilginx2, Muraena und Modlishka, um die MFA zu umgehen. Mithilfe der Reverse-Proxies können sich die Angreifer zwischen das Opfer und den E-Mail-Server des Anbieters schalten. Daher wird diese Angriffstechnik auch „AitM“ (Adversary in the middle = Angreifer in der Mitte) genannt.

Auch andere bekannte Unternehmen und Dienstleistungen werden ausgenutzt. So wird beispielsweise die LinkedIn-Funktion „Smart Links“ missbraucht, um bestimmte Sicherheitsfilter zu umgehen. Mit dieser Funktion können Kunden Landing Pages aus bis zu 15 Dokumenten erstellen und anderen den Zugriff auf diese Seiten über nachverfolgbare Links gewähren. Leider kann dies auch als Umleitungsfunktion verwendet werden, sodass Angreifer die anvisierten Empfänger über solche Links auf Phishing-Seiten weiterleiten können. Ein aktuelles Beispiel sind Nachrichten über Paketzustellungen, die den slowakischen Postdienst imitieren. Ein anderer Phishing-Akteur hat es derzeit auf staatliche Vertragsnehmer in den U.S.A. abgesehen. In entsprechenden E-Mails wird ein Zugriff auf Regierungsportale versprochen, auf denen man sich für lukrative Regierungsprojekte bewerben kann. In Wirklichkeit verweisen die E-Mails jedoch auf eine PDF-Datei, die zu einer schädlichen Phishing-Seite weiterleitet.

Eine neue Instagram-Phishing-Kampagne hat versucht, Nutzer der beliebten Social Media-Plattform zu täuschen, indem diese mit einem Angebot für einen blauen Haken (zur Profilverifikation) gelockt wurden. Im Verlauf dieses Vorgangs wurden die Nutzer aufgefordert, persönliche Daten (einschließlich ihres Kennworts) preiszugeben, die dann natürlich direkt an den Angreifer übermittelt wurden.

Im Rahmen der Kampagne, die über mehrere Wochen aktiv war, wurden täglich mehr als 1.000 E-Mails verschickt. Die Angreifer haben eine gewisse Dringlichkeit und zeitlich begrenzte Chance suggeriert, indem sie die Nutzer gewarnt haben, dass das Anmeldeformular für den blauen Haken in 48 Stunden vollständig entfernt wird, wenn sie die Nachricht bis dahin ignorieren sollten. Durch die Verwendung einer Multi-Faktor-Authentifizierung (MFA) kann das Risiko minimiert und Ihr Konto geschützt werden, aber es ist kein Patentrezept.

Dropbox wurde missbraucht, um die Nutzlast der Angreifer bei einer neuen zweistufigen Phishing-Kampagne abzulegen. Die Anwender wurden zunächst auf eine saubere Seite mit einer Schaltfläche oder einem anklickbaren Text geleitet. Nach dem Anklicken werden die Anwender auf eine schädliche Website geleitet und aufgefordert, sich an ihrem Konto anzumelden. Der Benutzer fällt dabei unwissend auf die Masche des Angreifers herein – erst werden Haken und Leine ausgelegt, dann werden die Anmeldedaten gefischt. Das Besondere an solchen zweistufigen Phishing-Angriffen ist, dass sie in der Regel über E-Mail-Konten erfolgen, die bereits selbst durch diese Technik kompromittiert wurden. Dann werden die Kontakte des Opfers verwendet, um an diese weitere Phishing-E-Mails zu senden.

Wir sollten nicht die lokalen Phishing-Kampagnen vergessen, die nur in bestimmten Regionen stattfinden.

Die Anzahl der COVID-19-Phishing-Nachrichten hat sich im September in den USA verdoppelt. Die Angreifer geben sich in den E-Mails typischerweise als US-amerikanische Small Business Administration (SBA, Behörde für kleine Unternehmen) aus und missbrauchen Google-Formulare, um Phishing-Seiten zu hosten, über die persönliche Daten der Unternehmensbesitzer gestohlen werden sollen. Da die SBA zuvor COVID-19-Programme zur finanziellen Wiederherstellung bereitgestellt hat, konnten über die Phishing-E-Mails vermeintliche Finanzhilfen (z.B. aus dem „Paycheck Protection Program“, dem „Revitalization Fund“ oder dem „COVID Economic Injury Disaster Loan“) versprochen werden. Die vermeintliche Bewerbung für diese Programme erfordert das Anklicken einer eingebetteten Schaltfläche, die zu einem Google-Formular führt, das wiederum offizielle Formulare der SBA imitiert und neben den Anmeldedaten für das Google-Konto weitere Informationen wie Sozialversicherungsnummern, Arbeitgeber-Identifikationsnummern, Staatsangehörigkeit, Person, Führerschein sowie Bankkontonummern abfragt.

Forscher haben eine neue Phishing-Kampagne entdeckt, die es auf Arbeitssuchende in den USA und Neuseeland abgesehen hat. Die schädlichen E-Mails unterbreiten dem Empfänger ein vermeintlich lukratives Jobangebot, tatsächlich enthalten sie aber schädliche Dokumente. In bestimmten Fällen löst das Öffnen des Dokuments einen Exploit aus und bewirkt, dass eine Word-Vorlage heruntergeladen wird, die in einem Bitbucket-Repository gehostet wird. In anderen Fällen werden Cobalt Strike-Beacons installiert, um remote auf die Geräte der Opfer zugreifen zu können. Mit einem Cobalt Strike-Beacon können Bedrohungsakteure Remote-Befehle auf dem infizierten Gerät ausführen, um Daten zu stehlen oder sich lateral im Netzwerk zu verbreiten. Die aktuelle Phishing-Kampagne umfasst mehrere Stufen, wobei die meisten Schritte darauf beruhen, dass verschleierte Skripte aus dem Arbeitsspeicher des Hosts heraus ausgeführt werden und der Bitbucket-Dienst missbraucht wird, um einer Entdeckung zu entgehen.

Eine neue Phishing-Kampagne verbreitet den Fernzugriff-Trojaner „Warzone RAT“ (RAT = Remote Access Trojaner) in Ungarn. Die Kampagne basiert auf einer vermeintlichen Regierungs-E-Mail, die sorgfältig gefälscht ist und die Anwender dazu verleiten soll, die angehängte Malware auszuführen. Der Empfänger bekommt eine E-Mail, die sich als ungarisches Regierungsportal ausgibt, über das offizielle Geschäftsaktivitäten (wie das Einreichen von offiziellen Dokumenten oder die Bestellung von Ausweisen) abgewickelt werden können. Die E-Mail informiert den jeweiligen Empfänger, dass die benötigten Anmeldedaten, um auf das Portal zugreifen zu können, in der angehängten ZIP-Datei enthalten sind. Sobald dieser Anhang geöffnet wird, wird die Schadsoftware Warzone RAT extrahiert und ausgeführt. Warzone ist ein weit verbreiteter Trojaner, der im Rahmen eines Malware-as-a-Service (MaaS)-Modells betrieben wird. Die Malware kann als Abonnement für 37 Dollar pro Monat erworben werden. Cyberkriminelle können über diesen Trojaner diverse Dateien runter- oder hochladen, diese ausführen oder löschen, Befehle an die Konsole (Eingabeaufforderung) des infizierten Computers senden, Prozesse über den Task-Manager anzeigen oder beenden und unter Verwendung der IP-Adresse des Computers im Internet surfen. Mithilfe von Warzone kann auf die Webcams der Opfer zugegriffen und gespeicherte Kennwörter aus Browsern und E-Mail-Clients ausgelesen werden.

Ein weiteres Beispiel ist die Malware Lampion, die in jüngster Zeit in größeren Umfang verbreitet wurde, wobei die entsprechenden Bedrohungsakteure den bekannten Dienst WeTransfer für ihre Phishing-Kampagne missbrauchten. WeTransfer ist ein legitimer File-Sharing-Service, der kostenlos genutzt werden kann. Der Service wird monatlich von ca. 87 Millionen Nutzern in 190 Ländern genutzt. In einer neuen Kampagne verschicken die Betreiber des Banking-Trojaners „Lampion“ Phishing-E-Mails von kompromittierten Firmenkonten, über die die Opfer dazu verleitet werden sollen, einen angeblichen Zahlungsnachweis von WeTransfer herunterzuladen. Die Angriffsziele erhalten dafür ein ZIP-Archiv mit einer VBS-Datei (Virtual Basic Script). Das entsprechende Opfer muss aber die Datei ausführen, damit der Angriff starten kann. An diesem Punkt werden die enthaltenen DLL-Nutzlasten in den Arbeitsspeicher geladen, wodurch Lampion heimlich auf den kompromittierten Systemen ausgeführt werden kann. Lampion stiehlt dann Daten vom betroffenen Computer und versucht speziell an Bankkonto-Informationen heranzukommen, indem er Injektionen von einem C2-Server (Command & Control) abruft und manipulierte Formulare auf Anmeldeseiten einblendet. Wenn die Anwender dort ihre Anmeldedaten eingeben, werden die Daten über die fingierten Formulare gestohlen und an den Angreifer gesendet.

**Zusammengefasst:**

## Ein mehrschichtiger Cyberschutz-Ansatz, der auch eine Anti-Phishing-Technologie umfassen sollte, ist sehr wichtig. Selbst wenn manche Phishing-Versuche nicht direkt neutralisiert werden, können weitere Erkennungstools im mehrschichtigen Ansatz dann die tatsächliche Ausführung der Schadsoftware verhindern.

# 3. Datenschutzverletzungen erreichen einen neuen Höchststand

Laut dem „Cost of a Data Breach Report 2022“ von IBM belaufen sich die durchschnittlichen Gesamtkosten durch eine Datenschutzverletzung auf 4,35 Millionen Dollar (weltweit gemittelt). Gegenüber dem Vorjahr entspricht dies einem Anstieg von 0,11 Millionen Dollar. Wie zudem eine aktuelle Studie von Surfshark zeigt, wurden im dritten Quartal 2022 mehr als 100 Millionen Konten geknackt.

Es überrascht daher kaum, dass Cyberangriffe 88% aller Datenschutzverletzungen ausmachen, wie die „Q3 2022 Data Breach Analysis“ von Identity Theft zeigt. Im Rahmen von IT-Governance konnten 285 öffentlich bekannt gewordene Sicherheitsvorfälle zwischen Juli und September 2022 identifiziert werden, bei denen 232.266.148 Datensätze kompromittiert wurden. In einem kürzlich veröffentlichten Bericht meldete die ENISA (Agentur der Europäischen Union für Cybersicherheit), dass bei Ransomware-Angriffen monatlich Daten im Umfang von mehr als 10 TB gestohlen werden. Wie ein neuer Bericht der israelischen Sicherheitsfirma KELA zeigt, verkaufen sogenannte Initial Access Broker (IABs) weltweit die Zugriffe auf 576 Unternehmensnetzwerke für einen kumulierten Gesamtwert von 4.000.000 Dollar – und motivieren damit andere Cyberkriminelle zu Angriffen auf Unternehmen.

Auch wenn solche Zahlen je nach Quelle etwas variieren mögen, können auch wir von Acronis bestätigen, dass die Anzahl der Datenschutzverletzungen in der zweiten Jahreshälfte 2022 zugenommen hat – was ebenso für das gesamte Jahr gilt. Immer mehr Angreifer nutzen sogenannte MFA-Ermüdungsangriffe, die bei hochkarätigen Sicherheitsverletzungen auf dem Vormarsch sind. Diese spezielle Social Engineering-Technik hat sich insbesondere für die Bedrohungsakteure Lapsus$ und Yanluowang als sehr erfolgreich erwiesen, als sie in große und bekannte Unternehmen eingedrungen sind. Aber solche Datenschutzverletzungen sind nicht allein mit Ransomware-Angriffen assoziiert. Auch herkömmliche Datenexfiltrationen sind nach wie vor sehr beliebt. Entsprechend gab es im 3. Quartal 2022 eine Reihe großer Datenschutzverletzungen (siehe unten, gemessen an den Nutzern):

- **Neopets (69 Millionen)**
- **Shanghai COVID-19-App (48,5 Millionen)**
- **Mangatoon (23 Millionen)**
- **Swachh City-Plattform (16,4 Millionen)**

Die Crypto-Industrie ist trotz ihres jüngsten Absturzes immer noch ein attraktives Ziel für Cyberkriminelle. So hat die Cryptowährungsbrücke Nomad hat bei einem Angriff einen Verlust von fast 200 Millionen Dollar erlitten. Nomad ist eine Blockchain-übergreifende Brücke zwischen Ethereum, Moonbeam, Avalanche, Evmos und Milkomeda. Der Twitter-Nutzer „foobar“ hat darauf hingewiesen, dass das mutmaßliche Sicherheitsproblem hinter dem Cyberdiebstahl bereits zusammen mit Dutzenden weiteren Problemen bei einer Prüfung entdeckt wurde, die das Blockchain-Sicherheitsunternehmen Quantstamp in diesem Jahr durchgeführt hatte. Nomad glaubt allerdings, dass der Angriff nicht von einer einzelnen Person ausgeführt wurde. Zusätzlich könnten viele White Hat-Hacker oder Sicherheitsforscher Token auf ihre eigenen Adressen übertragen haben, um die Fonds zu schützen. Sollte dies zutreffen, werden die White Hat-Hacker die Fonds wahrscheinlich zurückgeben. Entsprechend hat Nomad auch eine Wallet-Adresse für diesen Zweck bereitgestellt.

Ein weiterer aktueller Crypto-Fall war der sogenannte QANplatform-Hack. Die Cryptowährungsbrücke gab bekannt, dass sie Cryptowährungen im Wert von schätzungsweise 2 Millionen Dollar verloren habe, nachdem ein Angreifer einen ihrer Smart Contracts manipulieren konnte.

Auch Großunternehmen werden weiterhin angegriffen. Medibank, einer der größten australischen privaten Krankenversicherer (mit ca. 3,9 Millionen Kunden), hat bekannt gegeben, dass bei einem kürzlichen Ransomware-Angriff unbefugt auf persönliche Kundeninformationen zugegriffen wurde. Nach einer Untersuchung meldete das Unternehmen, dass persönliche Daten von seiner Tochtergesellschaft „AHM Health Insurance“ und von internationalen Studenten angegriffen wurden. Es ist jedoch unklar, wie viele Kunden insgesamt betroffen waren. Zu den kompromittierten Daten gehören Vor- und Nachnamen, Adressen, Geburtsdaten, Krankenversicherungsnummern, Nummern der Versicherungspolice, Telefonnummern und Passnummern. Medibank betonte, dass es keinen Belege dafür gibt, dass auf Lastschriftdaten zugegriffen worden ist. Das Unternehmen hat die australische Bundespolizei (AFP) benachrichtigt und mitgeteilt, dass es von einem Kriminellen kontaktiert wurde, der vorgab, 200 GB an Daten entwendet zu haben. Die durch den Vorfall entstandenen Kosten wurden von Medibank auf 16-22 Millionen Dollar veranschlagt.

In Australien haben sich noch zwei weitere schwere Vorfälle ereignet. Der Einzelhandelsriese Woolworths hat eine Datenschutzverletzung gemeldet, von der etwa 2,2 Millionen MyDeal-Kunden betroffen waren. Auch das australische Mobilfunkunternehmen Optus, das eine Tochtergesellschaft von Singtel ist und über 10,5 Millionen Kunden betreut, hat eine Sicherheitsverletzung bekannt gegeben. Der Angreifer gab an, die Daten von rund 11 Millionen Kunden gestohlen zu haben. Eine kleine Auswahl dieser gestohlenen Daten wurde in einem Forum veröffentlicht, zusammen mit einer Lösegeldforderung von 1 Million Dollar. Optus hat sich daraufhin an die Strafverfolgungsbehörden gewendet, um den Vorfall

untersuchen zu lassen. Nachdem kein Lösegeld gezahlt wurde, haben die Angreifer einen Großteil der gestohlenen Daten veröffentlicht, sodass auch andere Bedrohungsakteure diese herunterladen und für ihre Kampagnen missbrauchen können. Nachdem der Bedrohungsakteur in den Fokus der Strafverfolgungsbehörden geriet, hat er schließlich seine Forderungen zurückgezogen. Die Angreifer haben sich außerdem bei über 10.000 Personen entschuldigt, deren persönliche Daten bereits veröffentlicht wurden.

Im September 2022 hat auch Uber eine Sicherheitsverletzung bekannt gegeben. Die Bedrohungsakteure haben sich Zugriff auf das Firmennetzwerk verschafft und interne Dokumente gestohlen. Laut der New York Times haben sich die Bedrohungsakteure zuerst in das Slack-Konto eines Mitarbeiters gehackt und dies dann ausgenutzt, um Mitarbeiter darüber zu informieren, dass das Unternehmen angeblich Opfer einer Datenschutzverletzung geworden wäre. Außerdem wurde eine Liste mit angeblich gehackten internen Datenbanken bereitgestellt. Das Unternehmen wurde dadurch gezwungen, seine internen Kommunikationssysteme und technischen Systeme offline zu nehmen, um den vermeintlichen Angriff einzudämmen und den Einbruch zu untersuchen. Die Angreifer haben mutmaßlich mehrere interne Systeme kompromittiert und der New York Times sowie einigen Cyber Security-Forschern Images von E-Mail-, Cloud Storage- und Code-Repositories zur Verfügung gestellt. Der Hacker behauptete, 18 Jahre alt zu sein, und fügte hinzu, dass die Sicherheitsmaßnahmen bei Uber unzureichend seien. In einer über Slack verbreiteten Nachricht forderte er außerdem, dass Uber-Fahrer eine höhere Bezahlung erhalten sollten. Dies ist nicht das erste Mal, dass das Unternehmen von einer Sicherheitsverletzung betroffen war. Schon in 2017 hatte eine Datenschutzverletzung, die offenbar bereits ein Jahr zuvor stattgefunden hatte, für Schlagzeilen gesorgt. Uber machte dafür einen Bedrohungsakteur verantwortlich, der vermutlich mit der Hacker-Gruppe Lapsus$ assoziiert war.

Der Elektronikriese Samsung hat eine neue Datenschutzverletzung bestätigt, nachdem im Juli 2022 einige seiner US-amerikanischen Systeme kompromittiert worden waren. Das Unternehmen hatte am 4. August entdeckt, dass sich Bedrohungsakteure Zugriff auf seine Systeme verschafft und persönliche Kundendaten exfiltriert haben.

Die Hotelgruppe Shangri-La hat eine Datenschutzverletzung in acht ihrer asiatischen Hotelanlagen bekannt gegeben, bei der Bedrohungsakteure zwischen Mai und Juli 2022 auf eine Datenbank mit den persönlichen Daten von Kunden zugreifen konnten. Von diesem Vorfall waren Hotels in Hongkong, Singapur, Chiang Mai, Taipeh und Tokio betroffen. Das Unternehmen hat eine Untersuchung veranlasst, um festzustellen, welche Daten von den Angreifern gestohlen wurden. Außerdem wurden die Behörden und alle potenziell betroffenen Gäste informiert.

