Cybersicherheit: Im Herzen der Ransomware-Industrie

WHITEPAPER

STORMSHIELD

Ransomware-Angriffe häufen sich und bedrohen das wirtschaftliche Gleichgewicht und den Fortbestand vieler Unternehmen und Organisationen. Es vergeht keine Woche, in der nicht ein Unternehmen oder eine Behörde von einem solchen Angriff betroffen ist und eine damit verbundene Lösegeldforderung erhält.

Innerhalb von 30 Jahren hat sich dieses Phänomen von einem bösartigen Programm auf einer Diskette, dass hundert Dollar verlangt, zu einer strukturierten kriminellen Industrie entwickelt, die jährlich mehrere Millionen Dollar erpresst. Welches sind die aktuellen Vorgehensweisen von Ransomware-Gruppen? Wie werden sie von Cyberkriminellen in Unternehmen eingesetzt? Störung oder gar Einstellung des Geschäftsbetriebs, Offenlegung von Daten – welche Druckmittel setzen sie ein? Und vor allem: Wie kann man sich davor schützen?

Dieses Whitepaper befasst sich erneut mit der Entwicklung von Ransomware und den Akteuren, die sie zu einer bedeutenden Bedrohung machen. Es entschlüsselt die Funktionsweise dieser Malware und stellt gute Praktiken zur Abwehr der Folgen vor. Ohne die zentrale Frage zu verschweigen, die sich durch viele, mit dem Problem konfrontierte Strukturen zieht: Zahlen oder nicht zahlen, soll man nachgeben?

01.

Von der Erpressung Einzelner bis zum *Big Game Hunting*: Ransomware von gestern bis heute

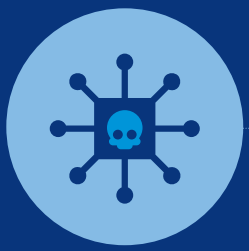
Ransomware ist das meist diskutierte Werkzeug von Cyberkriminellen und kann die Abläufe jedes Unternehmens oder jeder Behörde stören, unabhängig von ihrer Größe und ihrem Sicherheitsniveau. Wie hat sich diese Bedrohung in den letzten dreißig Jahren verändert? Rückblick auf ein sich ständig veränderndes Phänomen.

Die Entwicklung von Ransomware von den Anfängen bis heute

1989-2006

URSPRÜNGE „VOR DEM INTERNET“

AIDS-TROJANER, PGPCODER



2007-2013

EINE VERBREITUNG „ÜBER DAS NETZ“

WINLOCK

2013-2016

DIE ERSTEN TECHNOLOGISCHEN REVOLUTIONEN

CRYPTOLOCKER, SYPENG

2019-2021

DAS ZEITALTER DES BIG GAME HUNTING

MAZE

2017-2018

VON DEN ERSTEN WELTWEITEN STAATLICHEN ANGRIFFEN

WANNACRY, NOTPETYA.

2021-2022

AUF DEM WEG ZUR STRUKTURIERUNG VON CYBERCRIME

RANSOMWARE-AS-A-SERVICE

1.1
Von den Ursprüngen „vor dem Internet“ (1989 bis 2006)

1989

Die allererste Ransomware taucht in den späten 1980er Jahren auf. Diese Malware hat nur eine Aufgabe: den Betrieb des Arbeitsplatzes im Unternehmen und bei (wenigen) Privatpersonen mit Mikrocomputern zu blockieren.

Lösegeldforderungen sind damals jedoch aufgrund der Zahlungsinformationen relativ leicht zu verfolgen. Erst 15 Jahre später, mit dem Aufkommen der digitalen Währungen, wird die Ransomware zu einem Massenphänomen. PGPCoder, die „20-Dollar-Ransomware“, ist eine der ersten über das Internet verbreiteten Ransomware, die 2005 über die häufigsten Dateierweiterungen wie .rar, .zip, .jpg, .doc ou .xls. mit der Infizierung von Windows-Systemen beginnt. –

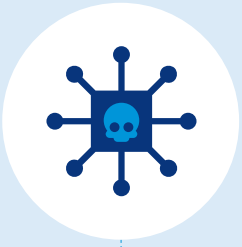
STICHTAG

Die allererste Ransomware, der „AIDS-Trojaner“, wird 1989 per Diskette verbreitet. Er verschlüsselt die Dateien der von ihm infizierten Rechner nach einer bestimmten Anzahl von Neustarts und die Opfer werden aufgefordert, ein Lösegeld von 189 $ zu zahlen, damit ihre Daten wiederhergestellt werden.

2007-2013

Eine Verbreitung über das „Netz“

1.2
Eine Verbreitung „über das Netz“ (2007-2013)



Scareware

Mit der Verbreitung von Instant-Messaging-Diensten, sozialen Netzwerken, Foren oder auch *Peer-to-Peer* kann sich Ransomware über neue Kanäle verbreiten. WinLock hat z. B. die Besonderheit, die Daten auf dem infizierten Computer nicht zu verschlüsseln. Der Zugriff auf den Rechner wird blockiert, indem ein Fenster mit einem pornografischen Foto und einer Zahlungsaufforderung über einen Premium-SMS-Dienst angezeigt wird.

Diese erste Entwicklung in der Funktionsweise von Ransomware wird als „Locker" bezeichnet, um ihr Ziel widerzuspiegeln: den Start des Betriebssystems zu blockieren.

Zur gleichen Zeit tauchen Varianten auf, die das Image von Strafverfolgungsbehörden annehmen, wie die Reveton-Ransomware im Jahr 2012. Verbreitet auf den *Peer-to-Peer*-Plattformen oder Pornoseiten gibt es sich als FBI aus, sperrt die Computer seiner Opfer und verlangt die Zahlung einer „Geldstrafe" von 200 $.

In der Folge werden die Lösegeldforderungen immer kreativer, um die Erfolgschancen zu erhöhen. –

STICHWORT

Scareware: Erpressungsmethode mit gefälschten Antivirenprogrammen, die in den 2010er-Jahren sehr beliebt war.

2013-2016

Die ersten technologischen Revolutionen

1.3 Die ersten technologischen Revolutionen (2013-2016)

Die Ransomware CryptoLocker markiert 2013 einen technologischen Wendepunkt mit ihrem Command & Control-Server, der es ermöglicht, mit dem Opfer zu chatten und noch mehr Druck auszuüben. Es handelt sich zudem um eine der ersten Ransomwares, die ein Lösegeld in Bitcoin verlangte.

Denn Kryptowährungen markieren eine neue Schlüsselphase in der Entwicklung der Ransomware. Mit ihnen – und insbesondere mit dem Aufkommen von Bitcoin – ist die Lösegeldforderung durch die Anonymisierung der Geldempfänger nicht mehr nachvollziehbar. Parallel dazu führt Ransomware wie Sypeng 2014 über gefälschte Update-Nachrichten der Adobe-Flash-Software die ersten Angriffe auf Android-Tablets und -Mobiltelefone durch. Im Jahr 2016 beginnt mit Petya die Ära der Phishing-Angriffe. Petya zielt auf geschäftliche E-Mail-Adressen ab und versteckt sich in einem Word- oder PDF-Dokument. –

27 Mio. $

KENNZAHL

Dies ist der Betrag, den CryptoLocker in den ersten beiden Monaten seines Betriebs erwirtschaftet hat.

2017-2018

Erste weltweite staatliche Angriffe

1.4 Erste weltweite staatliche Angriffe (2017-2018)

Dank der Veröffentlichung von Zero-Day-Schwachstellen, die von einer US-Regierungsbehörde entwendet wurden, verfügen Ransomware-Angriffe nun über die technischen Möglichkeiten, sich massiv von einem Unternehmen zum anderen zu verbreiten, sobald Netzwerke nebeneinander existieren.

WannaCry wird 2017 gestartet und löst eine große Medienberichterstattung aus. In nur wenigen Wochen befällt sie 300.000 Computer in 150 Ländern, indem sie sich über die Sicherheitslücke EternalBlue auf Microsoft Windows-Betriebssystemen ausbreitet.

Einige Monate später werden einige der grundlegenden Elemente von WannaCry (EternalBlue-Exploit, Seitenverschiebung) von der Ransomware NotPetya im Zusammenhang mit dem staatlichen Konflikt zwischen Russland und der Ukraine wiederverwendet. Diese Ransomware verschleiert auch die Sabotageversuche an der ukrainischen U-Bahn,[1], dem Flughafen von Kiew, dem Kernkraftwerk Tschernobyl[2], der Zentralbank und den nationalen Energieversorgern.

Auch heute noch nutzen Akteure wie der chinesische Konzern Bronze Starlight Ransomware-Kampagnen, um Spionageoperationen zu verschleiern.

Im Jahr 2018 entdeckt die Cybersicherheitswelt dann die Ransomware Ryuk, die es besonders auf große Unternehmen abgesehen hat. Und das verheißt nichts Gutes für die Zukunft ... –

„Die Ransomware war nur eine Fassade. Das eigentliche Ziel von NotPetya war nicht die Erpressung von Geld, sondern die Zerstörung von Daten, und zwar in sehr großem Maßstab, indem ein ganzes Land ins Visier genommen wurde.“

PIERRE-OLIVIER KAPLAN – CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

2019-2021

das Zeitalter des Big Game Hunting

1.5
Das Zeitalter des Big Game Hunting (2019-2021)

Leakware

Die Zahl der Vorfälle mit Ransomware stieg bis Ende 2019 um 365 %. Um nicht Gefahr zu laufen, von Sicherheitstools entdeckt zu werden, wenden sich Cyberkriminelle von groß angelegten Kampagnen wie WannaCry ab und **konzentrieren sich auf große Unternehmen**.

Diese Vorgehensweise, die auf der Erkundung der Umgebung und der Entwicklung fortgeschrittener Angriffsszenarien beruht, wird als Big Game Hunting (Großwildjagd) bezeichnet. Diese neue Strategie zahlt sich aus, da sich der durchschnittliche Betrag der Lösegeldforderung in diesem Zeitraum verdreifacht hat, von 13.000 auf 36.000 $[3].