Auch American Airlines hat eine Datenschutzverletzung gemeldet, bei der sich die Täter Zugriff auf eine unbekannte Anzahl von Mitarbeiter-E-Mail-Konten verschafft konnten. Zu den betroffenen Daten gehörten Namen, Geburtsdaten, Postanschriften, Telefonnummern, E-Mail-Adressen, Führerscheinnummern, Passnummern und/oder verschiedene medizinische Informationen, die von den betroffenen Personen angegeben worden waren. Der Sicherheitsverstoß wurde am 5. Juli 2022 entdeckt. Die Fluggesellschaft hat daraufhin umgehend Maßnahmen ergriffen, um den Vorfall einzudämmen und die betroffenen E-Mail-Konten abzusichern. American Airlines hat anschließend mithilfe einer führenden Cyber Security-Forensikfirma eine Untersuchung eingeleitet.

Die britische Fintech-Firma Revolut wurde Opfer eines Cyberangriffs, bei dem die Bedrohungsakteure Zugriff auf die persönlichen Daten von Zehntausenden von Kunden erlangen konnten. Bei dem Angriff wurden, wie von den Behörden bestätigt, die Daten von 50.150 Kunden in aller Welt (darunter allein 20.687 im Europäischen Wirtschaftsraum) kompromittiert. Zu den betroffenen Daten gehörten Namen, Adressen, E-Mails, Postanschriften, Telefonnummern, Auszüge aus Zahlungskartendaten (laut dem Unternehmen waren die eigentlichen Kartennummern maskiert) sowie Kontoinformationen und mehr. Die Angreifer konnten dagegen nicht auf Geldmittel der Nutzer zugreifen.

Bedrohungsakteure haben Quellcode und Gameplay-Videos für das anstehende Videospiel Grand Theft Auto 6 (GTA6) durchsickern lassen, nachdem sie angeblich in die Entwicklerfirma, Rockstar Games, eindringen konnten. Es scheint, dass die Angreifer den Slack-Server sowie das Confluence-Wiki von Rockstar Game kompromittiert haben, um an die Daten zu kommen.

Bei der Geschäftsstelle von Starbucks in Singapur kam es zu einem Datenschutzvorfall, von dem über 219.000 Kunden betroffen waren. Ein Datenverkäufer in den einschlägigen Foren behauptete, er habe schon eine Kopie der gestohlenen Daten für 3.500 Dollar verkauft und er wolle noch mindestens vier weitere Kopien an entsprechende Interessenten verkaufen.

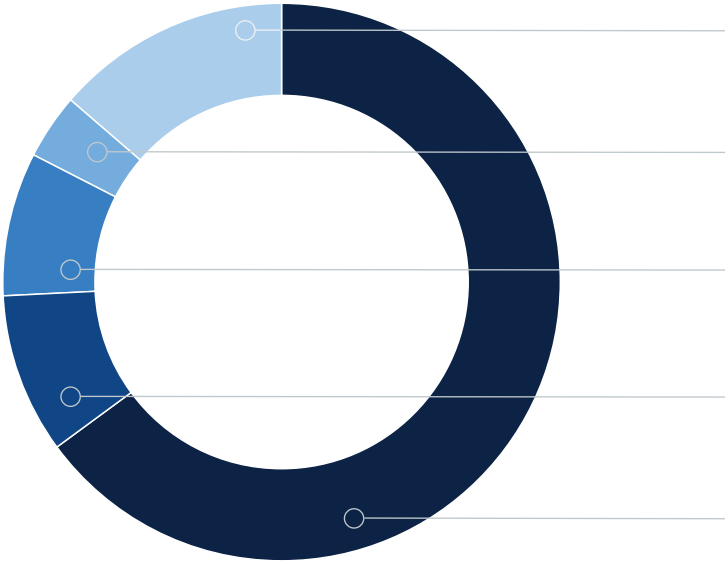
Und nicht zuletzt gilt: Vergessen Sie nie, dass man durch Datenschutzverletzungen nicht nur Daten, Geld und Zeit verlieren kann, sondern auch potenzielle Bußgelder drohen. Ein entsprechendes Beispiel dafür aus 2022 ist das Unternehmen SHEIN: Die New Yorker Generalstaatsanwaltschaft hat den chinesischen Online-Händler mit einer Geldstrafe von 1,9 Millionen Dollar für einen Dateneinbruch belegt, der schon in 2018 stattfand und bei dem Hacker die Daten von 6,42 Millionen Kunden erbeuten konnten.

# Allgemeine Malware-Bedrohung

Im 3. Quartal 2022 wurde bei durchschnittlich 11,7% unserer Kunden mindestens ein Malware-Angriff auf deren Endpunkten erfolgreich blockiert. Gegenüber dem zweiten Quartal entspricht dies einem leichten Anstieg von 9,4%. Diese Zahlen zeigen, dass immer noch jede zehnte Bedrohung bis zum Endpunkt kommt, trotz aller Bemühungen der Unternehmen bezüglich Sensibilisierungstraining und Sicherheitspatching. Da diese Erkennungsraten auf den geschützten Endpunkten erhoben wurden, bedeutet dies auch, dass ein Proxy oder E-Mail-Schutz, der auf diesen Endpunkten bereitgestellt wurde, diese Bedrohungen nicht zuverlässig blockieren kann.

AV-TEST

In den ersten zwei Wochen vom November 2022 entdeckte Malware-Typen (Quelle: av-test.org)



**13,8%** Andere

**3,6%** Backdoor

**8,4%** Downloader

**9,3%** Würmer

**64,9%** Trojaner

**Prozentsatz der Kunden mit blockierter Malware**

| Monat in 2022 | Prozentsatz der Kunden mit blockierter Malware |
|---|---|
| Januar | 10,7 |
| Februar | 8,7 |
| März | 8 |
| April | 9,2 |
| Mai | 9,7 |
| Juni | 9,4 |
| Juli | 8,7 |
| August | 8,4 |
| September | 17,9 |
| Oktober | 9,6 |
| November | 10,4 |

Die Zahl der neuen Malware-Samples, die in freier Wildbahn auftauchen, ist seit 2021 leicht gestiegen. Das Wachstum pro Jahr hat sich jedoch verlangsamt. Wie aus verschiedenen Quellen hervorgeht, liegt die Rate immer noch bei fast 9 Millionen neuen Samples pro Monat. Dieser Anteil entspricht auch der Anzahl der neuen Samples, die von den Acronis CPOCs beobachtet wurden.

Die durchschnittliche Lebensdauer der Malware-Samples betrug im November 2022 1,7 Tage. Danach verschwindet eine Bedrohung und wird nie wieder gesehen. Im 2. Quartal 2022 lag diese Zahl noch bei 2,3 Tagen. Dies zeigt, dass Malware immer schnelllebiger wird. Denn die Angreifer können neue Malware-Samples dank Automatisierungs- und Personalisierungstechniken mittlerweile so schnell erstellen, dass herkömmliche, auf Signaturen basierende Erkennungsmethoden überfordert sind. 74% der beobachteten Samples wurden in unserer Kundenbasis nur ein einziges Mal gesehen.

**Folgende Malware-Familien wurden im dritten Quartal am häufigsten beobachtet, wobei der Schwerpunkt eindeutig bei Bots und Informationsdiebstahl liegt:**

- FormBook
- AgentTesla
- LokiBot
- Snake Keylogger
- Remcos
- RedLine Stealer
- Emotet
- Raccoon Stealer
- njRAT
- AsyncRAT

Die USA waren im Oktober 2022 mit 22,1% das Land mit den meisten Malware-Erkennungen bei den Kunden von Acronis – gefolgt von Deutschland mit 8,8% und Brasilien mit 7,8%. Diese Ergebnisse sind denen vom 2. Quartal sehr ähnlich, mit Ausnahme der USA und Deutschland (wo es einen leichten Anstieg gab, insbesondere bei den Finanz-Trojanern).

In diesen Ländern waren vor allem MSP und Großunternehmen für die Cyberkriminellen attraktiv.

So war beispielsweise der Notrufdienst 111 des britischen Gesundheitssystems (NHS) von einem erheblichen und anhaltenden Ausfall betroffen. Auslöser war ein Cyberangriff auf die Systeme des britischen MSP „Advanced“, der die entsprechende Software für ca. 85% der Notrufstellen liefert. Advanced erstellt Unternehmenssoftware für mehr als 22.000 Kunden weltweit und ist in verschiedenen Branchen tätig, vom Gesundheits- und Bildungswesen bis hin zu gemeinnützigen Organisationen. Auf der Kundenliste des MSP stehen unter anderem das NHS, das britische Ministerium für Arbeit und Renten (DWP) sowie der Londoner City Airport. Die nationale Strafverfolgungsbehörde (NCA) und das nationale Zentrum für Cybersicherheit (NCSC) wurden beide an den Ermittlungen beteiligt.

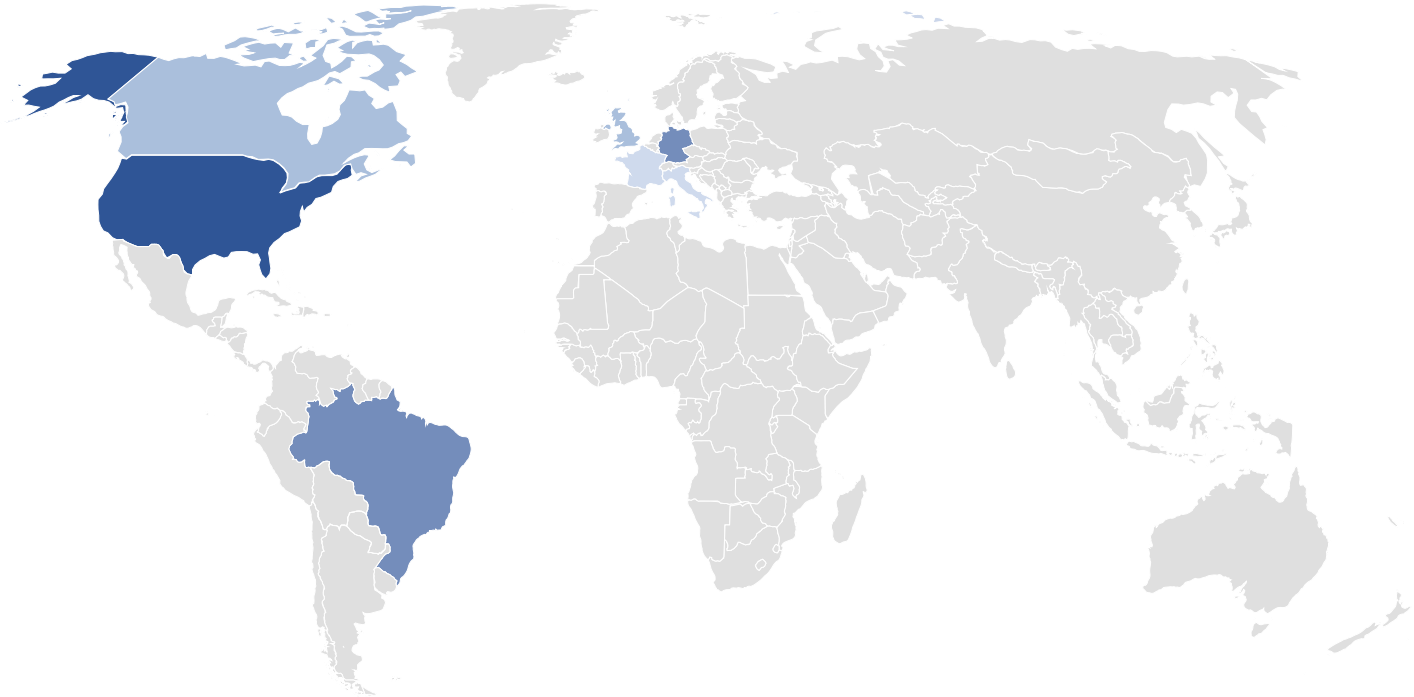
Ein weiteres Beispiel ist das Unternehmen SHI, welches zu den 15 größten IT Service Providern der Welt gehört. Es beschäftigt über 5.000 Mitarbeiter und konnte 2021 seinen Jahresumsatz um 10% (auf 12,3 Milliarden Dollar) steigern. SHI wurde Opfer eines koordinierten und professionellen Malware-Angriffs. Es gibt jedoch keine Anzeichen dafür, dass irgendwelche Daten seiner rund 15.000 Kunden (von Klein- bis Großunternehmen, aus dem öffentlichen Sektor oder aus dem akademischen Bereich) exfiltriert wurden. Und es scheinen auch keine Systeme von Drittanbietern in der Lieferkette von SHI von dem Angriff betroffen gewesen zu sein. Der Umstand, dass die betroffenen Systeme offline genommen wurden und die Wiederherstellungmaßnahmen noch andauern, lässt vermuten, dass es sich um einen Angriff mit Ransomware gehandelt haben dürfte. Der in New Jersey ansässige Reseller arbeitet mit US-amerikanischen Behörden wie dem FBI und der CISA (Cyber Security & Infrastructure Security Agency) zusammen, um den Angriff zu untersuchen.

Auch der Bankensektor ist weiterhin ein Hauptziel für Angriffe. Und die Bedrohungen in diesem Bereich entwickeln sich weiter. Die EAST (European Association of Secure Transactions), ein Branchenverband von Banken und Geldautomatenanbietern, gab bekannt, dass ihr mindestens 501 Fälle von Geldautomatendiebstählen bekannt geworden sind, bei denen Angreifer eine neue Art eines sogenannten MitM/Relay-Angriffs verwendeten, um Kundengelder zu stehlen.

## Prozentsatz der globalen Malware-Erkennungen (in 2022, aufgeschlüsselt nach Monat und Land)

| Land | Jan | Feb | Mrz | Apr | Mai | Jun | Jul | Aug | Sep | Okt | Nov |
|---|---|---|---|---|---|---|---|---|---|---|---|
| USA | 24,4 | 25,4 | 24,6 | 23,7 | 22,8 | 21,8 | 20,1 | 22,6 | 21,9 | 22,1 | 21,5 |
| Deutschland | 13,2 | 12,7 | 11,2 | 11 | 9,4 | 8,9 | 8,2 | 8,5 | 9,1 | 8,8 | 8,9 |
| Brasilien | 4,7 | 3,6 | 3,9 | 4,5 | 7,2 | 7,8 | 9,6 | 9,5 | 7,7 | 7,3 | 6,9 |
| Italien | 4,8 | 4,3 | 5,1 | 5,7 | 6,6 | 6 | 6,2 | 4,5 | 5,9 | 5 | 5,1 |
| Kanada | 7,1 | 7,2 | 7,3 | 6,5 | 6,2 | 5,6 | 4,9 | 6 | 4,7 | 5,5 | 5,8 |
| Vereinigtes Königreich (UK) | 5 | 5,4 | 5,4 | 5,3 | 5,3 | 4,9 | 4,8 | 5 | 6,7 | 5,2 | 4,9 |
| Singapur | 4,2 | 5 | 4,9 | 4,9 | 3,9 | 4,8 | 5,4 | 4,6 | 3,5 | 4,3 | 4,5 |
| Japan | 2,6 | 3 | 3,1 | 3 | 2,8 | 3,1 | 3,2 | 3 | 3,1 | 3,7 | 3,4 |
| Frankreich | 2,8 | 2,9 | 2,8 | 2,9 | 2,9 | 2,5 | 2,7 | 2,5 | 3,5 | 3 | 3,2 |
| Schweiz | 3 | 2,8 | 2,9 | 2,6 | 2,4 | 4,1 | 2,3 | 2,7 | 2,9 | 2,7 | 3,2 |

## Malware-Erkennungen, im November 2022



Prozentsatz

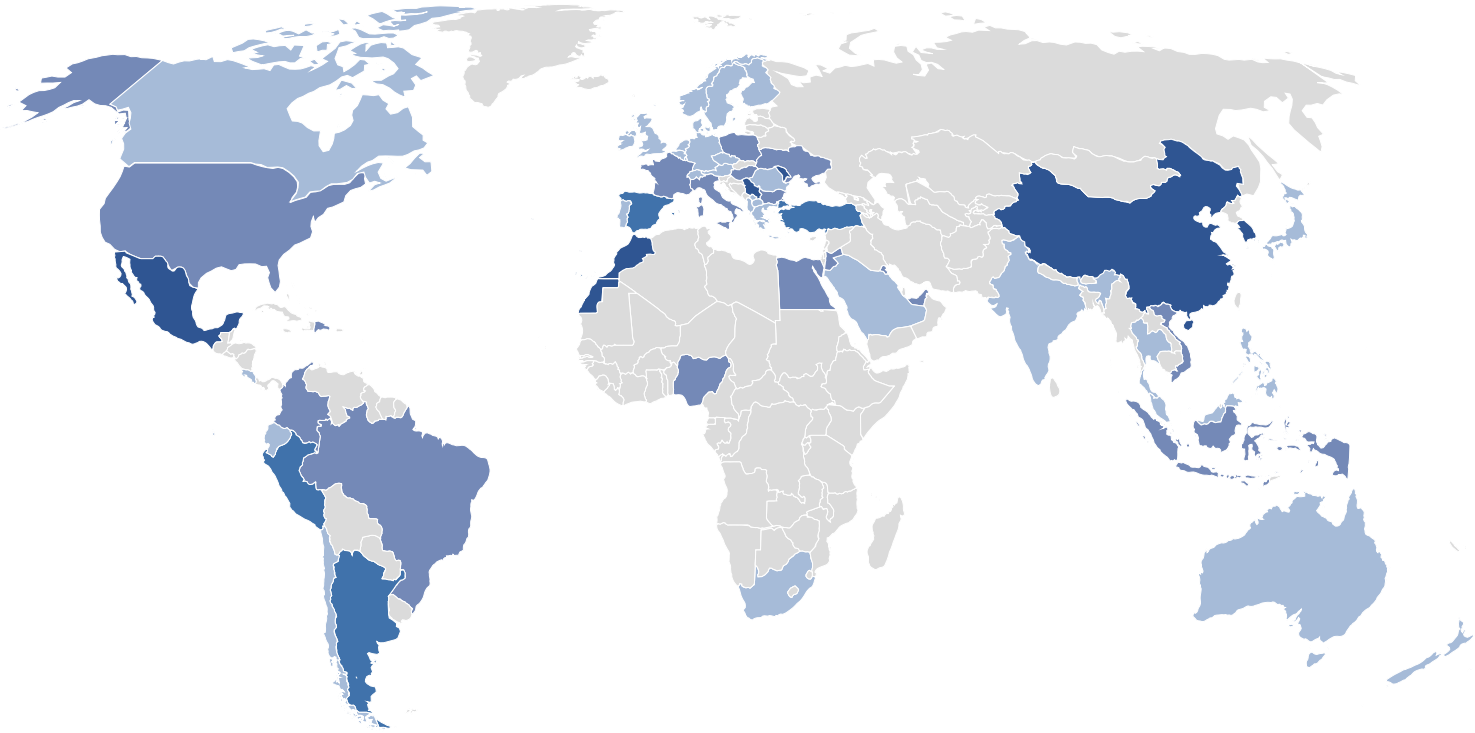
3% 22%

Wenn wir die Anzahl der Malware-Erkennungen pro aktivem Kunden und pro Land normalisieren, erhalten wir eine etwas andere Verteilung. Die nachfolgende Tabelle zeigt den normalisierten Prozentsatz von Kunden mit mindestens 25 aktiven Maschinen und mindestens 25 Malware-Erkennungen pro Land im November 2022. Dieser Prozentsatz bedeutet, dass von allen aktiv geschützten Workloads in dem betreffenden Land mindestens ein Malware-Angriff blockiert wurde.

**Prozentsatz der globalen Malware-Erkennungen (in 2022, aufgeschlüsselt nach Monat und Land)**

| Rang | Land | Prozentsatz der Kunden mit Malware-Erkennungen im November 2022 |
|---|---|---|
| 1 | Ägypten | 32,3 |
| 2 | China | 27,6 |
| 3 | Nigeria | 26,3 |
| 4 | Marokko | 25,2 |
| 5 | Thailand | 25 |
| 6 | Südkorea | 24,5 |
| 7 | Türkei | 23,9 |
| 8 | Vietnam | 22,5 |
| 9 | Indien | 22,5 |
| 10 | Singapur | 21,7 |
| 11 | Taiwan | 21,5 |
| 12 | Republik Moldau | 21,3 |
| 13 | Dominikanische Republik | 21,2 |
| 14 | Serbien | 19 |
| 15 | Bulgarien | 18,6 |
| 16 | Ungarn | 18 |
| 17 | Peru | 17,9 |
| 18 | Israel | 17,7 |
| 19 | Argentinien | 16,6 |
| 20 | Königreich Jordanien | 16,5 |
| 21 | Philippinen | 15,9 |
| 22 | Indonesien | 15,6 |
| 23 | Brasilien | 15 |
| 24 | Spanien | 14,6 |
| 25 | Vereinigte Arab. Ermirate | 14,5 |
| 26 | Ukraine | 14,2 |
| 27 | Ecuador | 14 |
| 28 | Kuwait | 13,8 |
| 29 | Mexiko | 13,7 |
| 30 | Nord-Mazedonien | 13,3 |

## Normalisierte Malware-Erkennungen, im November 2022



Prozentsatz

4% 32%

## Regional normalisierte Malware-Erkennungsraten

Die Top-10-Länder: normalisierte Malware-Erkennungsraten nach Region

**Asien**

| Rang | Land | Regional normalisierter Prozentsatz der Malware-Erkennungen im November 2022 |
|---|---|---|
| 1 | China | 27,6 |
| 2 | Thailand | 25 |
| 3 | Südkorea | 24,5 |
| 4 | Vietnam | 22,5 |
| 5 | Indien | 22,5 |
| 6 | Singapur | 21,7 |
| 7 | Taiwan | 21,5 |
| 8 | Philippinen | 15,9 |
| 9 | Indonesien | 15,6 |
| 10 | Japan | 12,2 |

## EMEA

| Rang | Land | Regional normalisierter Prozentsatz der Malware-Erkennungen im November 2022 |
|---|---|---|
| 1 | Ägypten | 32,3 |
| 2 | Nigeria | 26,3 |
| 3 | Marokko | 25,2 |
| 4 | Türkei | 23,9 |
| 5 | Republik Moldau | 21,3 |
| 6 | Serbien | 19 |
| 7 | Bulgarien | 18,6 |
| 8 | Ungarn | 18 |
| 9 | Israel | 17,7 |
| 10 | Königreich Jordanien | 16,5 |

## Amerika

| Rang | Land | Regional normalisierter Prozentsatz der Malware-Erkennungen im November 2022 |
|---|---|---|
| 1 | Dominikanische Republik | 21,2 |
| 2 | Peru | 17,9 |
| 3 | Argentinien | 16,6 |
| 4 | Brasilien | 15 |
| 5 | Ecuador | 14 |
| 6 | Mexiko | 13,7 |
| 7 | Kolumbien | 12 |
| 8 | Costa Rica | 11,5 |
| 9 | USA | 10,1 |
| 10 | Chile | 8,8 |

# Ransomware-Bedrohung

Wie bereits im Abschnitt über die wichtigsten Trends erwähnt, stellt Ransomware immer noch die größte Cyberbedrohung für Unternehmen dar. In diesem Abschnitt konzentrieren wir uns auf die Aktivitäten von Juli bis November 2022. Dazu gehören Angriffe, die von unserer bedrohungsagnostischen Acronis Active Protection-Technologie abgewehrt wurden, sowie Daten, die auf Untergrund-Leakseiten von Ransomware-Betreibern veröffentlicht wurden.

**Dies sind die zehn aktivsten Ransomware-Familien, die wir im zweiten Halbjahr 2022 beobachten und verfolgen konnten.**

- Lockbit
- Black Basta
- LV
- Ragnar Locker
- STOP
- BlackCat/ALPHV
- Vice Society
- Hive
- Everest
- Royal

Beachten Sie, dass einige Gruppen versuchen, mit einem breit angelegten Ansatz möglichst viele Endbenutzer zu infizieren, während andere sich auf bestimmte hochwertige Ziele konzentrieren. Hier erfolgen meist zwar nur wenige gezielte Infektionsversuchen, diese sollen dafür aber einen hohen Gewinn abwerfen. Daher ist die Anzahl der erkannten Bedrohungen allein kein Hinweis darauf, wie gefährlich eine bestimmte Bedrohung wirklich ist. Darüber hinaus betreiben viele Gruppen ein Ransomware-as-a-Service-Business. Außerdem können Angreifer mehrere Bedrohungsfamilien bei ähnlichen Angriffen einsetzen.

Im dritten Quartal wurden insgesamt 576 Kompromittierungen durch Ransomware öffentlich bekannt, was einem leichten Anstieg gegenüber dem Vorquartal entspricht. Dies ist natürlich nur eine Teilmenge der tatsächlichen Opfer, da einige mit den Ransomware-Gruppen verhandeln und diese schließlich bezahlen, damit der Angriff eben nicht öffentlich bekannt wird. Außerdem haben sich einige Gruppen auf reine Datenexfiltrationen verlegt. Solche Angriffe werden daher evtl. nicht mehr als Ransomware-Vorfälle, sondern nur als Datenschutzverletzungen eingestuft.

### Ransomware-Erkennungen (pro Tag)

Die Zahl der Ransomware-Vorfälle ist im 3. Quartal leicht zurückgegangen – nach einem Höchststand in den Sommermonaten. Von Juli bis August haben wir bei den blockierten Ransomware-Angriffen einen weltweiten Anstieg um 49% verzeichnet. Darauf folgte im September ein Rückgang um 12,9% und im Oktober um 4,1%.

### Veränderungen in der Anzahl der Ransomware-Erkennungen pro Quartal und Region:

| Monat | EMEA | Amerika | Asien | Global |
|---|---|---|---|---|
| Juli–August | 36,3 | 23,3 | 28,6 | 49 |
| August–September | -11,7 | -5,9 | -21,2 | -12 |
| September–Oktober | -23,2 | 5,8 | -6 | -4,1 |

### Weltweite Ransomware-Erkennungen (pro Tag):

### Ransomware-Erkennungen pro Tag:

| Monat | Ransomware-Erkennungen pro Tag |
|---|---|
| Januar | 540 |
| Februar | 335 |
| März | 201 |
| April | 237 |
| Mai | 566 |
| Juni | 329 |
| Juli | 272 |
| August | 242 |
| September | 237 |
| Oktober | 295 |
| November | 307 |

### Die Top-10-Länder: Ransomware-Erkennungen nach Region

**Asien**

| Land | Regionaler Prozentsatz der Ransomware-Erkennungen im 3. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 2. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 1. Quartal 2022 |
|---|---|---|---|
| Japan | 26,6 | 37,3 | 34,3 |
| China | 9,8 | 12 | 13,1 |
| Philippinen | 2,4 | 5,8 | 4 |
| Taiwan | 3,9 | 5,1 | 4,9 |
| Indien | 2,5 | 4,2 | 5,9 |
| Südkorea | 2,9 | 4,1 | 4,5 |
| Türkei | 2,6 | 4 | 5,1 |
| Singapur | 0,6 | 3 | 1,8 |
| Vietnam | 1,4 | 2,6 | 1,4 |
| Thailand | 1,5 | 2,1 | 2,7 |

## EMEA

| Land | Regionaler Prozentsatz der Ransomware-Erkennungen im 3. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 2. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 1. Quartal 2022 |
|---|---|---|---|
| Deutschland | 54,2 | 44 | 48,1 |
| Vereinigtes Königreich (UK) | 11,1 | 8,7 | 7,7 |
| Frankreich | 9,3 | 8,1 | 7,1 |
| Italien | 7,6 | 6,2 | 5,3 |
| Schweiz | 6,5 | 4,7 | 5 |
| Spanien | 4,1 | 4,6 | 3,5 |
| Niederlande | 3,7 | 2,9 | 3 |
| Österreich | 3,3 | 2,6 | 2,8 |
| Tschechische Republik | 2,5 | 1,8 | 2 |
| Ukraine | 1,8 | 1,8 | 1,9 |

## Amerika

| Land | Regionaler Prozentsatz der Ransomware-Erkennungen im 3. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 2. Quartal 2022 | Regionaler Prozentsatz der Ransomware-Erkennungen im 1. Quartal 2022 |
|---|---|---|---|
| USA | 60 | 62,7 | 65 |
| Kanada | 19,7 | 23,9 | 25,1 |
| Mexiko | 2,7 | 3,8 | 2,8 |
| Brasilien | 1,4 | 1,7 | 1,6 |
| Argentinien | 1,2 | 1,4 | 0,9 |
| Kolumbien | 0,5 | 1,1 | 0,6 |
| Peru | 0,4 | 0,9 | 0,5 |
| Chile | 0,5 | 0,8 | 0,6 |
| Guatemala | 0,1 | 0,6 | 0,4 |
| Ecuador | 1,2 | 0,4 | 0,3 |

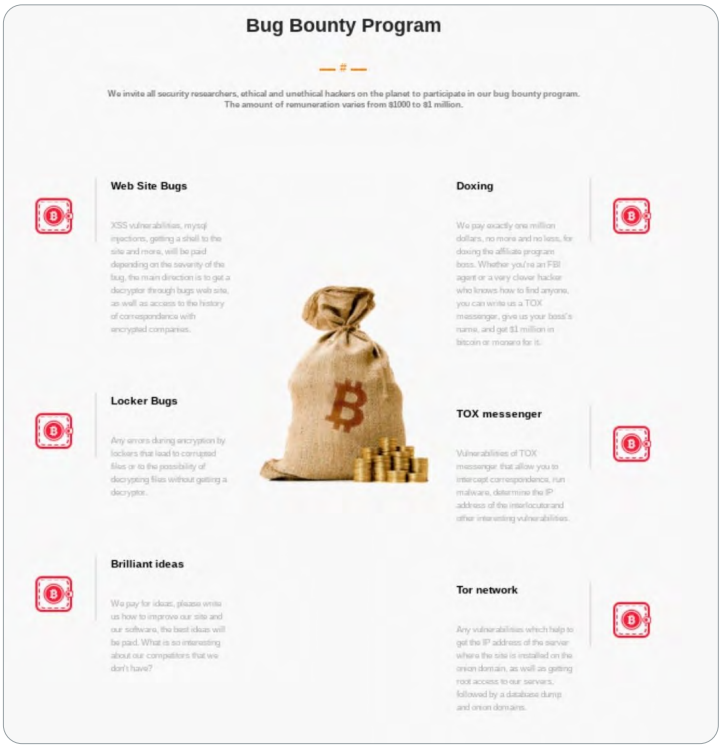
# Ransomware-Gruppen im Blickpunkt

**LockBit 3.0: Ransomware mit Bug Bounty-Programm**

Am 17. Mai 2022 hat der LockBit-Sprecher „LockBitSupp“ bekannt gegeben, dass in naher Zukunft eine neue Version der berüchtigten Ransomware veröffentlicht werden wird.

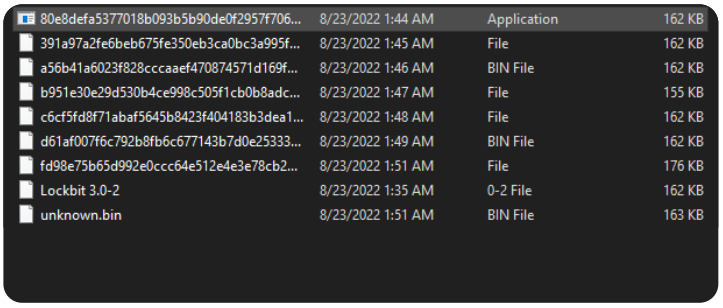
Später wurde über das Twitter-Konto **vx-underground** Bilder der LockBit 3.0-Website, generierte Ransomware-Dateien und Verschlüsselungsergebnisse geteilt. Die Version 3.0 wurde von Bedrohungsakteuren als „LockBit Black“ bezeichnet. Cyber Security-Analysen ergaben Ähnlichkeiten mit der Ransomware BlackMatter/DarkSide.

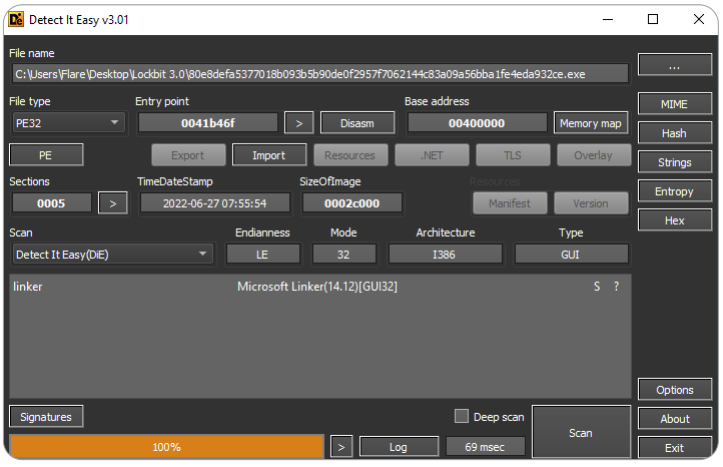
Diese neue Version 3.0 verfügt über eine chiffrierte Funktionalität im Abschnitt '.text', die nur mit einem Schlüssel dechiffriert werden kann, der als '-pass'-Argument in der Befehlszeile anzugeben ist. Die Version kann Dateien verschlüsseln, deren Symbole, Dateinamen und Erweiterungen ändern, den Hintergrund des Desktops ändern und eine Lösegeldforderung in jedem verschlüsselten Ordner ablegen. Bemerkenswert ist, dass mit LockBit 3.0 das erste Ransomware-Bug-Bounty-Programm eingeführt wurde, bei dem Personen, die Fehlerberichte einreichen, Geld dafür erhalten. Es hat bereits mehrere solcher Meldungen und mindestens eine Auszahlung gegeben.




## Überblick über Lockbit 3.0

Fast alle gefundenen Samples sind ausführbare PE32-Dateien und haben eine ähnliche Größe. Tatsächlich verwendet jedes Sample die gleiche Logik. Auch das Tool „Detect It Easy“ kann nicht feststellen, in welcher Sprache sie geschrieben wurden.



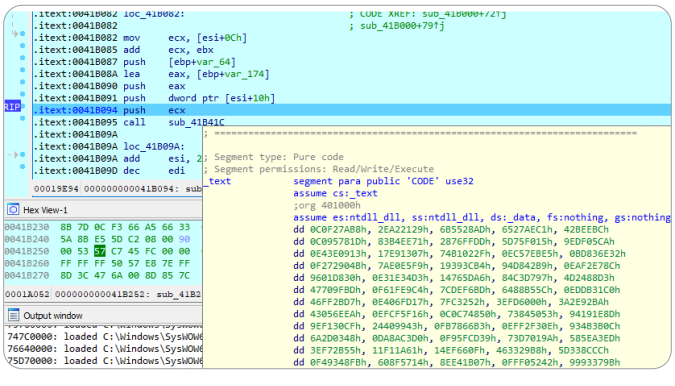

Bei einem ersten Blick in den IDA-Disassembler haben diese Samples nicht viele Funktionen, Strings und Importe. Es gibt jedoch ein verschlüsseltes '.text'-Segment mit einer Ausführungsberechtigung, das mehr als die Hälfte des Dateiumfangs ausmacht.

```
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Write/Execute
.text:00401000 _text           segment para public 'CODE' use32
.text:00401000                 assume cs:_text
.text:00401000                 ;org 401000h
.text:00401000                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000                 dd 0C0F27AB8h, 2EA22129h, 6B5528ADh, 6527AEC1h, 428EEBCh
.text:00401000                 dd 0C095781Dh, 83B4EE71h, 2876FFDDh, 5D75F015h, 9EDF05CAh
.text:00401000                 dd 0E43E0913h, 17E91307h, 74B1022Fh, 0EC57EBE5h, 0BD836E32h
.text:00401000                 dd 0F2729048h, 7AE0E5F9h, 19393CB4h, 94D842B9h, 0EAF2E78Ch
.text:00401000                 dd 9601D830h, 0E31E34D3h, 14765DA6h, 84C3D797h, 4D2488D3h
.text:00401000                 dd 47709FBDh, 0F61FE9C4h, 7CDEF6BDh, 6488B55Ch, 0EDDB31C0h
.text:00401000                 dd 46FF2BD7h, 0E406FD17h, 7FC3252h, 3EFD6000h, 3A2E92BAh
.text:00401000                 dd 43056EEAh, 0EFCF5F16h, 0C0C74850h, 73845053h, 94191E8Dh
.text:00401000                 dd 9EF130CFh, 24409943h, 0FB7866B3h, 0EFF2F30Eh, 934B3B0Ch
.text:00401000                 dd 6A2D0348h, 0DA8AC3D0h, 0F95FCD39h, 73D7019Ah, 585EA3EDh
```

## Ausführung

LockBit 3.0 muss über die Eingabeaufforderung mit dem Argument '-pass' ausgeführt werden. Dies erinnert an die Ransomware ALPHV, die einen Zugriffstoken verwendet, um die Ausführung zu starten. Bei LockBit ist dieses Argument ein Schlüssel, der zur Dechiffrierung des '.text'-Segments verwendet wird. Die Schlüssel unterscheiden sich je nach Sample. Ein Beispiel: Für das Sample sha256:80e8defa5377018b093b5b90de0f29 57f7062144c83a09a56bba1fe4eda932ce lautet der darauf folgende Schlüssel: db66023ab2abcb9957fb01ed50cdfa6a


Beim Ausführungsstart ruft LockBit die Funktion 'sub41B000' auf, die den angegebenen Schlüssel übernimmt und das Segment '.text' in die Funktion 'sub_41B41C' lädt.