Der Mechanismus der doppelten Erpressung taucht ebenfalls in dieser Zeit auf. Das Opferunternehmen erhält nicht nur eine Lösegeldforderung, sondern ihm wird auch mit dem Weiterverkauf seiner Daten im Darknet gedroht. Wenn diese Erpressung nicht ausreicht, um die Unwilligsten zur Zahlung des Lösegelds zu bewegen, geben die Cyberkriminellen einen Teil der entwendeten kritischen Daten (Quellcode, Kundendaten) preis. Einige Banden gehen sogar so weit, dass sie den Endkunden oder Patienten dieser Unternehmen damit drohen, ihre persönlichen Daten preiszugeben: das ist die dreifache Erpressung.

Dazu gehört auch die Gruppe von Cyberkriminellen, die mutmaßlich die Ransomware Maze erstellt hat. Ihre Besonderheit? Eine ständige Kommunikation mit seinen Opfern, um konstanten Druck auszuüben.

Im Jahr 2020 erweitert der Angriff von Darkside auf den US-amerikanischen Transport- und Vertriebsriesen für Ölprodukte, Colonial Pipeline, die Jagdliste des *Big Game Hunting*. Die Ransomware, die technisch gesehen REvil ähnelt, erpresst im Handumdrehen ein Lösegeld in Höhe von 5 Millionen US-Dollar. –

„Wenn der durch die Verschlüsselung erzeugte Druck nicht ausreicht, gehen Ransomware-Gruppen zur Erpressung über und drohen damit, die exfiltrierten Daten offenzulegen. Und wenn das nicht reicht, greifen sie auch auf DDoS-ähnliche Angriffe zurück, um ihre Opfer zur Zahlung zu zwingen.“

ÉDOUARD SIMPÈRE – LEITER CYBER THREAT INTELLIGENCE, STORMSHIELD

STICHWORT

Modul zum Datendiebstahl, das in der neuesten Ransomware enthalten ist.

HINWEIS

Immer mehr Druck. Die ALPHV/BlackCat-Gruppe veröffentlicht gestohlene Daten auf ihrer .onion-Website, aber auch auf einer herkömmlichen Website, deren Domainname den Namen des angegriffenen Unternehmens enthält. Sie ist leicht durchsuchbar und sieht sogar eine Suchfunktion vor, damit Kunden selbst überprüfen können, ob ihre Daten betroffen sind.

2012-2022

Auf dem Weg zur Strukturierung der cyberkriminellen Branche

1.6
Auf dem Weg zur Strukturierung von Cybercrime (2021-2022)

Die jüngste Revolution in der Vorgehensweise von Cyberkriminellen ist das Aufkommen von Ransomware-as-a-Service-Plattformen (RaaS). Weniger erfahrene Angreifergruppen finden hier White-Label-Ransomware für schlüsselfertige Kampagnen. Gegen einen bestimmten Prozentsatz des erbeuteten Lösegelds erhalten sie die komplette Infrastruktur für eine Malware, die von anderen Cyberkriminellen entwickelt wurde. Es handelt sich also um eine gut strukturierte Branche, in der jeder seine klar definierte Rolle hat.

2021 tauchen die Initial Acces Brokers (IABs) auf. Als Spezialisten für das Eindringen verschaffen bzw. verkaufen sie anderen bösartigen Gruppen Zugang zu Unternehmensnetzwerken, den diese dann für ihre eigenen Angriffe nutzen.

Diese zunehmende Raffinesse der Angriffskette lässt sich durch die Verbesserung des Schutzniveaus der Unternehmen erklären. Leider führt die Industrialisierung von Ransomware auch zu einer Verkürzung der Einsatzzeiten[5]. Im März 2022 schickte eine Gruppe iranischer Cyberkrimineller[6] ihre Lösegeldforderung an den lokalen Drucker einer US-Behörde, ohne die Daten zuvor verschlüsselt zu haben. –

STICHTAG

Zwei Tage lang versammelte das Weiße Haus Dutzende von Ländern, darunter Frankreich oder auch Deutschland, zu einem Gipfeltreffen, um Lösungen für das weltweite Problem der Ransomware zu finden. Reicht das aus, um das Thema endlich in Angriff zu nehmen?

Oktober 2022

KENNZAHL

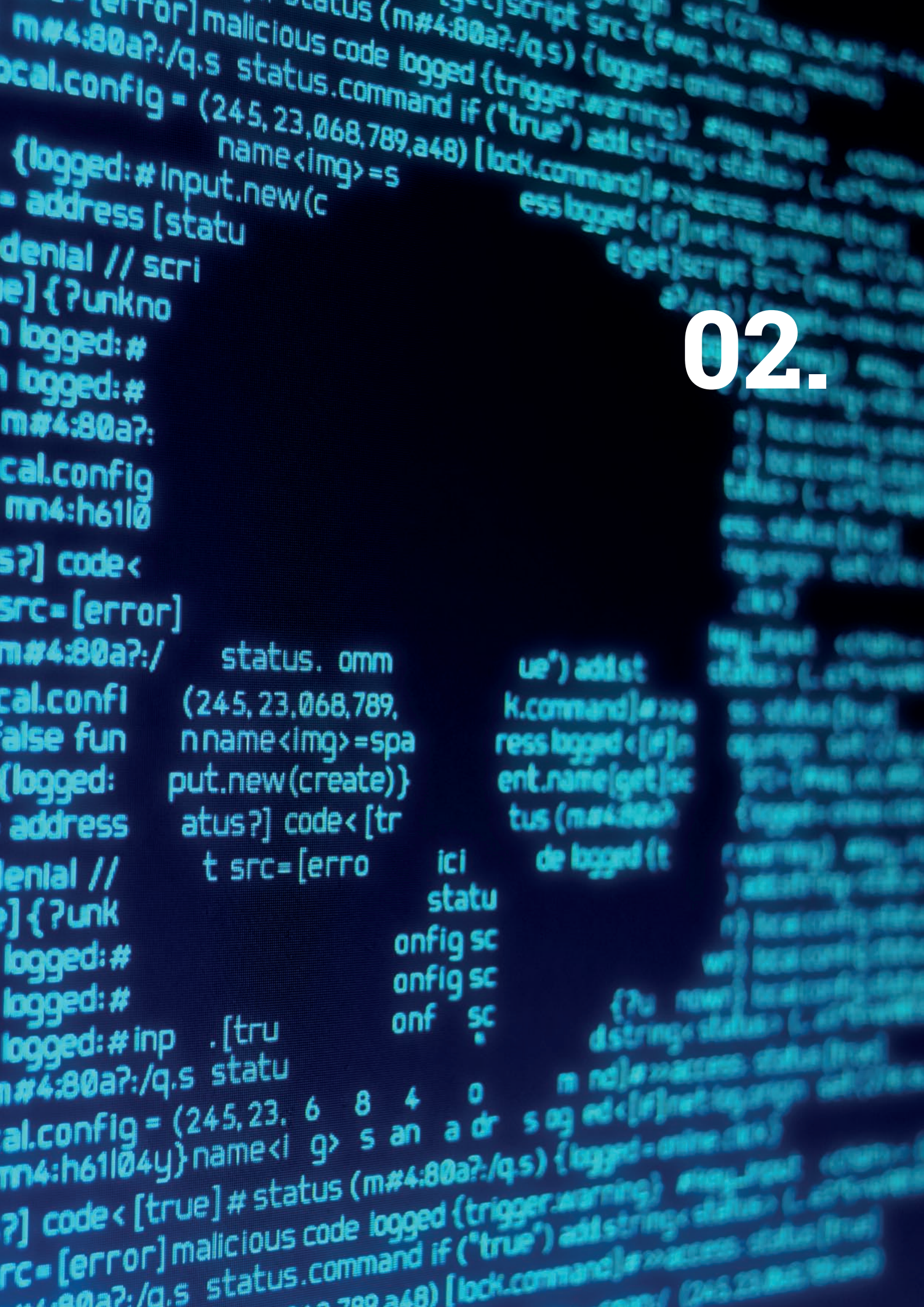
X2

Weltweit haben sich die Ransomware-Angriffe im Jahr 2021 verdoppelt[4].

WEITERFÜHRENDE INFORMATIONEN

KURZE GESCHICHTE DER RANSOMWARE

Die „kleine" Geschichte der Ransomware finden Sie ausführlicher in unserem Artikel zu diesem Thema[7].


02.

Preis und Schaden: Was sind die Folgen eines Ransomware-Angriffs?

Ein Angriff mit Ransomware bleibt selten ohne Folgen für die Opfer. Abgesehen von den finanziellen Verlusten wird die gesamte Wertschöpfungskette von Organisationen destabilisiert. Beschäftigen wir uns mit den Hintergründen eines Angriffs, seinen Preis und den Schäden.

2.1 Wer profitiert von Ransomware-Angriffen?

In den letzten drei Jahrzehnten hat sich die Welt der Ransomware gut aufgestellt. Banden von Cyberkriminellen kommen und gehen, aber ihre größeren Fähigkeiten sind nicht mehr zu übersehen.

Die Ransomware-Gruppen lassen sich in verschiedene „Familien“ einteilen, die über die ganze Welt verteilt sind. Von den 100 Familien oder Varianten, die das FBI[8] aufgespürt hat, stammen viele von in Asien und Osteuropa ansässigen Gruppen. In Frankreich sind etwa 30 Ransomware-Gruppen aktiv, die unter den berüchtigten Namen LockBit, Conti, ALPHV/BlackCat oder Hive bekannt sind.