LockBit unterteilt die geladenen Segmente in kleinere Abschnitte und entschlüsselt diese mit der Dechiffrierungsfunktion 'sub_41B41C'.

```
.itext:0041B41C push    ebp
.itext:0041B41D mov     ebp, esp
.itext:0041B41F push    ebx
.itext:0041B420 push    esi
.itext:0041B421 push    edi
.itext:0041B422 xor     eax, eax
.itext:0041B424 mov     ebx, [ebp+arg_C]
.itext:0041B427 xor     ecx, ecx
.itext:0041B429 xor     edx, edx
.itext:0041B42B mov     esi, [ebp+arg_4]
.itext:0041B42E mov     edi, [ebp+arg_0]
.itext:0041B431 test    esi, esi
.itext:0041B433 jz      short loc_41B468
.itext:0041B435 push    ebp
.itext:0041B436 mov     ebp, [ebp+arg_8]
.itext:0041B439
.itext:0041B439 loc_41B439:                             ; CODE XREF: sub_41B41C+49↓j
.itext:0041B439 mov     dl, [ebp+ecx+var_s0]
.itext:0041B43D add     dl, bl
.itext:0041B43F mov     bl, [ebp+edx+var_s0]
.itext:0041B443 mov     dl, [ebp+ebx+var_s0]
.itext:0041B447 mov     dl, [ebp+edx+var_s0]
.itext:0041B44B inc     dl
.itext:0041B44D mov     al, [ebp+edx+var_s0]
.itext:0041B451 xor     [edi], al
.itext:0041B453 mov     dl, [ebp+ebx+var_s0]
.itext:0041B457 xchg    dl, [ebp+ecx+var_s0]
.itext:0041B45B mov     [ebp+ebx+var_s0], dl
.itext:0041B45F inc     cl
.itext:0041B461 inc     edi
.itext:0041B462 dec     esi
.itext:0041B463 test    esi, esi
.itext:0041B465 jnz     short loc_41B439
.itext:0041B467 pop     ebp
```

Danach wird die Funktion aus dem entschlüsselten Segment aufgerufen:

```
.itext:0041B46F public start
.itext:0041B46F start:
.itext:0041B46F nop
.itext:0041B470 nop     dword ptr [eax+eax+00000000h]
.itext:0041B478 call    sub_41B000                      ; decrypt
.itext:0041B47D nop     dword ptr [eax+00h]
.itext:0041B481 call    loc_408254                      ; decrypted segment
.itext:0041B486 xchg    ax, ax
.itext:0041B488 call    sub_40B804
.itext:0041B48D nop     dword ptr [eax+eax+00h]
.itext:0041B492 call    loc_418F78                      ; decrypted segment
.itext:0041B497 nop     dword ptr [eax+eax+00000000h]
.itext:0041B49F push    0
.itext:0041B4A1 call    dword_4275C0
```

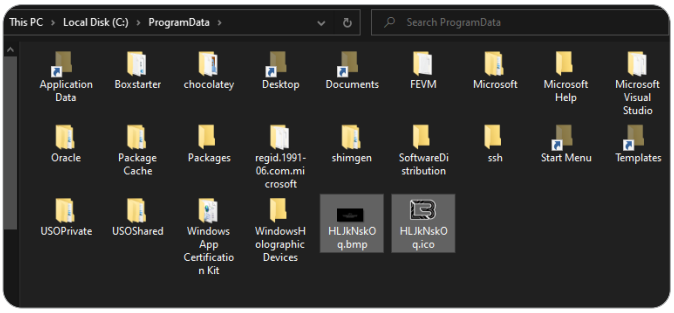
Im dechiffrierten Abschnitt verbirgt LockBit seine WinAPI-Funktionen, Aufrufe und Strings. Es verwendet die Funktion 'sub_407C5C', um die tatsächlichen APIs aufzulösen. Diese Technik wird auch von der Ransomware BlackMatter verwendet.

```
.text:004082B1 push    offset unk_407DA4
.text:004082B6 push    offset unk_427408
.text:004082BB call    sub_407C5C
.text:004082C0 push    edi
.text:004082C1 push    esi
.text:004082C2 push    offset unk_407E94
.text:004082C7 push    offset unk_4274F4
.text:004082CC call    sub_407C5C
.text:004082D1 push    edi
.text:004082D2 push    esi
.text:004082D3 push    offset unk_407F88
.text:004082D8 push    4275E4h
.text:004082DD call    sub_407C5C
.text:004082E2 push    edi
.text:004082E3 push    esi
.text:004082E4 push    40802Ch
.text:004082E9 push    427684h
.text:004082EE call    sub_407C5C
.text:004082F3 push    edi
.text:004082F4 push    esi
.text:004082F5 push    408040h
.text:004082FA push    427694h
.text:004082FF call    sub_407C5C
.text:00408304 push    edi
.text:00408305 push    esi
.text:00408306 push    40807Ch
.text:0040830B push    4276CCh
.text:00408310 call    sub_407C5C
.text:00408315 push    edi
.text:00408316 push    esi
.text:00408317 push    4080D4h
.text:0040831C push    427720h
.text:00408321 call    sub_407C5C
```

Diese Funktion lädt eine verschleierte Zeichenfolge und führt eine XOR-Operation mit '4506DFCA' als Schlüssel durch. Das Ergebnis ist der WinAPI-Name.

```
.text:00407C62 mov     esi, [ebp+arg_4]
.text:00407C65 lodsd
.text:00407C66 xor     eax, 4506DFCAh
.text:00407C6B push    eax
.text:00407C6C call    sub_407AE0
.text:00407C71 test    eax, eax
.text:00407C73 jz      loc_407D9C
.text:00407C79 mov     edi, [ebp+arg_0]
.text:00407C7C add     edi, 4
```

Während der Ausführung legte LockBit zwei Dateien im Ordner 'C:\ProgramData' ab. Die erste Datei (eine .bmp-Datei) wird zum Ändern des Desktophintergrunds verwendet. Die zweite Datei (eine .ico-Datei) wird verwendet, um die Symbole der verschlüsselten Dateien zu ändern.



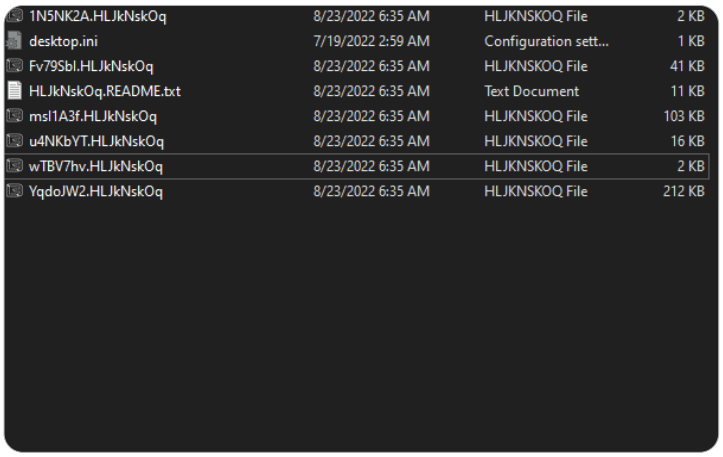

Um einer Entdeckung zu entgehen, ändert LockBit nach der Ausführung alle Unterschlüssel im Registry-Pfad HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\. Diese Schlüssel betreffen das Windows-Ereignisprotokoll. LockBit ändert bei allen von diesen Schlüsseln zwei Werte:

**ChannelAccess –** O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)

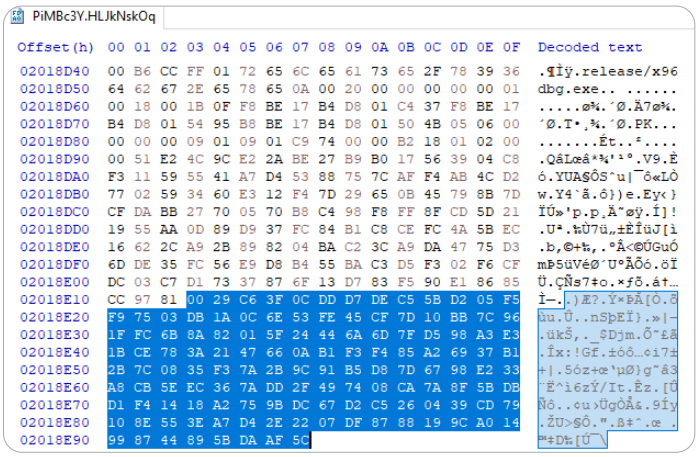
**Enabled –** 0

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| ChannelAccess | REG_SZ | O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA) |
| Enabled | REG_DWORD | 0x00000000 (0) |
| Isolation | REG_DWORD | 0x00000001 (1) |
| MaxSize | REG_DWORD | 0x00040000 (262144) |
| MaxSizeUpper | REG_DWORD | 0x00000000 (0) |
| OwningPublisher | REG_SZ | {11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78} |
| Type | REG_DWORD | 0x00000001 (1) |

Die verschlüsselten Dateien erhalten die Erweiterung '.HLJkNskOq' sowie einen neuen, zufällig generierten Namen und ein geändertes Dateisymbol. An das Ende aller verschlüsselten Dateien werden außerdem 133 Bytes angehängt, die als Dechiffrierungs-ID dienen.

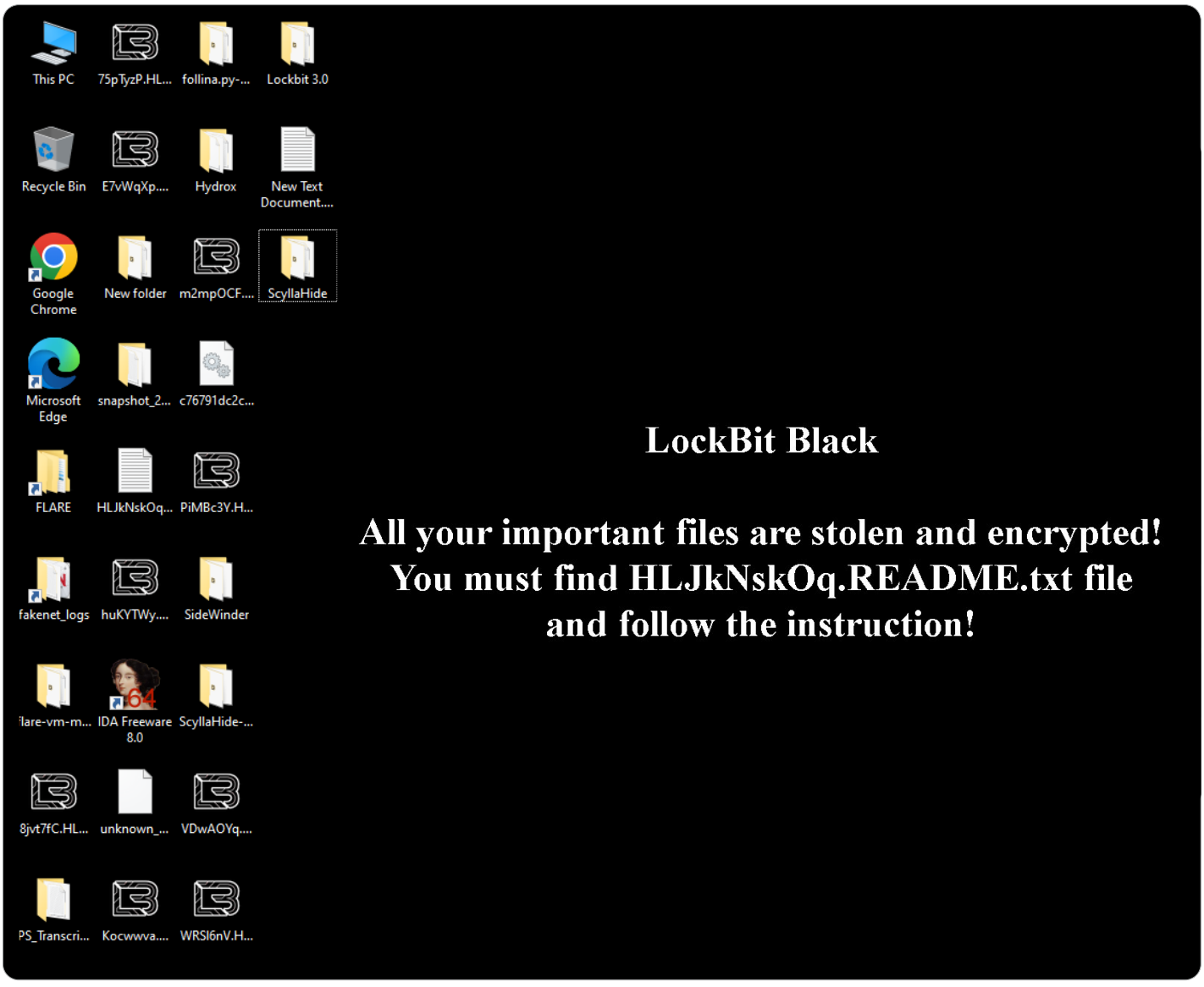


| | | | |
|---|---|---|---|
| 1N5NK2A.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 2 KB |
| desktop.ini | 7/19/2022 2:59 AM | Configuration sett... | 1 KB |
| Fv79Sbl.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 41 KB |
| HLJkNskOq.README.txt | 8/23/2022 6:35 AM | Text Document | 11 KB |
| msl1A3f.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 103 KB |
| u4NKbYT.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 16 KB |
| wTBV7hv.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 2 KB |
| YqdoJW2.HLJkNskOq | 8/23/2022 6:35 AM | HLJKNSKOQ File | 212 KB |



PiMBc3Y.HLJkNskOq

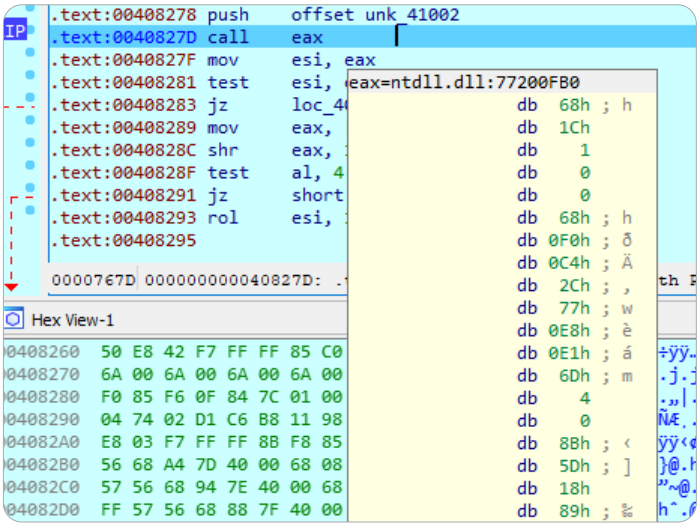
| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 02018D40 | 00 | B6 | CC | FF | 01 | 72 | 65 | 6C | 65 | 61 | 73 | 65 | 2F | 78 | 39 | 36 | .¶Ìÿ.release/x96 |
| 02018D50 | 64 | 62 | 67 | 2E | 65 | 78 | 65 | 0A | 00 | 20 | 00 | 00 | 00 | 00 | 00 | 01 | dbg.exe.. ..... |
| 02018D60 | 00 | 18 | 00 | 1B | 0F | F8 | BE | 17 | B4 | D8 | 01 | C4 | 37 | F8 | BE | 17 | .....ø¾.´Ø.Ä7ø¾. |
| 02018D70 | B4 | D8 | 01 | 54 | 95 | B8 | BE | 17 | B4 | D8 | 01 | 50 | 4B | 05 | 06 | 00 | ´Ø.T•¸¾.´Ø.PK... |
| 02018D80 | 00 | 00 | 00 | 09 | 01 | 09 | 01 | C9 | 74 | 00 | 00 | B2 | 18 | 01 | 02 | 00 | .....Ét..².... |
| 02018D90 | 00 | 51 | E2 | 4C | 9C | E2 | 2A | BE | 27 | B9 | B0 | 17 | 56 | 39 | 04 | C8 | .QâLœâ*¾'¹°.V9.È |
| 02018DA0 | F3 | 11 | 59 | 55 | 41 | A7 | D4 | 53 | 88 | 75 | 7C | AF | F4 | AB | 4C | D2 | ó.YUA§ÔS^u¦¯ô«LÒ |
| 02018DB0 | 77 | 02 | 59 | 34 | 60 | E3 | 12 | F4 | 7D | 29 | 65 | 0B | 45 | 79 | 8B | 7D | w.Y4`ã.ô})e.Ey‹} |
| 02018DC0 | CF | DA | BB | 27 | 70 | 05 | 70 | B8 | C4 | 98 | F8 | FF | 8F | CD | 5D | 21 | ÏÚ»'p.p¸Ä˜øÿ.Í]! |
| 02018DD0 | 19 | 55 | AA | 0D | 89 | D9 | 37 | FC | 84 | B1 | C8 | CE | FC | 4A | 5B | EC | .Uª.‰Ù7ü„±ÈÎüJ[ì |
| 02018DE0 | 16 | 62 | 2C | A9 | 2B | 89 | 82 | 04 | BA | C2 | 3C | A9 | DA | 47 | 75 | D3 | .b,©+‰‚.ºÂ<©ÚGuÓ |
| 02018DF0 | 6D | DE | 35 | FC | 56 | E9 | D8 | B4 | 55 | BA | C3 | D5 | F3 | 02 | F6 | CF | mÞ5üVéØ´UºÃÕó.öÏ |
| 02018E00 | DC | 03 | C7 | D1 | 73 | 37 | 87 | 6F | 13 | D7 | 83 | F5 | 90 | E1 | 86 | 85 | Ü.ÇÑs7‡o.×ƒõ.á†… |
| 02018E10 | CC | 97 | 81 | 00 | 29 | C6 | 3F | 0C | DD | D7 | DE | C5 | 5B | D2 | 05 | F5 | Ì—.).Æ?.Ý×ÞÅ[Ò.õ |
| 02018E20 | F9 | 75 | 03 | DB | 1A | 0C | 6E | 53 | FE | 45 | CF | 7D | 10 | BB | 7C | 96 | ùu.Û..nSþEÏ}.»\|– |
| 02018E30 | 1F | FC | 6B | 8A | 82 | 01 | 5F | 24 | 44 | 6A | 6D | 7F | D5 | 98 | A3 | E3 | .ükŠ‚._$Djm.Õ˜£ã |
| 02018E40 | 1B | CE | 78 | 3A | 21 | 47 | 66 | 0A | B1 | F3 | F4 | 85 | A2 | 69 | 37 | B1 | .Îx:!Gf.±óô…¢i7± |
| 02018E50 | 2B | 7C | 08 | 35 | F3 | 7A | 2B | 9C | 91 | B5 | D8 | 7D | 67 | 98 | E2 | 33 | +\|.5óz+œ'µØ}g˜â3 |
| 02018E60 | A8 | CB | 5E | EC | 36 | 7A | DD | 2F | 49 | 74 | 08 | CA | 7A | 8F | 5B | DB | ¨Ë^ì6zÝ/It.Êz.[Û |
| 02018E70 | D1 | F4 | 14 | 18 | A2 | 75 | 9B | DC | 67 | D2 | C5 | 26 | 04 | 39 | CD | 79 | Ñô..¢u›ÜgÒÅ&.9Íy |
| 02018E80 | 10 | 8E | 55 | 3E | A7 | D4 | 2E | 22 | 07 | DF | 87 | 88 | 19 | 9C | A0 | 14 | .ŽU>§Ô."..ß‡ˆ.œ . |
| 02018E90 | 99 | 87 | 44 | 89 | 5B | DA | AF | 5C | | | | | | | | | ™‡D‰[Ú¯\ |




Sobald die Ausführung abgeschlossen wurde, löscht sich LockBit selbst.

### Verschleierung

LockBit verwendet verschlüsselte Codefragmente, die nur beim Debugging zugänglich sind. Es verwendet eine Technik zur Verschleierung von Funktionsaufrufen, indem es diese in eines der Allzweckregister lädt.




Die Malware verfügt auch über Funktionen, um die Namen von WinAPI-Funktionen dynamisch auflösen zu können. Dadurch kann die eigentliche Importtabelle vor einer statischen Analyse verborgen werden.

### Lösegeldforderung

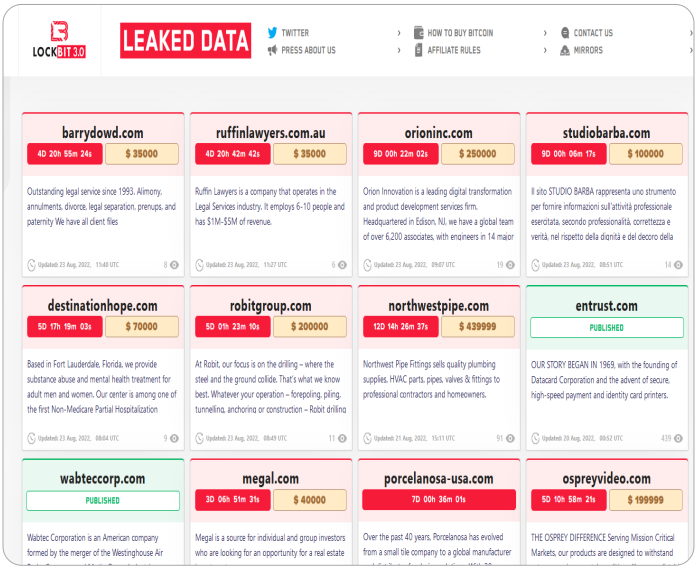
LockBit 3.0 hinterlegt in allen Ordnern, deren Inhalt verschlüsselt wurde, eine Lösegeldforderung mit der Bezeichnung 'HLJkNskOq.README.txt'. Diese Datei ist ziemlich lang und enthält die ID des Opfers sowie Links zur Datenleck-Website und zum entsprechenden Chat der Angreifer (sowohl für den Tor Browser als auch für normale Browser). Die Mitteilung informiert die Opfer darüber, was mit ihren Dateien geschehen wird, wenn sie das Lösegeld nicht zahlen, zur Polizei gehen oder anderweitig versuchen, ihre Dateien selbst wiederherzustellen.

### Datenleck-Website

Während die Datenleck-Seite geladen wird, wird folgender Text angezeigt:

> Does anyone know a good torrent tracker where I can upload greedy entrust.com com files? Please write to tox 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7

Auf der Datenleck-Seite befindet sich eine Zusammenstellung von Geschädigten. Jedes Opfer hat einen Timer und einen Preis, der an die Bedrohungsakteure gezahlt werden muss, damit seine Daten entschlüsselt (und ggf. nicht veröffentlicht) werden. Auf der Website werden auch Opfer aufgeführt, die kein Lösegeld gezahlt haben und deren Daten daraufhin veröffentlicht wurden.




### Zusammenfassung

Lockbit 3.0 (bzw. LockBit Black) verwendet jetzt einen Schlüssel, um seine Ausführung zu starten. Eine ähnliche Vorgehensweise findet man auch bei der Ransomware ALPHV, die dafür einen Zugriffstoken verwendet.

Die ersten Samples haben noch wenige Strings, Importe und Funktionen. Mehr als die Hälfte des Dateiinhalts wird stattdessen von einem '.text'-Abschnitt eingenommen. Dieser Abschnitt wird während der Laufzeit mit einem bereitgestellten Schlüssel in den auszuführenden Code decodiert. Der Abschnitt enthält zudem Funktionen, um WinAPI-Funktionsnamen mithilfe einer XOR-Chiffre dynamisch aufzulösen.

Während des Verschlüsselungsprozesses nimmt LockBit 3.0 außerdem Änderungen am Desktop-Hintergrund und der Windows-Registry vor. Bei allen verschlüsselten Dateien wird der Name, das Symbol und die Erweiterung geändert. Im Vergleich zu anderer Ransomware hat LockBit immer noch die schnellste Verschlüsselungsgeschwindigkeit. In den neuesten Samples kann sich diese sogar noch erhöhen, während sie gleichzeitig neue Funktionalitäten mitbringen. Es gibt derzeit kein offizielles universelles Entschlüsselungstool für LockBit 3.0. Aber das **RansomHunter Team bietet Hilfe** bei der Dechiffrierung der betroffenen Dateien an.

### Prestige: Eine neue Ransomware, die Transport- und Logistikunternehmen angreift

Am 14. Oktober 2022 hat das Microsoft Security Intelligence Team eine neue Ransomware gefunden, die es speziell auf Unternehmen aus dem Bereich Transport und Logistik in der Ukraine und Polen abgesehen hat. Diese Bedrohung wurde am 11. Oktober 2022 auf den Computern der Opfer aufgespielt und diente den Angreifern dazu, weitere schädliche Dateien auf den Systemen bereitzustellen. Wobei zwischen den Angriffen eine Verzögerung von einer Stunde eingehalten wurde. Der Name der Ransomware („Prestige“) wurde von der E-Mail-Adresse abgeleitet, die in der Lösegeldforderung angegeben wurde.

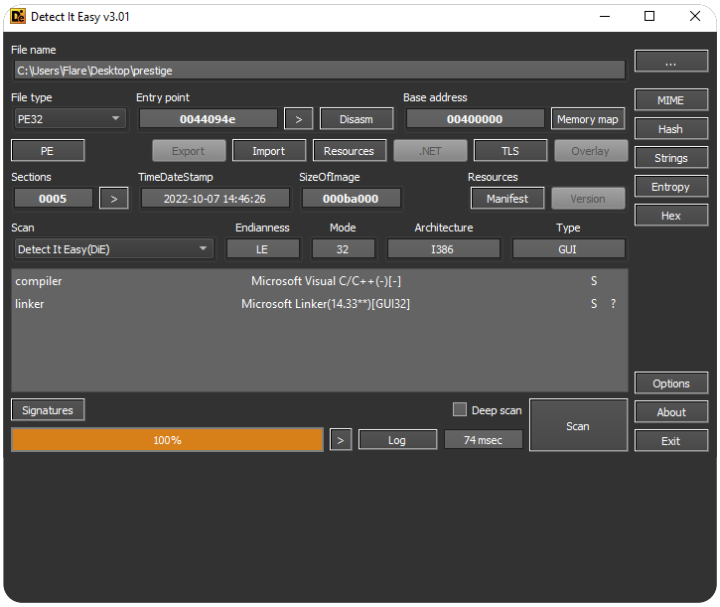
### Bereitstellung

Es wurden drei verschiedene Methoden beobachtet, wie Prestige auf Remote-Systemen bereitgestellt wird:

- Zuerst wird Zugriff auf die ADMIN$-Freigabe erlangt und dann schädliche Dateien dorthin kopiert. Anschließend wird mit dem Tool Impacket ein Aufgabenplanung erstellt, über die die Ransomware ausgeführt wird.
- Zuerst wird Zugriff auf die ADMIN$-Freigabe erlangt und dann schädliche Dateien dorthin kopiert. Anschließend wird mit dem Tool Impacket ein PowerShell-Skript geladen und ausgeführt, das wiederum die Ransomware ausführt.
- Die schädlichen Dateien werden auf den Active Directory Domain Controller kopiert und dann auf den Systemen bereitgestellt, die das Gruppenrichtlinienobjekt 'Standarddomäne' verwenden.

### Überblick

Prestige besteht aus einer PE32-Datei, die in der Programmiersprache C++ geschrieben ist. Der Zeitstempel der Kompilierung ist der 07.10.2022 (vier Tage vor den beobachteten Angriffen). Diese Datei ist weder gepackt noch verschlüsselt.




### Ausführung

Prestige prüft bei Ausführungsbeginn die CPU-Informationen mit der Anweisung 'cpuid' und der Funktion 'IsProcessorFeaturePresent' mit dem Argumentwert '10', der (falls gefunden) anzeigt, ob das System den SSE2-Befehlssatz unterstützt.

```
.text:0043FF9C          push    10              ; ProcessorFeature
.text:0043FF9E          call    ds:IsProcessorFeaturePresent
.text:0043FFA4          test    eax, eax
.text:0043FFA6          jz      loc_440158
.text:0043FFAC          and     [ebp+var_10], 0
.text:0043FFB0          xor     eax, eax
.text:0043FFB2          push    ebx
.text:0043FFB3          push    esi
.text:0043FFB4          push    edi
.text:0043FFB5          xor     ecx, ecx
.text:0043FFB7          lea     edi, [ebp+var_24]
.text:0043FFBA          push    ebx
text:0043FFBB           cpuid
```

Prestige verwendet viele SSE2-Anweisungen im Code, weshalb es diese Prozessor-Funktionalität benötigt, um korrekt arbeiten zu können.

```
.text:0045045B          movapd  xmm5, xmm0
.text:0045045F          unpcklpd xmm0, xmm0
.text:00450463          psrlq   xmm5, 34h
.text:00450468          pextrw  ecx, xmm5, 0
.text:0045046D          movapd  xmm1, ds:xmmword_474110
.text:00450475          movapd  xmm3, ds:xmmword_474170
.text:0045047D          movapd  xmm4, ds:xmmword_474120
.text:00450485          movapd  xmm6, ds:xmmword_474130
.text:0045048D          andpd   xmm0, xmm1
.text:00450491          orpd    xmm0, xmm3
.text:00450495          addpd   xmm4, xmm0
.text:00450499          pextrw  eax, xmm4, 0
.text:0045049E          and     eax, 7F0h
.text:004504A3          movapd  xmm4, ds:xmmword_476470[eax]
.text:004504AB          movapd  xmm7, ds:xmmword_476880[eax]
.text:004504B3          andpd   xmm6, xmm0
.text:004504B7          subpd   xmm0, xmm6
.text:004504BB          mulpd   xmm6, xmm4
.text:004504BF          subpd   xmm6, xmm3
.text:004504C3          addsd   xmm7, xmm6
.text:004504C7          mulpd   xmm0, xmm4
.text:004504CB          movapd  xmm4, xmm0
.text:004504CF          addpd   xmm0, xmm6
```

Ein Beispiel für die Verwendung von SSE2-Anweisungen in Prestige

Um starten zu können, benötigt die Ransomware Prestige administrative Berechtigungen. Sie beendet den Windows-Dienst MSSQL mit einem hartcodierten Befehl, an den 'MSSQLSERVER' angehängt wird:

```
.text:00405A8F          mov     [esp+38h+var_28], 0C0000000h
.text:00405A97          push    23h
.text:00405A99          push    offset aCWindowsSystem ; "C:\\Windows\\System32\\net.exe stop {}"
.text:00405A9E          mov     [eax+4], ecx
.text:00405AA1          lea     ecx, [esp+40h+CommandLine]
.text:00405AA5          mov     dword ptr [eax], 1
.text:00405AAB          call    sub_407B19
.text:00405AB0          add     esp, 10h
```

Um Systemwiederherstellungen nach der Verschlüsselung zu verhindern, werden Backup-Kataloge mit WBAdmin und alle Volumeschattenkopien mit VSSAdmin gelöscht.

```
aCWindowsSystem_2:                      ; DATA XREF: sub_411979+3B2↑o
                text "UTF-16LE", 'C:\Windows\System32\wbadmin.exe delete catalog -qui'
                text "UTF-16LE", 'et',0
                align 10h
aCWindowsSystem_3:                      ; DATA XREF: sub_411979+3F5↑o
                text "UTF-16LE", 'C:\Windows\System32\vssadmin.exe delete shadows /al'
                text "UTF-16LE", 'l /quiet',0
```

Für diese Befehle werden Tools verwendet, die sich im Ordner 'System32' befinden. Das Prestige-Sample selbst ist eine 32-Bit-Applikation. Sie deaktiviert Dateisystemumleitungen mit der Funktion 'Wow64DisableWow64FsRedirection'. Nach der Befehlsausführung wird die Funktion 'Wow64RevertWow64FsRedirection' aufgerufen, um die Dateisystemumleitungen wiederherzustellen.

```
.text:00431947                  call    edi ; CryptAcquireContextA
.text:00431949                  test    eax, eax
.text:0043194B                  jnz     short loc_43197A
.text:0043194D                  push    ebx
.text:0043194E                  call    ds:GetLastError
.text:00431954                  push    8               ; dwFlags
.text:00431956                  push    1               ; dwProvType
.text:00431958                  push    0               ; szProvider
.text:0043195A                  push    offset szContainer ; "Crypto++ RNG"
.text:0043195F                  push    esi             ; phProv
.text:00431960                  mov     ebx, eax
.text:00431962                  call    edi ; CryptAcquireContextA
.text:00431964                  test    eax, eax
.text:00431966                  jnz     short loc_431979
.text:00431968                  push    28h             ; dwFlags
.text:0043196A                  push    1               ; dwProvType
.text:0043196C                  push    eax             ; szProvider
.text:0043196D                  push    offset szContainer ; "Crypto++ RNG"
.text:00431972                  push    esi             ; phProv
.text:00431973                  call    edi ; CryptAcquireContextA
.text:00431975                  test    eax, eax
.text:00431977                  jz      short loc_43198C
```

Die Lösegeldforderung ist im Code hartcodiert und wird im Ordner 'C/Users/Public' als 'README'-Datei (ohne Erweiterung) abgelegt.

```
aPrestigeRanuso:                        ; DATA XREF: .rdata:off_49EF00↑o
                text "UTF-16LE", 'Prestige.ranusomeware@Proton.me',0
aYouPersonalFil:                        ; DATA XREF: sub_40226F+8E↑o
                text "UTF-16LE", 'YOU PERSONAL FILES HAVE BEEN ENCRYPTED.',0Dh,0Ah
                text "UTF-16LE", 0Dh,0Ah
                text "UTF-16LE", 'To decrypt all the data, you will need to purchase '
                text "UTF-16LE", 'our decryption software.',0Dh,0Ah
                text "UTF-16LE", 'Contact us {}. In the letter, type your ID = {:X}.',0Dh
                text "UTF-16LE", 0Ah
                text "UTF-16LE", 0Dh,0Ah
                text "UTF-16LE", '* ATTENTION *',0Dh,0Ah
                text "UTF-16LE", '- Do not try to decrypt your data using third party'
                text "UTF-16LE", ' software, it may cause permanent data loss.',0Dh,0Ah
                text "UTF-16LE", '- Do not modify or rename encrypted files. You will'
                text "UTF-16LE", ' lose them.',0Dh,0Ah,0
                align 10h
```

Sobald die Lösegeldforderung abgelegt wurde, werden zwei Änderungen in der Registry vorgenommen. Zuerst wird die neue Dateierweiterung ('.enc') der verschlüsselten Dateien registriert und danach die Lösegeldforderung in Notepad aufgerufen, wenn der betroffene Anwender eine verschlüsselte Datei öffnet.

```
aCWindowsSystem_0:                      ; DATA XREF: sub_4112A8+14↑o
                text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\.enc /ve /t RE'
                text "UTF-16LE", 'G_SZ /d enc /f',0
                align 10h
aCWindowsSystem_1:                      ; DATA XREF: sub_4112A8+34↑o
                text "UTF-16LE", 'C:\Windows\System32\reg.exe add HKCR\enc\shell\open'
                text "UTF-16LE", '\command /ve /t REG_SZ /d "C:\Windows\Notepad.exe C'
```

**Dateiverschlüsselung**

Bevor der Verschlüsselungsprozess gestartet wird, lädt Prestige eine Liste der Erweiterungen, die verschlüsselt werden sollen:

.1cd, .7z, .abk, .accdb, .accdc, .accde, .accdr, .alz, .apk, .apng, .arc, .asd, .asf, .asm, .asx, .avhd, .avi, .avif, .bac, .backup, .bak, .bak2, .bak3, .6h, .bkp, .bkup, .bkz, .bmp, .btr, .6z, .6z2, .bzip, .bzip2, .c, .cab, .cer, .cf, .cfu, .cpp, .crt, .css, .db, .db-wal, .db3, .dbf, .der, .dmg, .dmp, .doc, .docm, .docx, .dot, .dotm, .dotx, .dpx, .dsk, .dt, .dump, .dz, .ecf, .edb, .epf, .exb, .ged, .g1f, .gpg, .gzi, .gzip, .hdd, .img, .1so, .jar, .Java, .jpeg, .jpg, .js, .json, .kdb, .key, .1z, .1z4, .1zh, .1zma, .mdmr, .mkv, .mov, .mp3, .mp4, .mpeg, .myd, .nude, .nvram, .oab, .odf, .ods, .old, .ott, .ovf, .p12, .pac, .pdf, .pem, .pfl, .pfx, .php, .pkg, .png, .pot, .potm, .potx, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .pvm, .py, .qcow, .qcow2, .r0, .rar, .raw, .rz, .s7z, .sdb, .sdc, .sdd, .sdf, .sfx, .skey, .sldm, .s1dx, .sql, .sqlite, .svd, .svg, .tar, .taz, .tbz, .tbz2, .tg, .tib, .tiff, .trn, .txt, .txz, .tz, .vb, .vbox, .vbox-old, .vbox-prev, .vdi, .vdx, .vhd, .vhdx, .vmc, .vmdk, .vmem, .vmsd, .vmsn, .vmss, .vmx, .vmxf, .vsd, .vsdx, .vss, .vst, .vsx, .vtx, .wav, .wbk, .webp, .wmdb, .wmv, .xar, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .x1w, .xz, .z, .zbf, .zip, .zipx, .z1, .zpi, .zz