Häufig mit geopolitischen Ereignissen verbunden, tauchen Gruppen von Cyberkriminellen immer schneller auf und verschwinden wieder. Nachdem die Conti-Gruppe ihre Unterstützung für Russland angekündigt hatte, erlebte sie eine wahre Serie von Datenlecks: Interne Chat-Protokolle, Quellcodes und andere von der Gruppe verwendete Dateien wurden veröffentlicht. Die Gruppe schloss ihre Website 2022[9]; was für eine Gruppe, die erst 2020 entdeckt wurde, sehr schnell war … Sie könnte jedoch in anderer Form wieder auftauchen, wie die Lebenszeichen ihres Ablegers Karakurt im Juni[10] andeuteten. Dies erinnert an das Beispiel der Gruppe REvil, die zwar im Januar 2022 aufgelöst wurde, aber einige Monate später wieder von sich hören ließ[11].

Zusammenfassend lässt sich sagen, dass sich die Malware-Industrie gut aufgestellt hat und mit ihr eine regelrechte Schattenwirtschaft der Cyberbedrohung mit verschiedenen Berufsgruppen entsteht. Die Entwicklung des Marktes für Cyberangriffe ist so groß, dass *„man heute zweifellos von einer Schattenwirtschaft sprechen kann,“* erklärt Sébastien Viou, Direktor für Cybersicherheitsprodukte und Cyberexperte bei Stormshield. –

„Wir haben es jetzt mit einer organisierten Cyberkriminalität mit ihren Verkaufsforen zu tun, in denen verschiedene Profile zusammenkommen: diejenigen, die die Schwachstellen finden, diejenigen, die in die Systeme eindringen, diejenigen, die die Malware entwickeln usw. Über diese Kanäle werden auch Bediener rekrutiert, die in die Systeme eindringen.“

NICOLAS CAPRONI – HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

WICHTIGE DATEN

JUNIORPROFILE

Die Ransomware-Franchise Conti bildet „Junior“-Profile aus und bietet ihnen ein festes Gehalt sowie eine Erfolgsbeteiligung.

ÜBERBLICK ÜBER RANSOMWARE-GRUPPEN

Der Mitbegründer von Hackers sans Frontières, Clément Domingo, hat etwas mehr als die Hälfte aller Cyberkriminellen-Gruppen auf der Welt erfasst.

- → ALPHV
- → Ako
- → Arvin Club
- → Astro Team
- → AtomSilo
- → Avaddon
- → AvosLocker
- → Babuk
- → Babuk Locker
- → Bl4ckt0r
- → Black Shadow
- → BlackByte
- → Bonaci Group
- → CRYP70N1C0D3
- → Clop
- → Conti
- → Cuba
- → DarkLeaks
- → DarkSide
- → DoppelPaymer
- → Dotadmin
- → Egregor
- → Entropy
- → Everest
- → Exorcist
- → Grief
- → HARON
- → Hive
- → LV
- → LockBit
- → LockBit 2.0
- → LockData Auction
- → Lorenz
- → Maze
- → Medusa Locker
- → Midas
- → Mount Locker
- → Nefilim
- → Nemty
- → NetWalker
- → Night Sky
- → Pay2Key
- → payload.bin
- → Prometeus
- → Pysa (Mespinoza)
- → Qlocker
- → Quantum
- → REvil (Sodinokibi)
- → Ragnar Locker
- → Ramp
- → Ransom Cartel
- → RansomEXX
- → Ranzy Locker
- → Rook
- → Sekmet
- → Snatch
- → SunCrypt
- → Suncrypt
- → Vice Society
- → Xing

NEUE EXPERTISEN ... AUF BEIDEN SEITEN!

INTERVIEW **FLORENT CURTET**
- EHEMALIGER HACKER, DER SICH AUF DIE BETREUUNG VON CYBERKRISEN VERLEGT HAT, BILDET POLIZEIKRÄFTE, ANWALTSKANZLEIEN ODER AUCH DATENSCHUTZBEAUFTRAGTE IN DIESER NEUEN KUNST DES VERHANDELNS AUS

→ Die Akteure von Ransomware spezialisieren sich: Entwicklung, Updates, Austausch mit den Opfern, virtuelle Geldwäsche – in Zeiten von RaaS und Affiliate Marketing hat jeder seine Rolle. Auch auf der Sicherheitsseite entstehen neue Kompetenzen, wie der untypische Werdegang von Florent Curtet, Leiter von NeoCyber und Mitbegründer von Hackers sans Frontières, zeigt.

Was war Ihr größter Erfolg beim Verhandeln?

F. C. – Mit meinen Methoden konnte ich die Höhe des Lösegelds drastisch senken, z. B. von 1 Million auf 100.000 €. Es ist mir schon passiert, dass ich Cyberkriminelle davon überzeugt habe, in dem sehr speziellen medizinischen Kontext auf ihre Beute zu verzichten.

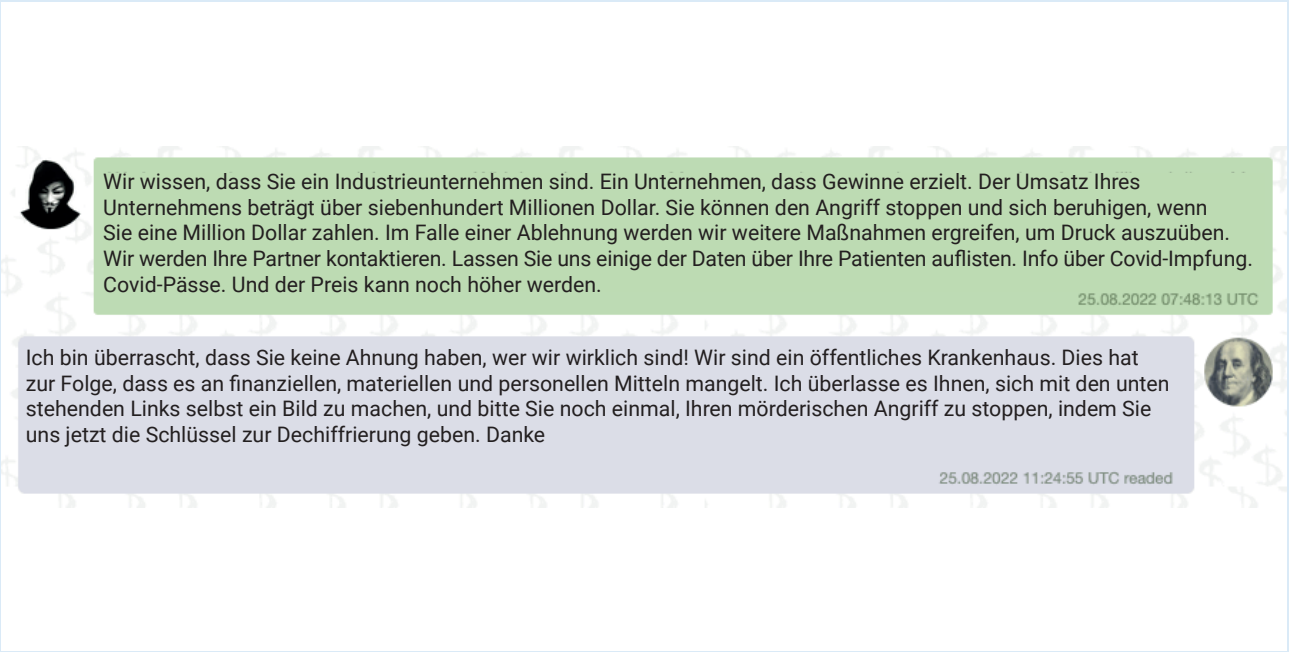
Welche Methoden waren das?

F. C. – In einem ersten Schritt geht es um die Kommunikationsmittel. In der Regel nehmen Cyberkriminelle per E-Mail Kontakt mit ihren Opfern auf. Mein Ziel war es, die Konversation auf den Echtzeit-Messenger Tox zu verlagern, um die Beziehung besser betreuen zu können. Das beschäftigt sie, um Zeit zu gewinnen, zeigt ihnen, dass wir da sind, und beginnt, in ihr Gehirn einzudringen.

Wie sieht das Profil der Cyberkriminellen aus, mit denen Sie verhandeln?

F. C. – Auch wenn sie oft von erfahreneren Personen betreut werden, handelt es sich in der Regel immer noch um eher junge und leicht zu beeinflussende Personen.

„Es scheint auf beiden Seiten Aufklärungsbedarf zu geben.“



LEGENDE

Im Fall des Angriffs auf das CHSF scheint der Cyberkriminelle davon überzeugt zu sein, dass er es mit einem Wirtschaftsunternehmen zu tun hat.[14]

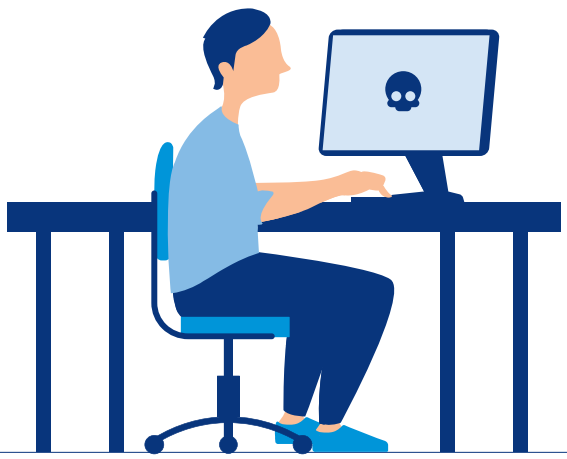
Die Rolle des Unterhändlers kann problematisch erscheinen, insbesondere vor dem Hintergrund, dass die ANSSI dringend davon abrät, bei einem Ransomware-Angriff Lösegeld zu zahlen. Warum haben Sie sich dafür entschieden, diese Expertise zu entwickeln?

F. C. – Es schien mir, dass es auf beiden Seiten einen Bedarf an Aufklärung gab. In der Vergangenheit bestanden Verhandlungen im Cyberspace vor allem darin, dem Opferunternehmen zu erklären, was Bitcoins, das Tor-Netzwerk usw. sind. In Gesprächen mit Cyberkriminellen musste ich manchmal den Unterschied zwischen Umsatz und Gewinn erklären oder die Geschäftstätigkeit des Unternehmens neu einordnen.
Tatsächlich können wir uns schnell in einer Grauzone wiederfinden, weshalb es wichtig ist, diese Aufgabe einzugrenzen, um Abweichungen zu vermeiden. Dennoch scheinen mir Verhandlungen eine pragmatische Antwort in einem Kontext zu sein, in dem einige kleine Betriebe dreifach bestraft werden: ihre Aktivitäten werden blockiert, ihre Daten offengelegt oder sie könnten sogar eine Geldstrafe durch die CNIL auferlegt bekommen, wenn sie die DSGVO nicht einhalten. –

„Wir können uns schnell in einer Grauzone wiederfinden, daher ist es wichtig, diese Aktivität zu betreuen, um Auswüchse zu vermeiden.“

2.2 Wer sind die Opfer?

Ransomware hat ihre Fähigkeit unter Beweis gestellt, jedes Unternehmen und jede Behörde zu stören, unabhängig von ihrer Größe und ihrem Sicherheitsniveau. Aber gibt es bestimmte Profile oder Sektoren, die besonders als Zielscheibe gewählt werden? Einige Antworten.



Das gesamte globale Wirtschaftsgefüge ist von der Bedrohung durch Ransomware betroffen, vom Kleinstunternehmen bis zum internationalen Großkonzern. In Europa ist jedes zweite Unternehmen, das Opfer von Ransomware wird, ein Kleinstunternehmen[15]. In Frankreich hat eines von drei kleinen und mittleren Unternehmen bereits einen derartigen Angriff erlitten[16]. Dies ist jedoch nur die Spitze des Eisbergs: Wie viele nicht gemeldete Ransomware gibt es für eine einzige gemeldete Ransomware?

Und alle Sektoren sind betroffen.
Auch wenn das Volumen der Angriffe zu bestimmten Zeiten geringer ist, sind sie insgesamt gezielter und konzentrieren sich auf bestimmte Branchen, insbesondere auf die Fertigungs-, Tech- und Finanzindustrie[17].

Wenn sie nicht direkt ins Visier genommen werden, können Unternehmen auch Kollateralschäden durch Ransomware-Angriffe auf ihre Dienstleister erleiden. –

11 Mio. $[18]

„Niemand ist vor Cyberkriminellen sicher, die betreiben sowohl Schleppnetzangriffe (Massenangriffe auf wenig geschützte Strukturen, um deren Tätigkeit zu unterbrechen) als auch Speerfischangriffe (gezielte Aktionen, um das Markenimage oder das industrielle Know-how von besser geschützten Akteuren anzugreifen).“

FLORENT CURTET – LEITER VON NEOCYBER UND MITBEGRÜNDER VON HACKERS SANS FRONTIÈRES

KENNZAHL

Diese Summe zahlte der brasilianische Lebensmittelriese JBS[19], der im Jahr 2021 durch einen Ransomware-Angriff der REvil-Gruppe lahmgelegt wurde.

BRANCHEN, DIE 2022 AM STÄRKSTEN VON RANSOMWARE BETROFFEN SIND

2 **TECHNOLOGIE**

1 **FERTIGUNG**

3 **FINANZDIENSTLEISTUNGEN**

4. BAUGEWERBE **5. EINZELHANDEL** **6. GESUNDHEITSWESEN** **7. BILDUNG** **8. REGIERUNGSBEHÖRDEN** **9. TRANSPORT** **10. RECHT**

11. ENERGIE **12. UNTERHALTUNG** **13. AUTOMOBIL** **14. VERSORGUNGSUNTERNEHMEN** **15. LANDWIRTSCHAFT** **16. GASTRONOMIE-FREIZEIT**

17. GEMEINNÜTZIGE UNTERNEHMEN/NGO/BÜRGERLICH-GESELLSCHAFTLICH/POLITISCH **18. VERSICHERUNGEN** **19. UNBEKANNT**

20. TELEKOMMUNIKATION **21. BERGBAU** **22. LUFTFAHRT** **23. VERTEIDIGUNG** **24. INFRASTRUKTUR**

Quelle: Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

2.3 Welche Auswirkungen gibt es auf die Zielstrukturen?

Über den Datenverlust hinaus sehen sich die betroffenen Organisationen mit weiteren, möglicherweise dauerhaften Folgen konfrontiert: Produktionsstopps, Umsatzeinbrüche, rechtliche Risiken, Verlust des Kundenvertrauens ...

2 bis 3 Milliarden €

KENNZAHL

Dies sind die geschätzten Kosten des Ransomware-Angriffs, der Clestra Hauserman im April 2022 traf. Der elsässische Hersteller von Trennwänden für Büros und „Reinräume", der bereits durch die wirtschaftliche und geopolitische Lage in Schwierigkeiten geraten war, wurde für sechs Monate unter Insolvenzverwaltung[21] gestellt.

Wie der Name schon sagt, ist die logische Folge eines Ransomware-Angriffs die Forderung nach einem Lösegeld. Dies ist jedoch nicht die einzige Konsequenz für die Opfer. In den meisten Fällen werden sie nur feststellen können, dass ihre Produktion gestört oder sogar eingestellt wird. Dies wiederum führt zu Umsatzeinbußen und im Extremfall sogar zur Schließung des Unternehmens.

Und auch die Daten bleiben nicht verschont. Sie können von Offenlegung bedroht sein, beschädigt oder sogar zerstört werden. Wenn Cyberkriminelle auf Daten zugreifen, setzen sie die betroffenen Unternehmen in jedem Fall einem rechtlichen Risiko aus, wenn sie nachweislich gegen die DSGVO verstoßen. Schließlich wird sehr oft der Ruf eines Unternehmens durch einen Ransomware-Angriff geschädigt.

Was die eher indirekten Folgen angeht, so haben Forscher[20] herausgefunden, dass der Druck, der durch die Bedrohung durch Ransomware auf IT-Sicherheitsexperten lastet, zu einer erhöhten Fluktuation in diesen Teams beiträgt.–

+71 %

KENNZAHL

LÖSEGELDFORDERUNGEN, DIE IMMER HÖHER STEIGEN ...

500 $ im Jahr 2016, 300.000 $ im Jahr 2020, fast 1 Million $ in den ersten fünf Monaten des Jahres 2022 (oder +71 % im Vergleich zu 2021).

WEITERFÜHRENDE INFORMATIONEN

PSYCHOLOGISCHE AUSWIRKUNGEN

Eine Folge aller Auswirkungen eines Cyberangriffs mit Ransomware ist natürlich finanzieller Art. Aber ist das wirklich die einzige Folge? Dies würde bedeuten, die gesellschaftlichen und psychologischen Dimensionen von Angriffen zu vergessen, die (zu) oft vernachlässigt werden.

2.4 Zahlen oder nicht zahlen, muss man nachgeben?

Zahlen oder nicht zahlen? Einer Lösegeldforderung nachgeben oder nicht? Dieses heikle Thema hat vielen Entscheidungsträgern schlaflose Nächte bereitet. Denn diese Entscheidungsfindung wirkt sich auf die finanzielle Stabilität der Einrichtung, ihre Tätigkeit, aber auch ihren Ruf und ihre Ethik aus.

KENNZAHL

80 %

Etwa 80 % der Unternehmen, die das geforderte Lösegeld zahlen, werden erneut Opfer eines Angriffs[23].

Wer sind die Unternehmen, die das geforderte Lösegeld zahlen? Die Antwort erweist sich als schwierig, denn nur wenige geben die Operation zu. Entschlüsseln statt neu aufbauen oder gar verschwinden: Kleinere Betriebe werden nicht lange zögern, da ihr Überleben davon abhängen kann ... Größere Unternehmen werden sich eher aus Gründen des Rufs oder der finanziellen Ergebnisse beugen. Aus welchen Gründen auch immer, die Zahlung eines Lösegelds bleibt oft der letzte Ausweg. Es ist auch wichtig, daran zu erinnern, dass ein bereits erfolgter Ransomware-Angriff nicht vor einem weiteren Angriff schützt. So musste ein britisches Unternehmen[22] zweimal im Abstand von wenigen Wochen ein Lösegeld zahlen.

In Frankreich könnte das grüne Licht, das das Wirtschaftsministerium für eine Entschädigung bei Lösegeldzahlungen durch Versicherer gegeben hat, wenn Klage eingereicht wird, nicht nur widersinnige Auswirkungen haben, sondern auch die Botschaft der nationalen Behörde ANSSI[24] zu diesem Thema vernebeln. –

„Es ist gut, dass es dieses Urteil gibt, denn es trägt dazu bei, dass in den höchsten Kreisen über das Thema gesprochen wird, aber das wird das Grundproblem nicht ändern. Ein positiver Aspekt ist, dass es den „verdeckten" Lösegeldzahlungen wohl ein Ende setzen wird, damit potenzielle Sanktionen der CNIL vermieden werden.[25]"

SÉBASTIEN VIOU – DIREKTOR FÜR PRODUKTSICHERHEIT UND CYBEREXPERTE BEI STORMSHIELD

PODCAST

RANSOMWARE: MUSS MAN VERSICHERN UND BEZAHLEN?

Was könnte bei dieser kniffligen Frage besser sein als ein Podcast unter Experten? Gespräche über die Richtigkeit dieses Gesetzesvorhabens mit Valéry Rieß-Marchive, Chefredakteurin des MagIT, Fabrice Epelboin, Damien Douani und Bertrand Lenotre[26].