Prestige verwendet die kryptografische Bibliothek Crypto++, um Dateien per AES-Algorithmus zu verschlüsseln. Der öffentliche RSA-Schlüssel ist hartcodiert und für jedes Sample unterschiedlich.

```
.rdata:0049FDC8 aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
.rdata:0049FDC8                                 ; DATA XREF: sub_40221B+51o
.rdata:0049FDC8                 db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4mpkHWE1p0nefE0PL/Qk',0Ah
.rdata:0049FDC8                 db 'gT7bjLTeJ9bpH6v41L1YGI688cwfEnjmIaDa0zwvHfbT8dn4o+Wh2iSpUZk0BYIi',0Ah
.rdata:0049FDC8                 db 'Lw6u5+9nSd2UzD4sB+MY9dv6oVTHInxqp4VNLHR2nMjgIS4rFHYzNJ7Tsj/j3YJZ',0Ah
.rdata:0049FDC8                 db 'dVPuPVCqbpZg5boXoSFbgLNIn6Mnr+vKc5tGh+pkGty0otyFd/ghM0b/xitowcvx',0Ah
.rdata:0049FDC8                 db 'eqZezPO0YXmkjjeTi0jFa7E9IIP3Z/DMOR9r/oJR0NyEIs9HNKdFGTAjJKDAKWxu',0Ah
.rdata:0049FDC8                 db '1nEPXiZoPPHgS7fxqg40+ciCjj2i7eUwqVkop5Pvwjqtq Q0TkIt8EqjvkmDtMrp8',0Ah
.rdata:0049FDC8                 db 'ZQIDAQAB',0Ah
.rdata:0049FDC8                 db '-----END PUBLIC KEY-----',0Ah,0
```

Die Funktion 'CryptAcquireContextA' wird verwendet, um einen Handle auf den Schlüsselcontainer Crypto++ RNG (RandomNumberGenerator) zu erhalten.

```
.text:00431947                 call    edi ; CryptAcquireContextA
.text:00431949                 test    eax, eax
.text:0043194B                 jnz     short loc_43197A
.text:0043194D                 push    ebx
.text:0043194E                 call    ds:GetLastError
.text:00431954                 push    8               ; dwFlags
.text:00431956                 push    1               ; dwProvType
.text:00431958                 push    0               ; szProvider
.text:0043195A                 push    offset szContainer ; "Crypto++ RNG"
.text:0043195F                 push    esi             ; phProv
.text:00431960                 mov     ebx, eax
.text:00431962                 call    edi ; CryptAcquireContextA
.text:00431964                 test    eax, eax
.text:00431966                 jnz     short loc_431979
.text:00431968                 push    28h             ; dwFlags
.text:0043196A                 push    1               ; dwProvType
.text:0043196C                 push    eax             ; szProvider
.text:0043196D                 push    offset szContainer ; "Crypto++ RNG"
.text:00431972                 push    esi             ; phProv
.text:00431973                 call    edi ; CryptAcquireContextA
.text:00431975                 test    eax, eax
.text:00431977                 jz      short loc_43198C
```

Um die AES-Verschlüsselungen durchzuführen, prüft Prestige, ob die CPU die Befehlssätze AES-NI (AES New Instructions) und SSE2 unterstützt.

```
cmp     byte_4AFD92, 0
push    esi
jz      short loc_432405
mov     ecx, [esp+8+arg_0]
push    offset aAesni   ; "AESNI"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

```
cmp     byte_4AFD8D, 0
jz      short loc_43242E
mov     ecx, [esp+8+arg_0]
push    offset aSse2    ; "SSE2"
call    sub_405C0D
mov     eax, [esp+8+arg_0]
pop     esi
pop     ecx
retn    4
```

Wenn die CPU diese Anweisungen unterstützt, wird der Verschlüsselungsprozess gestartet. Die 'aesenc'-Anweisungen führen die erste Verschlüsselungsrunde durch, während die letzte Runde durch 'aesenclast' erfolgt.

```
sub     [esp+8+arg_4], 1
lea     edi, [edi+10h]
movups  xmm1, xmmword ptr [edi-10
movups  xmm0, xmmword ptr [ecx]
aesenc  xmm0, xmm1
movups  xmmword ptr [ecx], xmm0
movups  xmm0, xmmword ptr [edx]
aesenc  xmm0, xmm1
movups  xmmword ptr [edx], xmm0
movups  xmm0, xmmword ptr [esi]
aesenc  xmm0, xmm1
movups  xmmword ptr [esi], xmm0
movups  xmm0, xmmword ptr [eax]
aesenc  xmm0, xmm1
movups  xmmword ptr [eax], xmm0
jnz     short loc_43CF50
mov     edi, [esp+8+arg_14]
```

```
mov     eax, [esp+8+arg_10]
add     edi, edi
movups  xmm0, xmmword ptr [ecx]
movups  xmm1, xmmword ptr [eax+ec
mov     eax, [esp+8+arg_C]
aesenclast xmm0, xmm1
movups  xmmword ptr [ecx], xmm0
movups  xmm0, xmmword ptr [edx]
aesenclast xmm0, xmm1
movups  xmmword ptr [edx], xmm0
movups  xmm0, xmmword ptr [esi]
aesenclast xmm0, xmm1
movups  xmmword ptr [esi], xmm0
movups  xmm0, xmmword ptr [eax]
aesenclast xmm0, xmm1
pop     edi
movups  xmmword ptr [eax], xmm0
```

Für die Schlüsselgenerierung wird 'aeskeygenassist' verwendet und 'aesimc' für die inverse MixColumns-Transformation.

```
call    sub_441A20
movaps  xmm1, [esp+3Ch+var_10]
mov     edx, edi
shr     edx, 2
add     esp, 0Ch
aeskeygenassist xmm0, xmm1, 0
pextrd  ecx, xmm0, 3
xor     ecx, [esi]
lea     eax, [edx+7]
mov     [esp+30h+var_24], offset unk_46FCF
shl     eax, 4
xor     ecx, 1
add     eax, esi
mov     [esi+edx*4], ecx
mov     [esp+30h+var_20], eax
```

```
aesimc  xmm0, xmmword ptr [edx+ec
aesimc  xmm1, xmmword ptr [edx+ea
movups  xmmword ptr [edx+eax*4],
add     eax, 4
movups  xmmword ptr [edx+ecx*4],
sub     ecx, 4
cmp     eax, ecx
jb      short loc_43D0A0
```

Nachdem eine Datei verschlüsselt wurde, hängt Prestige die zusätzliche Endung '.enc' an die Dateierweiterung an. Die Endung 'enc' wird außerdem an alle verschlüsselten Dateien angehängt.

```
00000B80  1F EB AF BE 50 2A E0 64 3C 8A 89 D7 0D B2 A6 DE
00000B90  65 36 F4 77 65 7A 60 AE 13 7A 55 2A 44 45 A0 BA
00000BA0  E3 F6 06 44 1F 51 9D 96 95 DC 6A D0 00 B0 30 10
00000BB0  F2 61 76 85 3E 40 80 93 24 35 72 F8 DF DC F3 42
00000BC0  45 81 06 07 04 75 E9 45 29 3B F3 C3 15 56 08 F5
00000BD0  DC 63 AC FC E0 FC 90 66 AF 8B 8F C8 63 21 2A 7A
00000BE0  EE 08 1B 56 15 E3 26 8C 08 15 06 34 3D 22 13 C5
00000BF0  3C 67 31 A8 26 A7 72 85 21 0D BF 5F 29 82 68 17
00000C00  C0 51 29 DE BE E9 22 3A 98 C9 17 AE 3E 8A A0 4C
00000C10  50 3D 99 04 53 E7 8D 9E 59 F0 31 B7 86 EA B6 7C
00000C20  B9 05 49 14 D3 89 65 6E 63
```

### Lösegeldforderung

Die Lösegeldforderung 'README' wird im Ordner 'C/Users/Public' abgelegt und jedes Mal, wenn der Benutzer eine verschlüsselte Datei öffnet, in Notepad geöffnet. Diese Mitteilung enthält eine eindeutige Opfer-ID und eine E-Mail-Adresse, über das Opfer den Bedrohungsakteur kontaktieren kann.

README - Notepad

File Edit Format View Help

```
YOU PERSONAL FILES HAVE BEEN ENCRYPTED.

To decrypt all the data, you will need to purchase our decryption software.
Contact us Prestige.ranusomeware@Proton.me. In the letter, type your ID = 289B23AC.