AKTUELL

ENTSCHÄDIGUNG FÜR UNTERNEHMEN, DIE OPFER VON RANSOMWARE GEWORDEN SIND

DAS HEIKLE THEMA DER CYBERVERSI-CHERUNG

Alles begann im Juni 2021. Bruno Le Maire, Minister für Wirtschaft und Finanzen sowie die industrielle und digitale Souveränität, und die Generaldirektion des Finanzministeriums bilden eine Arbeitsgruppe, um ein Versicherungsangebot zur Deckung von Cyberrisiken auszuarbeiten, an der staatliche Stellen, Unternehmensvertreter, Versicherungs- und Rückversicherungsorganisationen sowie Experten aus der akademischen Welt beteiligt sind.

Es zeichnet sich ein Aktionsplan mit vier Schwerpunkten ab:

- → **Klärung des rechtlichen Rahmens für die Versicherung von Cyberrisiken,**
- → **Besseres Verständnis und Messung von Cyberrisiken,**
- → **Verbesserte Aufteilung der Risiken unter Versicherten, Versicherern und Rückversicherten,**
- → **Verstärkte Bemühungen zur Aufklärung.**

Infolge dieses Berichts schlägt das Wirtschafts- und Finanzministerium dem Ministerrat Ende 2022 eine Maßnahme vor, die sich insbesondere mit Cyber-Ransomware im Rahmen des Gesetzentwurfs zur Ausrichtung und Programmierung des Innenministeriums (LOPMI) befasst.

Einzige Bedingung: Das Opferunternehmen muss innerhalb von 48 Stunden nach Entdeckung des Cyberangriffs Anzeige erstatten. Später enthielt der von der Rechtskommission (in der Nationalversammlung) angenommene Text nicht mehr das Wort Lösegeld, sondern verwendete einen umfassenderen Ausdruck für durch Cyberangriffe verursachte Schäden.

Bei der Veröffentlichung dieser Informationen wurden zahlreiche Stimmen laut, die auf verschiedene Risiken und Grauzonen dieses Ansatzes hinwiesen. Unsicherheiten zur Lösegeldforderung selbst: Wer wird zahlen? Ist es das Unternehmen selbst oder ein Vermittler wie z. B. ein Verhandlungsführer? Welche Betreuung genießen Letztere? Welche Beträge werden erstattet? Und die möglichen Folgen: Wird die Höhe des Lösegelds steigen? Werden französische Unternehmen stärker ins Visier genommen? Auch wenn es noch zu früh ist, sie zu beantworten, werden diese Fragen auch in Zukunft zentral bleiben.

Andere wiederum betonen, dass Lösegeldzahlungen auch Vorteile mit sich bringen können (z. B. eine bessere Überprüfung der Geldströme, die bei der Verfolgung von Cyberkriminellen als wichtige Indizien dienen können). Es ist also noch nichts entschieden. –

INTERVIEW

LÖSEGELD: ZAHLEN ODER NICHT ZAHLEN – STELLT SICH DIESE FRAGE AUCH HEUTE NOCH?

→ Die offizielle Empfehlung des ANSSI ist unmissverständlich: Das geforderte Lösegeld sollte nicht gezahlt werden. Dennoch hat in Frankreich im Jahr 2021 eines von fünf angegriffenen Unternehmen nachgegeben. Warum?

WARUM SOLLTE KEIN LÖSEGELD BEZAHLT WERDEN?

„Viele Unternehmen glauben, dass dies der beste Weg ist, um den Betrieb so schnell wie möglich wieder aufzunehmen. Aber das ist nicht zwangsläufig der Fall. Sehr oft ist das vom Angreifer entwickelte Dechiffrierungstool fehlerhaft. Außerdem zwingt der Vertrauensverlust dazu, vor der Wiederherstellung der Daten eine Analysephase zu durchlaufen. Man muss sich vor Augen halten, dass die Datenwiederherstellung immer noch die sicherste Methode ist, um seine Daten wiederzufinden: Im Durchschnitt bekommen nur 54 % der zahlenden Betriebe ihre Daten wieder."[28]

ARNAUD PILON –
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

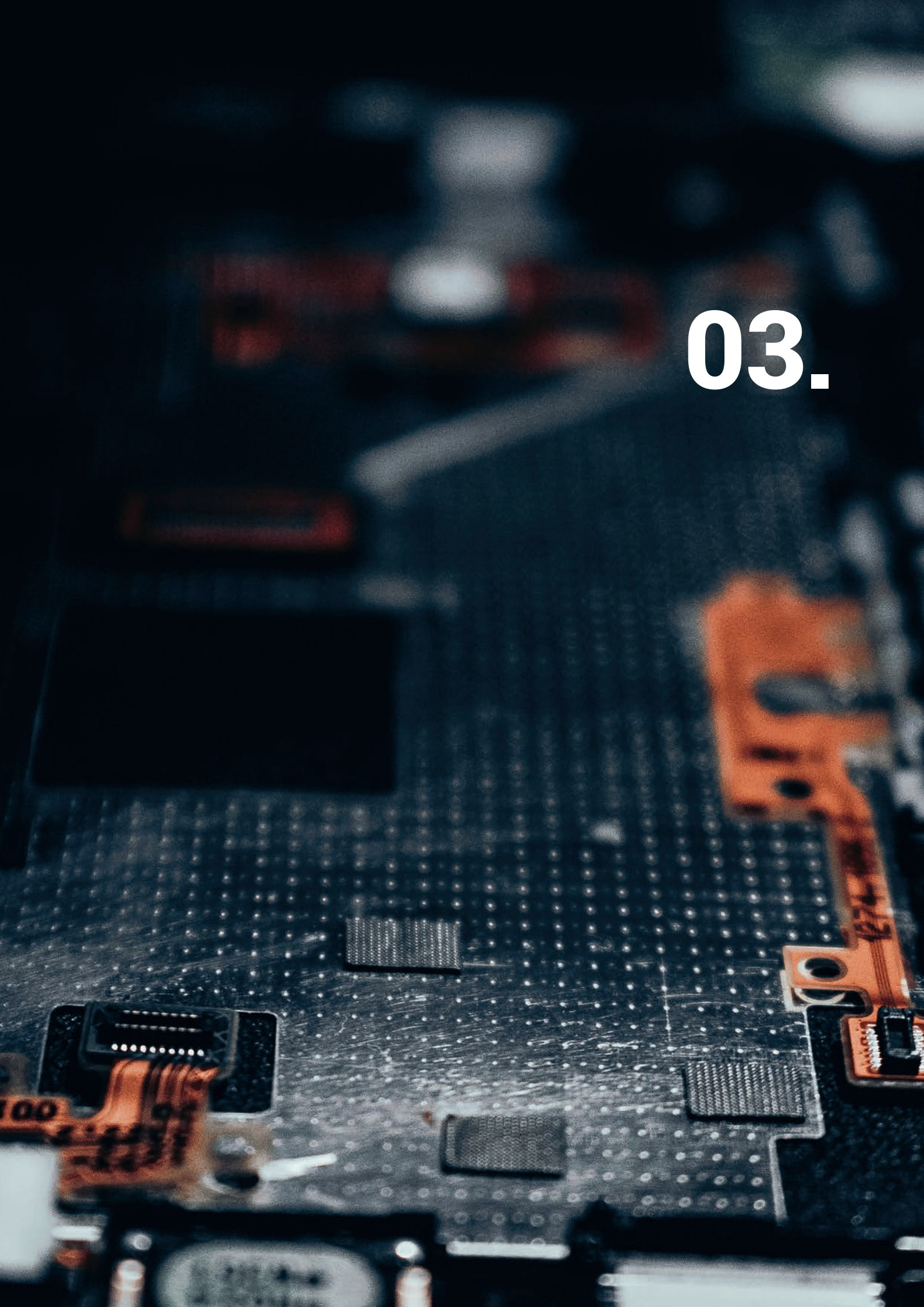
„Aus ethischer Sicht kann die Zahlung auch als Bestätigung des Modells angesehen werden. Dies ist übrigens auch der Ursprung der Kontroverse um das Risikomodell der Versicherer."

NICOLAS CAPRONI –
HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

WARUM HABEN MANCHE UNTERNEHMEN KEINE WAHL?

„Die Opfer sind manchmal ganz junge Unternehmen, die noch nicht in die Sicherung ihrer Daten investieren konnten. Für sie ist die Bezahlung eine Frage des Überlebens. Anstatt diese in die Enge getriebenen Betriebe zu verurteilen, könnten die Behörden die Zahlungen nachverfolgen, um Ransomware-Banden zu zerschlagen. Und parallel dazu über die Einführung einer Art Cyber-TÜV nachdenken. Warum nicht eine Steuergutschrift einführen, die es ermöglicht, die Sicherheit junger Unternehmen zu prüfen?"

FLORENT CURTET –
LEITER VON NEOCYBER UND MITBEGRÜNDER VON HACKERS SANS FRONTIÈRES



03.

Im Räderwerk der Ransomware: Reibungslose Mechanik

Verschiedene Endgeräte können Ziel von Ransomware sein: ein Arbeitsplatz, ein Mobiltelefon, ein Automat in einer Fabrik, ein vernetztes Fahrrad in einem Fitnessstudio … Aber was passiert bei einem solchen Angriff konkret?

3.1 Route einer Ransomware

Wie verbreitet sich Ransomware? Welches sind ihre wichtigsten Triebfedern? Initial Access und Infektion, Tarnung, Suche nach ausnutzbaren Schwachstellen … Der Prozess besteht aus mehreren strategischen und gut eingespielten Phasen.

Der Begriff „Ransomware“ bezog sich – historisch gesehen – hauptsächlich auf „Blocker“, die den Zugriff auf ein System blockierten, und „Crypto“, die die Daten verschlüsselten.

Heute gilt er für alle Programme, die Erpressung ermöglichen. Es handelt sich um eine komplexe Art des Angriffs, die auf verschiedenen Mechanismen und unterschiedlichen Zeitpunkten beruht. Dennoch geht diesen Angriffen immer eine Infektion voraus. Diese kann durch Phishing, Peer-to-Peer-Downloads, Drive-by-Downloads, Ausnutzung von Schwachstellen usw. erfolgen.

Danach folgt die eigentliche Angriffsphase, in der ein „Dropper“ eine Hintertür im System schafft, durch die alle für den Angriff notwendigen Werkzeuge vorbei an den Erkennungsmechanismen installiert werden können, bevor der „Loader“ dafür sorgt, dass der Angriff erfolgreich durchgeführt wird.

Danach tritt der Cyberkriminelle in die Phase der Defense Evasion ein, in der er versuchen wird, die Spuren seines Eindringens zu verwischen, damit die Hintertür einen Neustart des betroffenen Systems übersteht. In der nächsten Phase, genannt *Credential Access* versucht der Angreifer, durch den Diebstahl von Kontonamen und Passwörtern Zugang zum System zu erhalten. Es beginnt eine Phase von einigen Stunden bis zu einigen Monaten (*Discovery* oder Entdeckung des Netzwerks), während Cyberkriminelle nach Einfallstoren suchen, um sich dann weiter zu verbreiten. Diese Einfallstore können sowohl gestohlene Passwörter, ausnutzbare Schwachstellen oder falsche Sicherheitseinstellungen sein. Anschließend identifizieren sie Dateien mit wertvollen Daten (*Collection*) und verschlüsseln sie, manchmal indem sie die vorher exfiltrierten Daten und die Backups löschen.

Der letzte Schritt zielt darauf ab, das Opfer durch die Veröffentlichung von Beweisen für den Angriff unter Druck zu setzen, z. B. über Screenshots auf der Website der Gruppe, meist über das Tor-Netzwerk. Manchmal führen Cyberkriminelle parallel dazu auch eine Denial-of-Service-Attacke durch. Ein zusätzlicher Druck, um das Opfer zu einer schnelleren Zahlung zu veranlassen und auch, um zu verhindern, dass das Unternehmen z. B. auf seiner Website darüber berichtet. –

STICHWORT

Ein Dropper ist ein Computerprogramm, das dazu bestimmt ist, schädliche Software auf einem System zu installieren. Der Loader hingegen kümmert sich um die Ausführung.

Dropper

WIE LÄSST SICH DER MECHANISMUS VON RANSOMWARE EINFACH ERKLÄREN?

INITIAL ACCESS

↓

AUSFÜHRUNG
BEFEHLSZEILENSCHNITTSTELLE

↓

PERSISTENZ

↓

ESKALATION VON PRIVILEGIEN

↓

UMGEHUNG DER ABWEHRMECHANISMEN
KOMPILIERTE HTML-DATEI

↓

ZUGRIFF AUF ZUGANGSDATEN
PRIVATE SCHLÜSSEL

↓

ENTDECKUNG
PROZESSERKUNDUNG

↓

WEITERVERBREITUNG

↓

ERFASSUNG:
DATENFORMULAR LOKALES SYSTEM

↓

BEFEHL UND KONTROLLE

↓

EXFILTRATION
KOMPRIMIERTE DATEN

↓

AUSWIRKUNG
VERSCHLÜSSELTE DATEN FÜR AUSWIRKUNGEN

Quelle: Rahmenwerk MITRE ATT&CK

3.2 Fokus auf Initial Access

Sobald er ein Opferunternehmen ermittelt hat, beginnt der Cyberkriminelle mit der akribischen Arbeit, in das Informationssystem des Unternehmens einzudringen. Auf der Suche nach einem wertvollen Sesam-öffne-dich: dem berühmten Initial Access.

Sobald das Opferunternehmen ermittelt ist, beginnt der Cyberkriminelle mit der akribischen Arbeit, in das Informationssystem des Unternehmens einzudringen. Auf der Suche nach einem wertvollen Sesam-öffne-dich: dem berühmten Initial Access.

Diese Zugriffe sind der Grundstein von Ransomware-Gruppen, da sie dazu dienen, in das Informationssystem ihrer zukünftigen Opfer einzudringen. Sie benötigen eine lange Erkundungsphase. *„Bei der Untersuchung von Zielen geht es um mehr als nur die technische Untersuchung der im Internet exponierten Angriffsfläche,* Valéry Marchive erläutert dies in einem Artikel[29] auf Le Mag IT. *Sondern dazu gehört auch, Kontaktdaten zu erhalten, mit denen jede der identifizierten Personen kontaktiert werden kann. Vermutlich, um nach der Auslösung der Ransomware Druck auszuüben.“*

Um all diese Daten abzurufen, werden verschiedene Techniken eingesetzt. Mehr oder weniger ausgeklügelte **Phishing-E-Mails** sind der klassische Vektor schlechthin. Parallel dazu werden auch andere Kanäle mobilisiert, um ähnliche Social-Engineering-Techniken einzusetzen, wie z. B. der LinkedIn-Messenger.

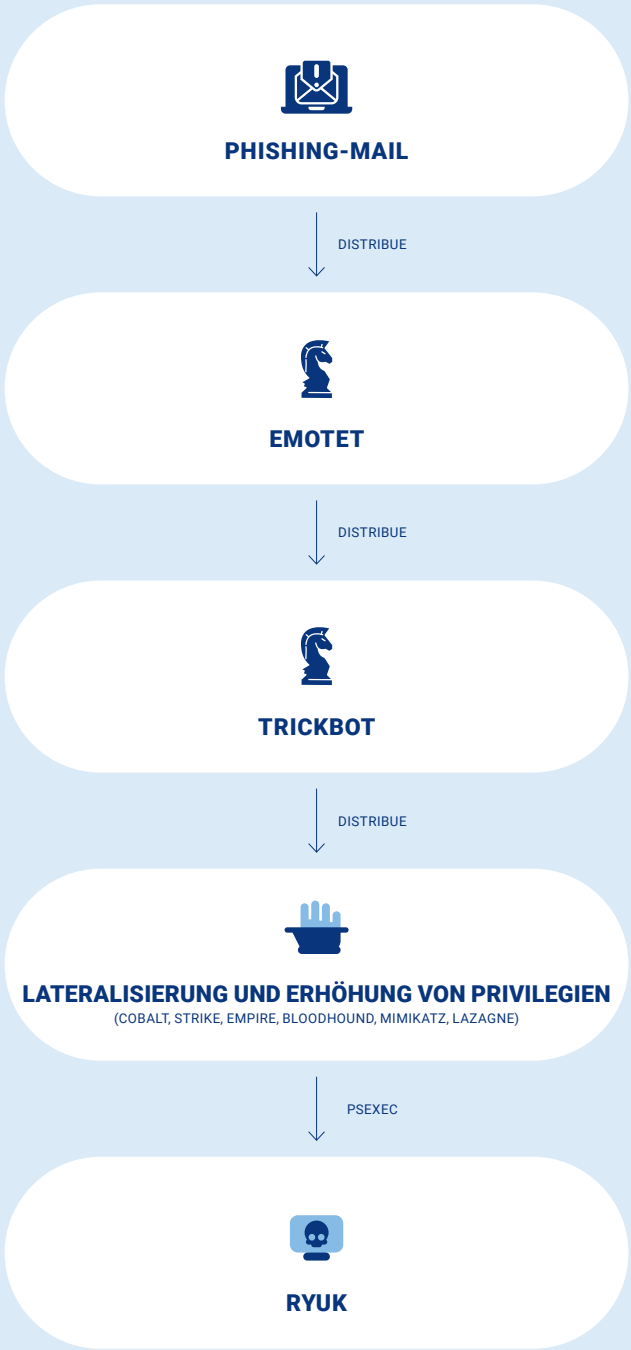
WEITERFÜHRENDE INFORMATIONEN

RANSOMWARE: WIE CONTI DIE CYBERANGRIFFE VORBEREITET.

Ein Artikel, um zu verstehen, wie die Conti-Gruppe den Initial Access auf die Informationssysteme vieler Organisationen weltweit erlangt.

RANSOMWARE IST AUCH TEIL EINER KOMPLEXEREN KETTE

VEREINFACHTER ABLAUF DER INFEKTIONSKETTE EMOTET-TRICKBOT-RYUK



Quelle: Rapport „Le rançongiciel Ryuk", ANSSI, 2021

Aber auch die in Unternehmen eingesetzte Software kann Teil der Angriffsfläche sein, wenn diese unwissentlich eine Schwachstelle besitzt, die häufig während der Replikationsphase ausgenutzt wird.

„Es ist nicht ungewöhnlich, dass Cyberkriminelle andere Malware wie Emotet, Trickbot oder den Bumblebee-Loader im Vorfeld ihres Angriffs einsetzen“

NICOLAS CAPRONI – HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

„Die Technologien sind schnittstellenfähig geworden. Hier agiert Emotet wie ein trojanisches Pferd, ruft vom Angreifer bereitgestellten Code ab und verbreitet sich dann wie ein Wurm. Es ist also eher ein Mittel als ein Zweck. Trickbot wiederum ist ein Botnet, das den Client infiltriert, auf die Anweisungen von Emotet wartet und diese dann ausführt.“

PIERRE-OLIVIER KAPLAN – FORSCHUNGS- UND ENTWICKLUNGSINGENIEUR, STORMSHIELD

Die Verbreitung über Lieferketten ist ein weiterer Faktor, der die Komplexität der Angriffe erhöht: Cyberkriminelle kompromittieren ganze Lieferketten, indem sie auf Schwachstellen in Managementsoftware und/oder Cloud-Diensten abzielen. So wird im Mai 2021 der IT-Lösungsanbieter Kaseya Opfer von REvil. Über die Netzwerke von 60 seiner Kunden sind mehr als 1.500 Unternehmen betroffen, und das geforderte Lösegeld beläuft sich auf 70 Millionen $[30]. –

+1500

KENNZAHL

Mehr als 1.500 Unternehmen waren von der Infektion mit Software des Anbieters Kaseya betroffen


04.
SYSTEM
HACKED

Welche Strategien sollte man anwenden, um diese Geldmaschinen zum Entgleisen zu bringen?