* ATTENTION *
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Do not modify or rename encrypted files. You will lose them.
```

**Zusammenfassung**

Diese neue Ransomware namens Prestige richtete sich gezielt gegen Transport- und Logistikunternehmen. Sie könnte im Zusammenhang mit dem laufenden russisch-ukrainischen Konflikt stehen und auf eine Störung von Logistikoperationen abzielen. Die Opfer können mit dieser Ransomware auf mindestens drei Arten infiziert werden, wobei die ersten Angriffe mit einer Verzögerung von einer Stunde erfolgen. Tatsächlich zeigen alle Angriffe auf die Ukraine diese Ähnlichkeiten und wurden dabei die gleichen Sicherheitslücken und Schwachstellen ausgenutzt. Dieses Sample ist relativ primitiv und nicht abgesichert, aber dennoch gefährlich.

Alle oben beschriebenen Samples wurden von Acronis Cyber Protect erfolgreich erkannt und gestoppt. Dies unterstreicht erneut, wie wichtig eine moderne Cyber Protection-Lösung für Unternehmen ist.

# Gefährliche Websites

Im dritten Quartal 2022 haben durchschnittlich 7,7% aller Endpunkte versucht, auf schädliche URLs zuzugreifen. Gegenüber dem Vorquartal (mit dort 8,3%) entspricht dies einem leichten Rückgang.

Den größten Anteil an blockierten schädlichen URLs auf den Endpunkten gab es mit 20,5% im November 2022 in den USA. Darauf folgen Deutschland mit 9,0% und Italien mit 8,6%.

Schädliche URLs sind in E-Mails weit verbreitet. Aber man findet sie auch immer häufiger in anderen Kommunikationsmedien (wie den Chats von Slack oder Teams). Die Angreifer versuchen, die Links weiter zu personalisieren, damit sie nicht mehr für alle Anwender blockiert werden können, selbst wenn eine einzelne Instanz erfolgreich erkannt werden sollte. In Phishing-Mails enthalten schädliche Links oft die E-Mail-Adresse des Ziels als Argument. Auf diese Weise kann der Angreifer überprüfen, wer auf die Links geklickt hat. Und die Phishing-Seite kann sich dynamisch an den anvisierten Benutzer anpassen. So verwenden beispielsweise einige Phishing-Kits die Haupt-Domain der E-Mail-Adresse und laden deren Hauptseite als Hintergrund für die Phishing-Website, um so ein weiteres Ablenkungsmittel nutzen zu können.

| Monat | Prozentsatz der Anwender, die auf schädliche URLs geklickt haben |
|---|---|
| Januar | 8,5 |
| Februar | 8,1 |
| März | 9 |
| April | 8 |
| Mai | 8,1 |
| Juni | 8,8 |
| Juli | 8,1 |
| August | 8,5 |
| September | 6,6 |
| Oktober | 8,5 |
| November | 8,7 |

**Die 10 Länder mit den am meisten blockierten URLs im November 2022**

| Rang | Land | Prozentsatz an blockierten URLs im November 2022 |
|---|---|---|
| 1 | USA | 20,5 |
| 2 | Deutschland | 9 |
| 3 | Italien | 8,6 |
| 4 | Japan | 5,4 |
| 5 | Brasilien | 5,4 |
| 6 | Vereinigtes Königreich (UK) | 5,2 |
| 7 | Kolumbien | 4,3 |
| 8 | Frankreich | 3,4 |
| 9 | Kanada | 3,3 |
| 10 | Singapur | 2,8 |

Diese Zahlen wurden analog zu den Malware-Erkennungsstatistiken normalisiert – und zwar nach der Anzahl der aktiven Maschinen in jedem Land mit mindestens 25 blockierten URLs. Nachfolgend finden Sie die normalisierten Aufschlüsselungen nach Regionen aufgeschlüsselt.

## Die Top-10-Länder: normalisierte blockierte URLs nach Region

### Asien

| Rang | Land | Nach Regionen normalisierter Prozentsatz der blockierten URLs im November 2022 |
|---|---|---|
| 1 | Philippinen | 19 |
| 2 | Indien | 16,8 |
| 3 | Japan | 16,2 |
| 4 | Malaysia | 15,4 |
| 5 | Indonesien | 14,8 |
| 6 | China | 14,4 |
| 7 | Taiwan | 13,8 |
| 8 | Südkorea | 12,4 |
| 9 | Hong Kong | 12,1 |
| 10 | Singapur | 11,4 |

### EMEA

| Rang | Land | Nach Regionen normalisierter Prozentsatz der blockierten URLs im November 2022 |
|---|---|---|
| 1 | Kuwait | 33,6 |
| 2 | Saudi-Arabien | 18,7 |
| 3 | Slowakei | 16,7 |
| 4 | Bulgarien | 16,3 |
| 5 | Italien | 14,1 |
| 6 | Griechenland | 13,9 |
| 7 | Nord-Mazedonien | 13,7 |
| 8 | Königreich Jordanien | 13,3 |
| 9 | Portugal | 12,9 |
| 10 | Vereinigte Arab. Ermirate | 12,4 |

### Amerika

| Rang | Land | Nach Regionen normalisierter Prozentsatz der blockierten URLs im November 2022 |
|---|---|---|
| 1 | Haiti | 39,9 |
| 2 | Panama | 36,4 |
| 3 | Peru | 25,6 |
| 4 | Kolumbien | 23,6 |
| 5 | Costa Rica | 19 |
| 6 | Dominikanische Republik | 14,4 |
| 7 | Chile | 11,2 |
| 8 | Brasilien | 9,9 |
| 9 | USA | 8,1 |
| 10 | Mexiko | 7,9 |

# Schwachstellen in Windows-Betriebssystemen und Software

Wir bei Acronis werden nicht müde, Unternehmen und Privatanwender davor zu warnen, dass sowohl alte, ungepatchte als auch neue Zero Day-Schwachstellen die Hauptangriffsvektoren für die Kompromittierung von Computersystemen darstellen. Auch wenn die meisten Software-Hersteller versuchen, mit der Entwicklung Schritt zu halten und regelmäßig Sicherheitspatches zu veröffentlichen, reichen diese Bemühungen oft nicht aus.

Nehmen wir nur einen aktuellen Fall: Hier wurde ein kostenloser inoffizieller Patch für einen aktives Zero-Day-Exploit veröffentlicht, mit dem Dateien, die mit fehlerhaften Signaturen signiert wurden, die sogenannte MotW-Sicherheitswarnungen (Mark of the Web) in Windows 10 und Windows 11 umgehen können.

Wie bereits in unserem letzten Bericht erwähnt, fügt Microsoft allen Dateien, die aus dem Internet heruntergeladen werden, eine MotW-Kennzeichnung hinzu. Diese Kennzeichung (auch Flag genannt) veranlasst das Betriebssystem, eine Sicherheitswarnung anzuzeigen, wenn eine so gekennzeichnete Datei gestartet wird. Später haben Bedrohungsakteure bestimmte eigenständige JavaScript-Dateien eingesetzt, um die Ransomware Magniber auf den Geräten ihrer Opfer zu installieren. Dabei zeigte sich, dass Windows keine Sicherheitswarnungen ausgab, wenn diese JavaScript-Dateien gestartet wurden – obwohl sie eine MotW-Kennzeichnung hatten. Wie war das möglich? Es lag daran, dass diese JavaScript-Dateien digital mit einer manipulierten Signatur signiert wurden und Windows die Ausführung von signierten Dateien erlaubt.

Nachdem diese Zero-Day-Schwachstelle aktiv für Ransomware-Angriffe ausgenutzt wird, hat 0patch (ein Service des slowenischen Sicherheitsunternehmens Arcos Security) einen inoffiziellen Fix veröffentlicht, der verwendet werden kann, bis Microsoft ein offizielles Sicherheitsupdate veröffentlicht. In einem Blog-Beitrag hat Mitja Kolsek, ein Mitbegründer von 0patch, erklärt, dass dieser Fehler durch die Unfähigkeit der Windows-Sicherheitsfunktion SmartScreen verursacht wird, fehlerhafte Signaturen in Dateien zu analysieren. Am regulären Patch-Tag im November (zweiter Dienstag im Monat) hat Microsoft dann selbst ein offizielles Sicherheitsupdate veröffentlicht.

## Der Patch-Dienstag von Microsoft

Wie üblich hat Microsoft eine Menge zu tun, um seine populären Produkte zu patchen. Im Juli diesen Jahres hat das Unternehmen beispielsweise 84 Sicherheitsupdates veröffentlicht, von denen vier als kritisch eingestuft wurden. Wir haben die wichtigsten Verbesserungen nachfolgend zusammengestellt.

Die schwerwiegendste Schwachstelle, die behoben wurde, war eine Remote-Codeausführung (Remote Code Execution = RCE), in der Windows-Grafik-Komponente. CVE-2022-30221 erhielt eine CVSS-Einstufung von 8,8. Um diese Schwachstelle ausnutzen zu können, müsste ein Angreifer jedoch den Benutzer dazu bringen, sich mit einem schadhaften RDP-Server zu verbinden, was möglicherweise nicht so einfach ist.

Ebenfalls kritisch und mit einer CVSS-Einstufung von 8,1 war ein RCE-Schwachstelle im Netzwerk-Dateisystem mit der Bezeichnung CVE-2022-22029. Wie bei früheren RCE-Schwachstellen muss der Angreifer einen nicht authentifizierten, speziell präparierten Aufruf an einen NFS-Dienst erstellen, um die Remote-Codeausführung auszulösen.

Im August 2022 hat Microsoft 123 Sicherheitsupdates veröffentlicht, von denen 17 als kritisch eingestuft wurden. Bei drei der 17 kritischen Schwachstellen handelt es sich um Schwachstellen, die zu einer Rechteausweitung bei Microsoft Exchange führen können. Gerade für Exchange gab es in diesem Jahr regelmäßig Sicherheitsupdates, da immer mehr Sicherheitslücken entdeckt werden, die bei Cyberangriffen ausgenutzt werden. CVE-2022-24477, CVE-2022-24516 und CVE-2022-21980 haben alle eine CVSS-Einstufung von 8,0. Außerdem hat Microsoft darauf hingewiesen, dass Kunden, die von diesem Problem betroffen sind, nicht nur die neuesten Updates aufspielen sollten, sondern auch die Sicherheitsfunktion 'Erweiterter Schutz' (Extended Protection) aktivieren müssen, um derartige Angriffe zu verhindern.

Eine weitere kritische Schwachstelle betrifft ausschließlich Windows 11. Mit einer CVSS-Einstufung von 8,8 ist CVE-2022-35804 laut der offiziellen Sicherheitsempfehlung wahrscheinlich ausnutzbar. Aufgrund eines Problems im Microsoft SMBv3-Protokoll und der Art, wie dabei bestimmte Anfragen verarbeitet werden, können Angreifer über diese Schwachstelle Programmcode auf einem Zielsystem ausführen.

Im September gab es weniger Bugfixes: Insgesamt 63, wobei fünf davon als kritisch eingestuft wurden. Bei nur einer von diesen fünf Schwachstellen ist die Wahrscheinlichkeit hoch, dass sie aktiv ausgenutzt wird. CVE-2022-34718 ist eine RCE-Schwachstelle, die eine beeindruckende und bedrohliche CVSS-Einstufung von 9,8 erhalten hat. Unter Ausnutzung dieser Schwachstelle kann ein nicht authentifizierter Angreifer ein speziell präpariertes IPv6-Paket an einen Windows-Knoten senden, auf dem IPSec aktiviert ist. Dies könnte wiederum ermöglichen, auf der betreffenden Maschine eine manipulierte Remote-Codeausführung zu starten. Allerdings bedeutet dies auch, dass nur solche Systeme für diesen Angriff anfällig sind, auf denen der IPSec-Dienst läuft.

Zwei weitere der kritischen Schwachstellen, nämlich CVE-2022-34721 und CVE-2022-34722, ermöglichen eine Remote-Codeausführung im Windows IKEv1-Protokoll. Davon sind alle Windows Server betroffen, weil sie sowohl IKEv1- als auch IKEv2-Pakete akzeptieren. Mithilfe dieser Schwachstellen kann ein nicht authentifizierter Angreifer ein präpariertes IP-Paket an eine Windows-Zielmaschine senden, auf der IPSec aktiviert ist, wodurch eine Remote-Codeausführung auf der Maschine möglich wird.

Am Patch-Tag im Oktober gab es 89 Aktualisierungen, von denen 13 als kritisch eingestuft wurden. Das kritischste Problem wurde dieses Mal in einer populären SharePoint-Website behoben. CVE-2022-41038 erhielt eine CVSS-Einstufung von 8,8. Ein Angreifer muss sich sowohl an der Ziel-Website authentifizieren als auch die Berechtigung haben, um auf die Verwaltungsliste in Sharepoint zugreifen und diese verwenden zu können. Wenn diese Schwachstelle ausgenutzt wird, können Angreifer auf SharePoint-Servern eine Remote-Codeausführung durchführen.
Des Weiteren wurden drei weitere, weniger schwerwiegende Schwachstellen in SharePoint behoben. Bei CVE-2022-41037, CVE-2022-41036 und CVE-2022-38053 handelt es sich allesamt um RCE-Schwachstellen mit einer CVSS-Einstufung von 8,8.

Sieben der kritischen Schwachstellen wurden im Windows PPT-Protokoll (Point-to-Point Tunneling) behoben. Alle haben eine CVSS-Einstufung von 8,1 erhalten. Zur Ausnutzung der Schwachstelle müsste ein Angreifer ein präpariertes und schädliches PPTP-Paket an einen PPTP-Server senden. Im Erfolgsfall kann der Angreifer dann auf der Zielmaschine eine Remote-Codeausführung durchführen.

Die letzte große Schwachstelle (CVE-2022-37968) hat die maximale CVSS-Einstufung von 10 erhalten. Sie steckt in der Cluster-Connect-Funktion von Azure Arc-fähigen Kubernetes-Clustern. Weil es Anwendern mit der Azure Stack Edge-Funktionalität möglich ist, Kubernetes-Workloads über Azure Arc auf Geräten bereitzustellen, gelten auch Azure Stack Edge-Geräte als anfällig für die Schwachstelle.

Der Patch-Tag im November 2022 brachte insgesamt 68 Sicherheitsupdates – unter anderem für sechs Windows-Schwachstellen, die bereits aktiv ausgenutzt wurden. Darunter waren auch 11 kritische Sicherheitslücken, die Rechteausweitungen, Spoofing oder Remote-Codeausführungen ermöglichen. Nicht enthalten waren zwei am 2. November bekannt gewordene OpenSSL-Schwachstellen, auf die wir später noch eingehen werden.

Werfen wir einen Blick auf die kritischen Schwachstellen. CVE-2022-41128 – die „Sicherheitsanfälligkeit in Windows-Skriptsprachen bezüglich Remotecodeausführung“ erfordert, dass ein Anwender mit einer betroffenen Version von Windows auf einen schädlichen Server zugreift. Ein Angreifer müsste eine speziell präparierte Server-Freigabe oder Website hosten und dann einen Anwender dazu bringen, diese zu besuchen – wie etwa über eine manipulierende E-Mail oder Chat-Nachricht.

Die Schwachstelle „Sicherheitsanfälligkeit in Windows Mark of the Web bezüglich Umgehung von Sicherheitsfunktionen“ (CVE-2022-41091) wurde ebenfalls behoben. Über die Schwachstelle „Sicherheitsanfälligkeit im Windows-Druckerpooler bezüglich Rechteerweiterungen“ (CVE-2022-41073) können Angreifer Systemberechtigungen erlangen.

Die Schwachstelle „Sicherheitsanfälligkeit in Microsoft Exchange Server bezüglich Rechteerweiterungen“ (CVE-2022-41040) wurde im Rahmen der Zero Day-Initiative offengelegt. Wenn sie ausgenutzt wird, können Angreifer die PowerShell im Kontext des Systems ausführen.

Eine weitere Exchange-Schwachstelle (CVE-2022-41082) ermöglicht ebenfalls eine Remote-Codeausführung. Angreifer können als vermeintlich authentifizierte Benutzer versuchen, über einen Netzwerkaufruf schädlichen Code im Sicherheitskontext des Server-Kontos auszuführen.

# Die Patching-Aktivitäten von Google, Adobe und anderen

In der zweiten Jahreshälfte hat sich Google erwartungsgemäß auf Sicherheitsprobleme im Chrome-Browser konzentriert. Die Browser-Version 107.0.5304.87/88 brachte einen Bugfix für die siebte Zero-Day-Schwachstelle in diesem Jahr. Die vorherigen sechs wurden mit einem etwa monatlichen Abstand behoben, wobei die letzten drei im Juli (CVE-2022-2294), August (CVE-2022-2856) und September (CVE-2022-3075) erfolgten. Diese Schwachstellen wurden in einigen Fällen über mehrere Wochen von staatlich gesponserten Bedrohungsakteuren ausgenutzt, bevor sie von Google entdeckt und gepatcht wurden.

Bei der hochgradig gefährlichen Schwachstelle CVE-2022-3723, die mit der oben genannten Chrome-Version behoben wurde, handelt es sich um die Verwechslung eines Datentyps in der Javascript-Engine V8. Schwachstellen durch Datentypverwechslung können auftreten, wenn das betreffende Programm eine Ressource, ein Objekt oder eine Variable einem bestimmten Typ zuordnet und dann über einen anderen, inkompatiblen Typ auf diese zugreift. Dies kann dann zu unzulässigen Zugriffen auf den Arbeitsspeicher führen. Durch Zugriffe auf verbotene Speicherbereiche aus dem Sicherheitskontext der Applikation heraus könnte ein Angreifer sensible Informationen aus anderen Applikationen lesen, Abstürze verursachen oder beliebigen Programmcode ausführen.

Auch Adobe hatte in den betrachteten fünf Monaten eine Menge zu tun. Der jüngste Schwung von Sicherheitspatches enthielt Korrekturen für 29 dokumentierte Schwachstellen in mehreren Unternehmensprodukten. Diese Schwachstellen könnten Hacker ausnutzen, um die vollständige Kontrolle über anfällige Maschinen zu erlangen. Die Schwachstellen können sowohl Windows- als auch macOS-Anwender gefährden, weil sie die Ausführung von Programmcodes, beliebige Schreibzugriffe im Dateisystem, die Umgehung von Sicherheitsfunktionen und Rechteausweitungsangriffe ermöglichen. Laut einer als kritisch eingestuften Sicherheitsempfehlung von Adobe wurden insgesamt 13 Schwachstellen in ColdFusion behoben, darunter einige mit einer CVSS-Einstufung von 9,8/10.

Die Schwachstelle "Adobe Commerce und Magento Open Source" (CVE-2022-35698) wurde vom Hersteller als Cross-Site-Skripting-Bug („Stored XSS“) mit einer CVSS-Einstufung von 10,0 beschrieben.

Auch bei Adobe Dimension gab es Fehler, die mit dem höchsten Schweregrad eingestuft wurden. Das Unternehmen hat neun dokumentierte Bedrohungen adressiert und darauf hingewiesen, dass sowohl Windows- als auch macOS-Anwender dem Risiko von Codeausführungs- und Speicherleck-Angriffen ausgesetzt sein können.

Zuvor hatte Adobe schon Sicherheitspatches für 25 dokumentierte Schwachstellen veröffentlicht, durch die Benutzer für Angriffe gefährdet sind. Mit Updates für Acrobat und dem Adobe Reader wurden mehrere kritische und wichtige Schwachstellen behoben. Eine erfolgreiche Ausnutzung könnte zur Ausführung von beliebigen Programmcodes und Speicherlecks führen. Außerdem hat Adobe ein Sicherheitsbulletin mit Details zu vier Sicherheitslücken im Adobe Illustrator 2022 veröffentlicht.

Mit dem Sicherheitsupdate vom September hat Adobe ganze 63 Schwachstellen in sieben Produkten behoben. Alle diese Schwachstellen haben eine CVSS-Einstufung zwischen 5,3 und 7,8 erhalten – wobei 35 davon als kritisch bewertet wurden. Eine Ausnutzung könnte zu diversen Problemen führen – wie die Ausführung von beliebigen Programmcodes, die Umgehung von Sicherheitsfunktionen, beliebige Lesezugriffe im Dateisystem oder Speicherlecks.

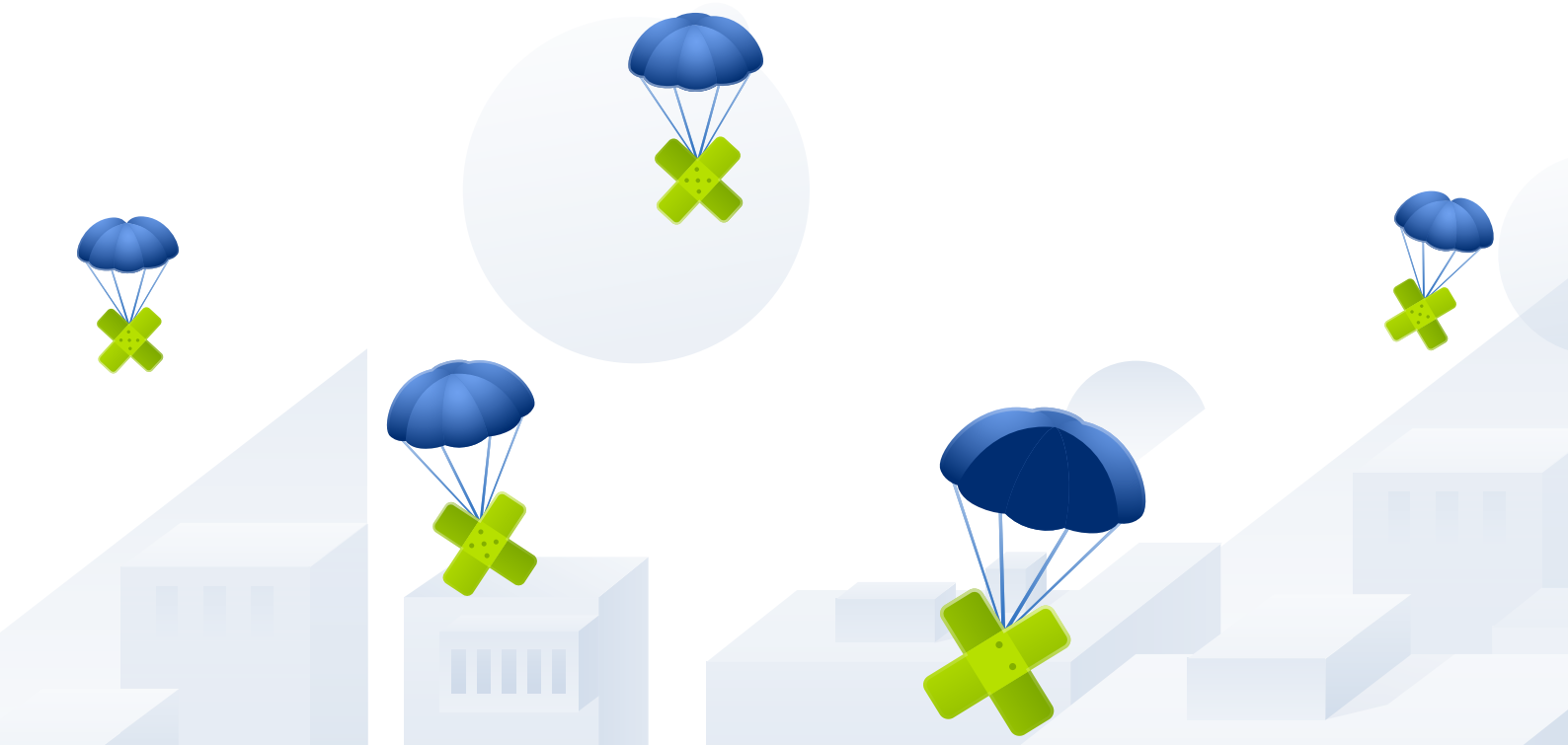
Der kritischste Fall (nämlich APSB22-49) betraf Adobe Bridge für Windows und macOS, wo 10 von 12 gepatchten Schwachstellen als kritisch eingestuft wurden. Auch Adobe InDesign (APSB22-50) für Windows und macOS war stark gefährdet, bevor 18 Schwachstellen (darunter 8 kritische) behoben wurden. Zu guter Letzt wurden zehn Schwachstellen in Adobe Photoshop 2021 und 2022 für Windows und macOS gepatcht (APSB22-52), von denen neun als kritisch eingestuft wurden.

Auch andere Hersteller haben wichtige Updates veröffentlicht. Das OpenSSL-Projekt hat zwei schwerwiegende Sicherheitslücken in seiner kryptografischen Open-Source-Bibliothek behoben, die zur Verschlüsselung von Kommunikationskanälen und HTTPS-Verbindungen verwendet wird. Von den Schwachstellen (CVE-2022-3602 und CVE-2022-3786) war die OpenSSL-Version 3.0.0 betroffen. Die Schwachstellen wurden mit OpenSSL 3.0.7 behoben.

CVE-2022-3602 ist ein beliebiger 4-Byte-Stack-Pufferüberlauf, der Abstürze auslösen oder zu einer Remote-Codeausführung (RCE) führen kann, während CVE-2022-3786 von Angreifern über schädliche E-Mail-Adressen ausgenutzt werden kann, um einen Denial-of-Service-Zustand per Pufferüberlauf auszulösen. OpenSSL hat zudem Abhilfemaßnahmen angegeben, die Administratoren von TLS-Servern auffordern, die TLS-Client-Authentifizierung solange zu deaktivieren, bis die Patches installiert sind.

In ähnlicher Weise hat Cisco seine Kunden gewarnt, dass zwei Schwachstellen im Cisco AnyConnect Secure Mobility Client für Windows im Umlauf sind und ausgenutzt werden. Über zwei Sicherheitslücken (CVE-2020-3433 und CVE-2020-3153) können lokale Angreifer DLL-Hijacking-Angriffe durchführen und Dateien mithilfe von Systemberechtigungen in Systemverzeichnisse kopieren. Durch eine erfolgreiche Ausnutzung können Angreifer auf den betroffenen Windows-Maschinen beliebigen Programmcode mit Systemberechtigungen ausführen. Für beide Schwachstellen sind Authentifizierungen erforderlich, für die die Angreifer im Besitz gültiger Anmeldedaten sein müssen.