Ransomware ist zum Sorgenkind der IT-Abteilungen und der Unternehmen im Allgemeinen geworden. Ist sie deshalb ein unabwendbares Schicksal? Wir fragen Sébastien Viou, Direktor für Produkt-Cybersicherheit und Cyberexperte von Stormshield, welche Maßnahmen ergriffen werden können, um dem entgegenzuwirken.

SCHUTZ VOR DEM RANSOMWARE-ANGRIFF

- **DATEN SICHERN ... UND BACKUPS SCHÜTZEN[31]**
  „Diese Vorsichtsmaßnahme allein reicht nicht aus, da die Ransomware zuerst die Backups zu zerstören versucht, noch vor der Verschlüsselung. Die Sicherungsdateien dürfen nicht mit dem Computer verbunden sein und Backups müssen häufig durchgeführt werden. Außerdem muss die Wiederherstellung getestet werden, um sicherzustellen, dass die Sicherungsdateien brauchbar sind."

- **SOFTWARE UND SYSTEME AUF DEM NEUESTEN STAND HALTEN**
  „Die Updates müssen kontinuierlich durchgeführt werden und Windows-PCs, aber auch Linux- und Mac-Systeme, die ebenfalls Einfallstore sein können, einschließen. Die gesamte Bürolandschaft ist betroffen, von Microsoft Exchange über das Active Directory bis hin zu allen exponierten Servern, auch wenn es sich um kleine handelt."

- **INFORMATIONSSYSTEME PARTITIONIEREN**
  „Dazu empfiehlt es sich, strenge Regeln für den zulässigen Datenfluss zwischen verschiedenen Bereichen je nach ihrer Kritikalität einzurichten."

- **BENUTZERRECHTE UND NUTZERBERECHTIGUNGEN EINSCHRÄNKEN**
  „In diesem Punkt ist das Zeitmanagement entscheidend: Um die Sicherheit aufrechtzuerhalten, muss man regelmäßige Überprüfungen einplanen."

- **PROTOKOLLÜBERWACHUNG IMPLEMENTIEREN**
  „Die Log-Sammlung ist ein Muss. In Fällen, in denen ein sehr hohes Sicherheitsniveau erforderlich ist, kann über ein SOC eine Komponente zur Erkennung von Eindringlingen hinzugefügt werden."

- **MITARBEITER SENSIBILISIEREN**
  „Mit dem Social Engineering ist das Haupteinfallstor in das Informationssystem eines Unternehmens immer noch die Belegschaft. Daher ist es wichtig, über Themen der Cybersicherheit zu sprechen, auch wenn die Sensibilisierung ihre Grenzen hat."

8 %

Dies ist der Anteil von CERN-Mitarbeitern, die mit einer nach einer Sensibilisierung durchgeführten, gefälschten Phishing-Kampagne getäuscht wurden[32]

- **STRATEGIE FÜR DIE KRISENKOMMUNIKATION IM CYBERSPACE ENTWERFEN**
  „Auch hier ist es hilfreich, wenn man im Vorfeld an seinen Botschaften und Kontakten gearbeitet hat, um mit den verschiedenen Zielgruppen angemessen zu kommunizieren. Mitteilungen, die dazu dienen, z. B. vor einem ungeplanten Produktionsstopp zu warnen oder auch vor dem Verlust persönlicher Daten, wie in der DSGVO vorgesehen."

- **PLAN ZUR REAKTION AUF CYBERANGRIFFE UMSETZEN**
  „Dieser Plan ist entscheidend, da er eine schnelle Reaktion ermöglicht, indem zum Beispiel die zuvor identifizierten CERT-Firmen so früh wie möglich kontaktiert werden. Er umfasst natürlich auch eine technische Komponente mit der Einführung von Schutzlösungen wie Stormshield Endpoint Security Evolution und Stormshield Network Security."

- **NUTZEN EINER CYBER-VERSICHERUNG BEURTEILEN**
  „Einige Cyber-Versicherungen enthalten Klauseln, die den Einsatz von Cyber-Sicherheitslösungen vorschreiben, und sind in dieser Hinsicht interessant, da sie einen gewissen Schutz vorsehen. Dennoch sollte man die Cyberversicherung nicht als Überlebensmaßnahme sehen, die allein ausreicht, und schon gar nicht als Schutzmaßnahme. Mit anderen Worten: Eine Versicherung gegen Ransomware ist niemals eine Cybersicherheitsstrategie."

02

SCHADENSBEGRENZUNG WÄHREND EINES RANSOMWARE-ANGRIFFS

- **GUTE REFLEXE ANNEHMEN**
  „Man muss in der Lage sein, schnell zu erkennen, dass etwas nicht stimmt, und nicht davor zurückschrecken, den Stecker zu ziehen, um das Risiko zu mindern und die Ausbreitung so weit wie möglich einzudämmen. Auch auf individueller Ebene muss man lernen zu reagieren, zu sagen „Ich habe an der falschen Stelle geklickt", denn jede Minute zählt."
- **STEUERUNG DES CYBER-KRISENMANAGEMENTS VOM VORSTAND**
- **AUF DER RICHTIGEN EBENE KOMMUNIZIEREN**
- **ANZEIGE ERSTATTEN**

03

WIEDERHERSTELLUNG NACH EINEM RANSOMWARE-ANGRIFF

- **SYSTEME AUS GESUNDEN QUELLEN WIEDERHERSTELLEN**
- **NACHFORSCHUNGEN ÜBER DEN ANGRIFFSPFAD ANSTELLEN**
  „Um den Ablauf des Angriffs und die Schwachstellen des eigenen Systems zu verstehen, muss man analysieren, was passiert ist. Auf diese Weise schafft man sich die besten Voraussetzungen, um zu verhindern, dass so etwas noch einmal passiert."
- **KORREKTURPLAN ERSTELLEN**
  „Je nach Fall muss man vielleicht eine Multi-Faktor-Authentifizierung einführen oder die auf den Rechnern vorhandenen Sicherheitslösungen verbessern."
- **FALL DER VERSICHERUNG VORLEGEN**
- **SETZEN SIE DEN KOMMUNIKATIONSPLAN BEI DEN BETROFFENEN KUNDEN, IHREN INVESTOREN USW. EIN.**
- **UMGANG MIT DEN PSYCHOLOGISCHEN AUSWIRKUNGEN AUF DIE MITARBEITER**
  „Kurzarbeit, Schuldgefühle, Überlastung der IT-Teams – Ransomware hat auch Auswirkungen auf die menschlichen Ressourcen, die berücksichtigt werden müssen."
- **STRAFVERFOLGUNG EINLEITEN, FALLS DIES NICHT BEREITS GESCHEHEN IST**
- **EINEN PRODUKTIONSPLAN ERSTELLEN, UM DEN RÜCKSTAND AUFZUHOLEN**

WAS BIETET STORMSHIELD ENDPOINT SECURITY EVOLUTION IN BEZUG AUF RANSOMWARE?

→ SES Evolution bietet Funktionen, die im Kampf gegen die Bedrohung durch Ransomware besonders nützlich sind: Erkennung von Dateiverschlüsselung, Schutz vor automatischen Backups und vor dll-Injektionen, Verhaltensanalyse und Echtzeitblockierung von Prozessen mit anormalem Verhalten. –

UM MEHR ZU ERFAHREN, SEHEN SIE SICH DIESES VIDEO AN


05.

Welche Zukunft hat Ransomware?

Morgen: Welche Folgen hat Ransomware? Wird sie Kryptowährungs-Wallets angreifen? Oder autonome Fahrzeuge? Werden Cyberkriminelle KI nutzen, um polymorphe Angriffe durchzuführen? Nein, Sie befinden sich nicht in einer Dystopie. Nur in der Welt, die auf uns zukommt.

5.1 Wie wird sie aussehen, die Ransomware von morgen?

Das typische Porträt der Ransomware von morgen ist noch nicht geschrieben. Eines ist jedoch sicher: Sie wird komplexer werden und sich an ein sichereres Umfeld anpassen. Sie wird auch nach reiferen Unternehmen und fragilen geopolitischen Kontexten Ausschau halten.

LockBit ist zwar derzeit die beliebteste Ransomware-Franchise, doch die Konkurrenz ist groß. Allein im ersten Halbjahr 2022 sind zwanzig neue Gruppen aufgetaucht.

„Wir können uns vorstellen, dass diese Ransomware morgen Kryptowährungs-Wallets, NFT, autonome Fahrzeuge angreift. Auch aufstrebende Technologien sind nicht davor geschützt."

PIERRE-OLIVIER KAPLAN – CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

Die geopolitische Lage und die sich anbahnenden Wirtschaftskrisen sind in der Tat ein fruchtbarer Nährboden für Ransomware. Die Akteure verdoppeln ihre Investitionen in Forschung und Entwicklung.

„Unsere technischen Untersuchungen haben auch ergeben, dass eine wenig bekannte RaaS-Erpressergruppe namens Vice Society eine Zweifachstrategie benutzt und je nach Ziel und System unterschiedliche Ransomware einsetzt: Zepplin für Windows, HelloKitty für Linux.[33]"

NICOLAS CAPRONI – HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

Diese Entwicklungen sind jedoch immer noch recht teuer. Dies zwingt Cyberkriminelle dazu, große Unternehmen ins Visier zu nehmen, damit sich die Operation amortisiert. –

NEUE RANSOMWARE-FAMILIEN IM 1. QUARTAL 2022

- → YourCyanide
- → Vandili
- → GoodWill
- → Vulcan Ransom Team
- → Cheerscrypt
- → NwGen
- → Axxes
- → RTM
- → Nokoyawa
- → Pandora
- → Hermetic Ransom
- → Mindware
- → Yashma
- → Onyx
- → Black Basta

Quelle: Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

WIE SPÜRT MAN RANSOMWARE AUF?