Dies war nur eine kleine Auswahl von zahlreichen Schwachstellen, die in den letzten fünf Monaten entdeckt und behoben wurden. Wir wissen, dass Ransomware-Angreifer im betrachteten Zeitraum über 150 Schwachstellen ausgenutzt haben. Dies zeigt einmal mehr, wie wichtig Lösungen zur Schwachstellenbewertung und zeitnah bereitgestellte Patches sind, um Unternehmen und Privatanwender zuverlässig schützen zu können.



# Empfehlungen von Acronis, um in der aktuellen und zukünftigen Bedrohungsumgebung sicher zu bleiben

## Moderne Cyberangriffe, Datenlecks und Ransomware-Ausbrüche weisen alle auf das Gleiche hin: Cyber Security ist unzureichend. Dieses Versagen ist das kumulierte Ergebnis von schwachen Technologien und menschlichem Versagen, häufig verursacht durch clevere Social Engineering-Techniken.

Selbst wenn Ihre Backup-Lösung funktionieren und nicht kompromittiert sein sollte, dauert es nach einem Cybervorfall oft Stunden oder sogar Tage, bis die betroffenen Systeme (und dazugehörigen Daten) wieder in ein betriebsbereites Stadium versetzt sind. Ein Backup ist insbesondere unerlässlich, wenn Cyber Security-Lösungen versagen. Gleichzeitig können solche Tools aber auch kompromittiert oder deaktiviert werden – oder einfach nur (zu) langsam arbeiten. All das kann dazu führen, dass Unternehmen eine Menge Geld durch Ausfallzeiten verlieren.

Zur Lösung dieser Probleme empfehlen wir eine integrierte Cyber Protection-Lösung wie Acronis Cyber Protect. Denn dies kombiniert Antimalware-, Endpoint Detection & Response (EDR)-, Data Loss Prevention (DLP)- und Email Security-Technologien sowie Schwachstellenbewertungs-, Patch-Verwaltungs-, Remote Monitoring & Management (RMM)- und Backup-Fähigkeiten in einem einzigen Agenten, der auf allen gängigen Windows-Betriebssystemen läuft. Diese Integration gewährleistet eine optimale Performance, beseitigt Kompatibilitätsprobleme und ermöglicht schnelle Wiederherstellungen: Sollte eine Bedrohung einmal übersehen oder erst entdeckt werden, wenn Ihre Daten schon manipuliert wurden, so werden diese Daten umgehend aus einem Backup wiederhergestellt. Dank dieses einzelnen Agenten weiß die Lösung, wann Daten verloren gegangen sind und wiederhergestellt werden müssen.

Mit einer eigenständigen Antimalware-Lösung, die einen eigenen Agenten verwendet, der nicht mit Ihrer Backup-Lösung verknüpft ist, wäre dies nicht möglich. Andere Cyber Security-Produkte können eine Bedrohung zwar stoppen. Aber sie können keine Daten wiederherstellen, die dennoch verloren gegangen sind. Und ein separater Backup-Agent weiß nicht automatisch über Gefährdungssituationen Bescheid. Daher werden betroffene Daten bei einem Angriff möglicherweise nur langsam oder gar nicht wiederhergestellt.

Natürlich ist auch Acronis Cyber Protect bestrebt, die Wiederherstellung von solchen Daten überflüssig zu machen, weil es Bedrohungen erkennen und beseitigen kann, bevor diese Ihre Umgebung schädigen können. Dies wird durch unsere fortschrittliche und mehrschichtige Cyber Security-Technologie gewährleistet.

Aber auch, wenn eine moderne Lösung wie Acronis Cyber Protect zum Einsatz kommt, sollten Unternehmen und Privatanwender die grundlegenden Sicherheitsregeln nicht außer Acht lassen.

**Patchen Sie Ihr Betriebssystem und Ihre Applikationen**

Dies ist besonders wichtig, da viele Angriffe aufgrund ungepatchter Schwachstellen erfolgreich sind. Eine Lösung mit integrierten Funktionen zur Schwachstellenbewertung und Patch-Verwaltung, wie sie in Acronis Cyber Protect enthalten sind, kann Ihnen dabei helfen. Wir erfassen alle entdeckten Schwachstellen und veröffentlichten Patches, die relevant sind, sodass Administratoren oder technische Mitarbeiter alle Endpunkte mit einer flexiblen Konfiguration und ausführlichen Berichten einfach patchen können. Acronis Cyber Protect unterstützt nicht nur alle integrierten Windows-Applikationen, sondern auch 300 beliebte Drittanbieter-Anwendungen (einschließlich Kommunikationstools wie Zoom und Slack) sowie gängige VPN-Clients, die im Rahmen von Remote-Arbeiten verwendet werden. Schließen Sie zuerst alle Schwachstellen mit höchstem Schweregrad und überprüfen Sie anhand des Erfolgsberichts, ob die entsprechenden Patches ordnungsgemäß aufgespielt wurden.

Wenn Sie weder Acronis Cyber Protect noch eine andere Software zur Patch-Verwaltung haben, wird diese Aufgabe deutlich schwieriger. Sie sollten zumindest aber immer dafür sorgen, dass Windows alle benötigten Updates erhält und diese zeitnah installiert werden. Benutzer neigen dazu, Systemmeldungen zu ignorieren, insbesondere wenn Windows zu einem Neustart auffordert. Dies kann ein großer Fehler sein. Vergewissern Sie sich auch bei Ihren Anwendungen von populären Software-Herstellern (wie Adobe), dass bei diesen die automatische Update-Funktion aktiviert ist, damit beliebte Anwendungen (wie der Adobe Reader) ebenfalls regelmäßig aktualisiert werden.

**Bereiten Sie sich auf Phishing-Versuche vor und klicken Sie nicht auf verdächtige Links**

Betrügerisch gestaltete Phishing- und andere schädliche Websites erscheinen täglich in großer Zahl. Diese werden zwar manchmal auch über den Browser herausgefiltert, aber moderne Cyber Protection-Lösungen wie Acronis Cyber Protect bieten hier dedizierte Funktionalitäten zur URL-Filterung. Schädliche Links gibt es überall – z.B. in Instant Messenger-Applikationen, E-Mails, Forenbeiträgen usw. Klicken Sie niemals auf Links, die Sie nicht benötigen oder deren Empfang Sie nicht erwartet haben.

Schädliche Inhalte können auch per E-Mail über betrügerisch gestaltete Anhänge zugestellt werden. Sie sollten möglichst immer überprüfen, woher Nachrichten mit Anhängen wirklich stammen, und sich fragen, ob Sie diese erwartet haben oder nicht. In jedem Fall sollten Sie einen Anhang, den Sie öffnen wollen, zuvor von einer Antimalware-Lösung scannen lassen.

**Verwenden Sie ein VPN bei der Arbeit mit Geschäftsdaten**

Egal, ob Sie eine Remote-Verbindung zu Unternehmens-ressourcen/-diensten herstellen müssen, im Internet surfen oder Telekommunikationstools verwenden wollen: Verwenden Sie möglichst immer ein VPN (Virtual Private Network). VPNs können Ihren gesamten Datenverkehr verschlüsseln und ihn so vor Angreifern schützen, die Ihre Daten während der Übertragung abfangen wollen.

Wenn Sie in Ihrem Unternehmen eine VPN-Lösung haben, erhalten Sie die entsprechenden Anweisungen dafür höchstwahrscheinlich von Ihrem Administrator oder MSP-Techniker. Wenn Sie Ihren Arbeitsplatz selbst absichern müssen, verwenden Sie renommierte, empfehlenswerte VPN-Apps/-Dienste, die auf Software-Marktplätzen oder direkt von den jeweiligen Anbietern erhältlich sind.

**Sorgen Sie dafür, dass Ihre Cyber Security-Lösung einwandfrei funktioniert**

Acronis Cyber Protect verwendet viele aufeinander abgestimmte Sicherheitstechnologien, darunter mehrere Detection Engines zur Erkennung von Schadprogrammen. Wir empfehlen, diese Lösung zu verwenden, statt auf die integrierten Sicherheitstools von Windows oder macOS zurückzugreifen.

Aber es reicht nicht aus, einen Malware-Schutz nur zu haben - er muss auch richtig konfiguriert werden.

Das bedeutet:

- Mindestens einmal pro Tag sollte ein vollständiger Scan durchgeführt werden.
- Das Produkt sollte häufig nach Updates suchen und diese abrufen – täglich oder idealerweise stündlich.
- Ein entsprechendes Produkt sollte mit seinen Cloud-Erkennungsmechanismen verbunden sein. Bei Acronis Cyber Protect ist dies die Acronis Cloud Brain. Diese Funktion ist standardmäßig aktiviert, aber Sie müssen sicherstellen, dass ein Internetverbindung besteht und diese nicht versehentlich für Antimalware-Software blockiert wird.
- Die On-Demand- und On-Access-Scan-Funktionen sollten aktiviert sein und auf jede neu installierte oder ausgeführte Programme reagieren.

Sie sollten die Meldungen Ihrer Antimalware-Lösung nicht ignorieren, sondern diese aufmerksam lesen. Und wenn Sie eine kostenpflichtige Sicherheitssoftware verwenden, sollten Sie sich vergewissern, dass die Lizenz gültig ist.

### Behalten Sie Ihre Kennwörter und Ihren Arbeitsbereich für sich

Sicherheitstipp Nr. 1: stellen Sie sicher, dass Ihre Kennwörter – und die Kennwörter Ihrer Mitarbeiter – sicher und geheim sind. Sie sollten Ihre Kennwörter mit niemandem teilen.

Verwenden Sie für jeden Service unterschiedliche und ausreichend lange Kennwörter. Eine Passwort Manager kann Ihnen helfen, sich diese zu merken. Eine bewährte Methode, ein starkes Kennwort zu erstellen, besteht darin, sich eine lange Phrase auszudenken, die Sie sich leicht merken können. Kennwörter mit acht Zeichen (oder weniger) sind heutzutage leicht durch Brute Force-Techniken zu knacken. Verwenden Sie möglichst eine Multi-Faktor-Authentifizierung als zusätzliche Sicherheitsebene.

Vergessen Sie nicht, Ihren Laptop/Desktop-PC wegzuschließen und den Zugriff darauf zu beschränken. Das gilt auch, wenn Sie von zu Hause aus arbeiten. Sensible Dateien können auf nicht gesperrten Systemen leicht von anderen Personen eingesehen, gestohlen oder (auch versehentlich) gelöscht werden.

# Die Cyber Security-Trends und Vorhersagen von Acronis für 2023

Die heutige Welt ist mehr denn je von der Digitalisierung abhängig. IT-Umgebungen werden immer komplexer, und kleine Schwächen bei der Resilienz können große Auswirkungen auf die Fähigkeit eines Unternehmens haben, nach einem Sicherheitsvorfall oder einer Datenschutzverletzung weiterzuarbeiten.

# Hier sind zehn Trends, die die Cyber Security-Landschaft im Jahr 2023 wahrscheinlich prägen werden:

**1. Authentifizierungs- und Identitätsmanagementsysteme stehen im Fadenkreuz**

Lösungen zur Authentifizierung und Verwaltung von Identitäts- und Zugriffsrechten (Identity Access Management, IAM) werden immer häufiger erfolgreich angegriffen. Viele Angreifer haben bereits damit begonnen, MFA-Tokens (Multi-Faktor-Authentifizierung) zu stehlen oder zu umgehen. In manchen Situationen kann eine Überflutung der Ziele mit MFA-Anfragen zu erfolgreichen Anmeldungen führen, ohne dass eine Schwachstelle vorliegt. Kürzlich erfolgte Angriffe auf Okta und Twilio haben gezeigt, dass auch solche externen Services angegriffen werden können. Dazu kommt natürlich noch das jahrelange Problem, dass Benutzer Kennwörter einsetzen, die zu schwach sind oder gar für mehrere Anwendungen eingesetzt werden. Umso wichtiger ist es, sicherzustellen, dass die MFA-Lösung korrekt konfiguriert ist und dass alle Mitarbeiter des Unternehmens die erforderlichen Mindestzugriffsrechte erhalten.

**2. Ransomware wird noch mehr Schaden anrichten**

Die Ransomware-Bedrohung ist nach wie vor stark und entwickelt sich ständig weiter. Während wir einerseits eine Verlagerung zu mehr Datenexfiltrationen beobachten, professionalisieren die Hauptakteure ihre Operationen weiter.

Die meisten Hauptakteure haben ihre Aktivitäten inzwischen auf macOS und Linux ausgeweitet und nehmen auch die Cloud-Umgebung ins Visier. Neue Programmiersprachen (wie Go und Rust) werden häufiger eingesetzt und erfordern eine Anpassung der Analysetools.

Die Anzahl der Angriffe wird weiter zunehmen, solange sie profitabel bleiben. Dies gilt insbesondere dann, wenn Cyberversicherungen einen Teil der Auswirkungen abdecken. Dies wird zweifellos die Cyberversicherungsbeiträge weiter in die Höhe treiben. Angreifer werden sich verstärkt darauf konzentrieren, wo immer möglich Sicherheitstools zu deinstallieren, Backups zu löschen und Disaster Recovery-Pläne zu deaktivieren. Sogenannte LOLBAS-Angriffstechniken (Living off the Land) werden dabei eine wichtige Rolle spielen.

**3. Datenschutzverletzungen für die breite Masse**

Malware, die Informationen stiehlt (wie Raccoon und RedLine), wird zur Norm bei Infektionen. Solche gestohlenen Daten enthalten oft Anmeldedaten, die dann über sogenannte Initial Access Broker (IABs) verkauft werden, um zukünftige Angriffe zu erleichtern. Die zunehmende Anzahl von Daten-Blobs in Kombination mit der Komplexität von vernetzten Cloud-Diensten wird es für Unternehmen schwieriger machen, den Überblick über ihre Daten zu behalten. Die Anforderung, dass oft mehrere Parteien auf die Daten zugreifen müssen, erschwert es, diese zu verschlüsseln und zu schützen. Ein beispielsweise auf GitHub oder über eine mobile App geleakter API-Zugriffsschlüssel kann ausreichen, um alle Daten zu stehlen. Dies wird aber auch zu Fortschritten beim datenschutzfreundlichen Computing führen.

**4. Phishing wird sich über E-Mails hinaus ausweiten**

Schädliche E-Mails und Phishing-Angriffe werden weiterhin millionenfach verschickt werden. Die Angreifer werden auch weiterhin versuchen, ihre Angriffe mithilfe von zuvor unrechtmäßig ermittelten Daten zu automatisieren und zu personalisieren. Social Engineering-Betrugsmaschen (wie BEC-Angriffe) werden sich zunehmend auf andere Messaging-Dienste (wie SMS, Slack, Teams-Chats usw.) ausweiten, um Filter- und Erkennungstechniken zu umgehen. Phishing hingegen wird weiterhin auf Proxys zurückgreifen, um Sitzungs-Token abzufangen, MFA-Token zu stehlen und Umleitungen wie QR-Codes zu nutzen, um sich weiter zu tarnen.

**5. Not-so-Smart Contracts**

Bei den Angriffen auf Cryptowährungsbörsen und Smart Contracts auf diversen Blockchains ist vorerst kein Ende in Sicht. Sogar nationalstaatliche Angreifer haben versucht, digitale Währungen im Wert von Hunderten von Millionen zu stehlen. Die ausgeklügelten Angriffe auf Smart Contracts, algorithmische Coins und DeFi-Lösungen gehen weiter – neben den klassischen Phishing- und Malware-Angriffen auf ihre Nutzer.

**6. Living off Your Infrastructure**

Auch Service Provider werden zunehmend angegriffen und kompromittiert. Die Angreifer missbrauchen dabei bereits installierte Tools (wie PSA-, RMM- oder andere Deployment-Tools). Man spricht auch von LotL-Angriffen für „Living of the Land“ (etwa für „von dem leben, was das Land bereitstellt“). Gemeint ist damit, zur Tarnung der Angriffe die Standard-Ressourcen zu verwenden, die in der jeweiligen Umgebung vorhanden sind. Dies bedroht nicht nur Managed IT Service Provider, sondern auch Beratungsunternehmen, First-Level-Support-Anbieter und ähnlich angebundene Partner. Ausgelagerte Insider sind oft als schwächstes Glied in einem Unternehmen eingebunden, sodass hier keine aufwendigen Angriffe auf die Software-Lieferkette erforderlich sind.

**7. Aufrufe aus dem Browser heraus**

Es wird mehr Angriffe im oder durch den Browser geben, wobei die Angriffe aus den Sitzungen heraus durchgeführt werden. So können etwa schädliche Browser-Erweiterungen im Hintergrund die Zieladressen von Cryptowährungs-transaktionen austauschen oder Kennwörter stehlen. Es gibt auch den Trend, die Quellcodes solcher Tools zu kapern und Hintertüren über das GitHub-Repository hinzuzufügen. Andererseits werden auch Websites weiterhin Benutzer mit JavaScript tracken und Sitzungs-IDs über HTTP-Referrer an Marketing-Services weiterreichen. Die Angreifer werden sogenannte Formjacking/Magecart-Techniken ausbauen, bei denen kleine hinzugefügte Snippets alle Informationen im Hintergrund der ursprünglichen Website stehlen. Mit zunehmender Verbreitung von serverlosem Computing kann die Analyse solcher Angriffe schwieriger werden.

**8. Cloud-Automatisierung über APIs**

Es hat bereits eine enorme Auslagerung von Daten, Prozessen und Infrastrukturen in die Cloud stattgefunden. Mit der zunehmenden Automatisierung zwischen den verschiedenen Diensten wird sich dies noch weiter fortsetzen. Viele IoT-Geräte werden Teil dieser großen, hypervernetzten „Cloud of Services“ sein. Dies wird aber wohl auch zur Folge haben, dass viele APIs über das Internet zugänglich sein werden, was wiederum das Risiko für umfangreiche automatisierte Angriffe erhöht.

**9. Angriffe auf Geschäftsprozesse**

Angreifer kommen immer wieder auf neue Ideen, wie sie Geschäftsprozesse zu ihrem Vorteil/Profit manipulieren können. So können sie beispielsweise die Details eines Empfängerkontos in der Rechnungssystemvorlage eines Unternehmens ändern oder ihr Cloud Storage-Bucket als Backup-Ziel für den E-Mail-Server einrichten. Bei solchen Angriffen wird oft keine Malware eingesetzt, sondern (ähnlich wie bei der wachsenden Zahl von Insider-Angriffen) das Anwenderverhalten genau analysiert.

**10. KI in allen Bereichen**

KI- und ML-Prozesse werden von Unternehmen aller Größen und aus allen Branchen genutzt. Die Fortschritte bei der Erstellung synthetischer Daten werden Identitätsbetrügereien und Desinformationskampagnen mit gefälschten Inhalten weiter befeuern. Noch alarmierender ist der Trend, dass Angriffe auf die KI- und ML-Modelle selbst erfolgen können. Die Angreifer könnten versuchen, Schwachstellen im Modell auszunutzen, absichtlich Verzerrungen in Datensätze einzupflanzen oder einfach die Auslöser zu nutzen, um IT-Operationen mit Alarmmeldungen zu überfluten.

# Über Acronis

Acronis vereint die Bereiche Data Protection und Cyber Security in seinen integrierten, automatisierten Cyber Protection-Lösungen, die die Herausforderungen der modernen digitalen Welt in Bezug auf Verlässlichkeit (Safety), Verfügbarkeit (Accessibility), Vertraulichkeit (Privacy), Authentizität (Authenticity) und Sicherheit (Security) – kurz „SAPAS“ genannt – erfüllen. Im Rahmen flexibler Bereitstellungsmodelle, die allen Anforderungen von Service Providern und IT-Experten gerecht werden, bietet Acronis herausragende, KI-basierte Cyber Protection-Lösungen – mit innovativen Antivirus-, Backup-, Disaster Recovery- und Endpoint Protection Management-Fähigkeiten der nächsten Generation – für alle marktüblichen Daten, Applikationen und Systeme. Unterstützt durch seine Blockchain-basierten Datenauthentifizierungs- und fortschrittlichen, mit modernster Maschinenintelligenz arbeitenden Antimalware-Technologien kann Acronis bei niedrigen und kalkulierbaren Kosten alle gängigen Umgebungen schützen – von Cloud- über Hybrid- bis zu reinen On-Premise-Infrastrukturen.

Acronis, 2003 in Singapur gegründet und seit 2008 mit einem Hauptsitz in der Schweiz ansässig, beschäftigt heute mehr als 2.000 Mitarbeiter und ist weltweit an 34 Standorten vertreten. Seinen Lösungen vertrauen weltweit mehr als 5,5 Millionen Privatanwender und 500.000 Unternehmen – wozu auch hochrangige Profisportteams gehören. Die Produkte von Acronis können über 50.000 Partner und Service Provider in über 150 Ländern und in 26 Sprachen bezogen werden.

Acronis

Weitere Informationen erhalten Sie unter
www.acronis.com