MIT **ARNAUD PILON** – DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ „Es ist nicht einfach, bei den Nachrichten über Ransomware auf dem aktuellen Stand zu bleiben. Wir versuchen, Invarianten bei den Vorgehensweisen, Techniken und Werkzeuge zu finden, denn es ist nicht ungewöhnlich, dass die verschiedenen Gruppen „Tricks" miteinander teilen, z. B. bei den Verbreitungsmethoden. Wir behalten auch die nicht zu unterschätzenden Phishing-Kampagnen im Auge. Schließlich versuchen wir zu ermitteln, welche Schwachstellen massenhaft ausgenutzt werden können." –

5.2 Welche Lösungen sollten weiterverfolgt werden?

Angesichts der sich ständig weiterentwickelnden Bedrohungen müssen die Lösungen zum Schutz von Arbeitsplätzen mit der Entwicklung Schritt halten. Die Verbesserung und Vervielfältigung von Erkennungsmitteln ist ein Weg, der erforscht werden muss, aber dies sollte uns nicht die notwendigen Schutzlösungen vergessen lassen.

Die Ransomware hat dafür gesorgt, dass über Bedrohungen der Informationssysteme geredet wird. Diese Mitteilung weckte die Datenschutzbeauftragten auf, die daraufhin die Sicherheitsstufen erhöhten. Der Druck durch Ransomware hat nicht nur für eine größere Widerstandskraft der Informationssysteme gesorgt, sondern auch die IT-Sicherheitsbranche wiederbelebt.

So bietet der Markt für Cybersicherheitslösungen bereits eine Reihe von Tools wie EDR oder XDR an, die die Möglichkeiten zur Erkennung und Blockierung von Ransomware erhöhen. Man darf jedoch nicht vergessen, dass diese Lösungen zur Erkennung und Behebung von Sicherheitslücken palliativ sind: Zu diesem Zeitpunkt hat der Cyberangriff in den Unternehmen bereits Schaden angerichtet. **Der erste Schritt, den Sie tun müssen, ist die Einrichtung von Schutzmaßnahmen** (für Daten, Computer und Netzwerke).

„Die Herausforderung der nächsten Jahre besteht darin, die Anzahl der false-positives bei großen SIEMs zu reduzieren. Dies kann durch die Unterstützung von maschinellem Lernen (KI) erfolgen, ist aber keineswegs ein Selbstläufer. Angesichts des vielschichtigen Sicherheitsproduktportfolios wird jedoch eine verbesserte Interoperabilität der Systeme entscheidend sein.“

ARNAUD PILON – DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

Die Instrumentalisierung von Lösungen ist daher einer der Wege, die es zu prüfen gilt, um die Ermüdung des SOC zu verringern.

Das Vertrauen in die eingesetzten Lösungen wird noch entscheidender werden, als es heute schon ist. Dies sollte die Bedeutung eines Qualifikationsschemas auf europäischer und/oder französischer Ebene erhöhen. –

WERDEN WIR EINES TAGES ÜBER EINEN „IMPFSTOFF“ GEGEN RANSOMWARE VERFÜGEN?

ARNAUD PILON – DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ ***„Leider passen sich die Bedrohungen schnell an diese Art von technischen Lösungen an. Solange diese Angriffe Geld einbringen, werden sich die Cyberkriminellen weiterhin anpassen, in Forschung und Entwicklung investieren und somit Fortschritte machen.“***

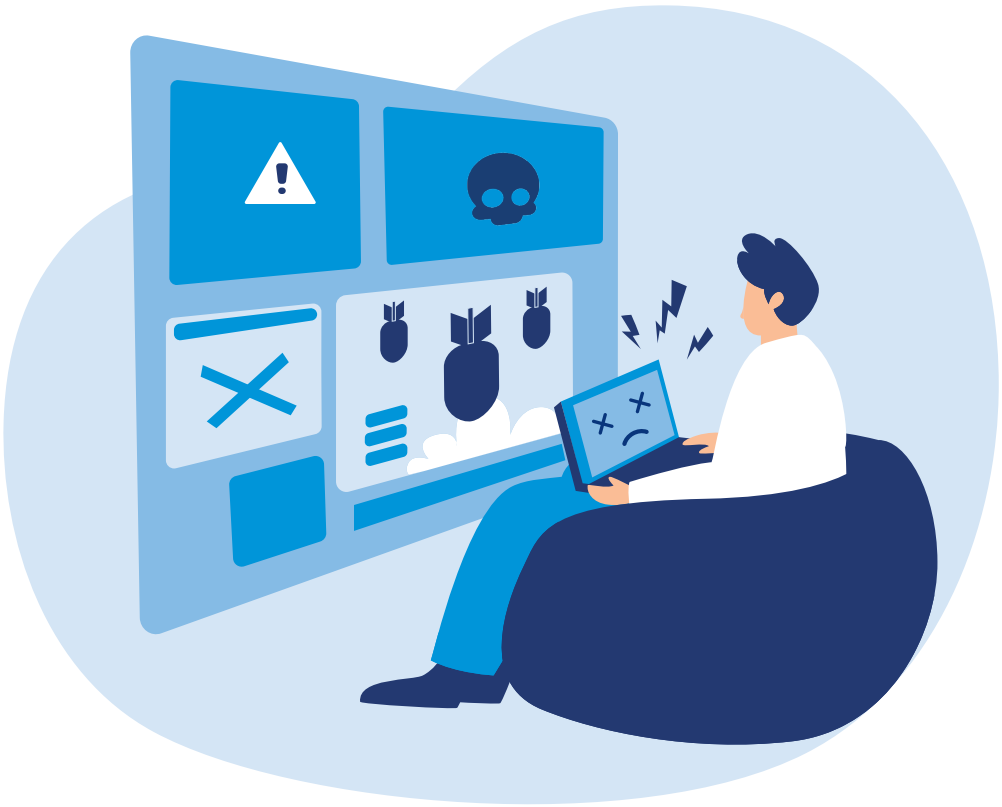
NICOLAS CAPRONI - HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

→ ***„Ich glaube nicht an einen Impfstoff, aber ich glaube auch nicht an das Schicksal. Die Opferforschung zeigt, dass die meisten Angriffe opportunistisch sind. Zwar wird es immer jemanden geben, der auf einen kompromittierten Anhang klickt, aber durch eine Kombination aus Bedrohungswissen und Erkennungstools ist es möglich, einen Angriff zu erkennen, bevor Daten verschlüsselt und extrahiert werden.“***

FLORENT CURTET - LEITER VON NEOCYBER UND MITBEGRÜNDER VON HACKERS SANS FRONTIÈRES

→ ***„Es gibt keine mittelfristigen Lösungen zur Eindämmung des Phänomens, zumal sich das Geschäftsmodell der Erpresser weiterentwickelt: Einige nutzen sehr fortgeschrittene Schwachstellen und bezahlen „Insider“ für die Ausführung des Virus.“***

Letztendlich sind Monitoring und Opferforschung im Kampf gegen Ransomware von entscheidender Bedeutung, da sie ein besseres Verständnis der cyberkriminellen Organisationen und damit eine bessere Bekämpfung dieser Bedrohung ermöglichen. Diese hat sich in den letzten drei Jahrzehnten nur verändert. Es ist also damit zu rechnen, dass noch regelmäßig neue Stämme und Varianten entdeckt werden, umso mehr vor dem Hintergrund des Aufkommens neuer Technologien und geopolitischer Konflikte.



QUELLEN UND ANHÄNGE

[1] https://www.liberation.fr/futurs/2017/06/28/notpetya-le-logiciel-ranconneur-a-propagations-multiples_1580043/
[2] https://www.leparisien.fr/high-tech/cyberattaque-les-centrales-nucleaires-francaises-sont-elles-en-securite-28-06-2017-7094979.php
[3] https://www.insurancebusinessmag.com/asia/news/cyber/ransomware-big-game-hunting-has-major-impact-on-insurers-189773.aspx
[4] https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
[5] https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
[6] https://www.zdnet.com/article/these-ransomware-attackers-sent-their-ransom-note-to-the-victims-printer/
[7] https://www.stormshield.com/fr/actus/petite-histoire-des-ransomwares/
[8] https://www.fbi.gov/news/testimony/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks
[9] https://www.zdnet.fr/actualites/le-groupe-de-ransomware-conti-ferme-son-site-vitrine-39943928.htm
[10] https://www-lemagit-fr.cdn.ampproject.org/c/s/www.lemagit.fr/actualites/252522126/Cyberattaques-Karakurt-fait-un-retour-en-fanfare?amp=1
[11] https://www.zdnet.fr/actualites/le-site-du-groupe-revil-donne-des-signes-de-vie-39940953.htm
[12] https://www.latribune.fr/technos-medias/informatique/qui-est-lockbit-3-0-le-cyber-ranconneur-de-la-poste-mobile-925065.html
[13] https://www.linkedin.com/posts/clementdomingo_cybersaezcuritaez-ransomwares-ransomgangs-activity-6985605220269441024-ZqLc
[14] https://www.lemagit.fr/actualites/252524255CHSF-lattaquant-ne-semble-pas-comprendre-que-cest-un-hopital-public
[15] https://www.ouest-france.fr/societe/cyberattaque/cyberattaques-voici-combien-les-entreprises-francaises-ont-perdu-depuis-janvier-482ff564-dfe7-11ec-b2a8-056c7579e285
[16] https://www.channelnews.fr/une-pme-francaise-sur-trois-a-deja-ete-victime-dun-ransomware-114729
[17] https://www.zdnet.com/article/ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
[18] https://www.lemondeinformatique.fr/actualites/lire-ransomware-jbs-debourse-11-m$-pour-recuperer-son-it-83225.html
[19] https://www.zdnet.fr/actualites/le-geant-de-l-agroalimentaire-jbs-vise-par-revil-39923901.htm
[20] https://www.lesechos.fr/pme-regions/grand-est/clestra-hauserman-demande-sa-mise-en-redressement-pour-trois-mois-1778519
https://www.lemoniteur.fr/article/clestra-place-en-redressement-judiciaire.2217432
[21] https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
[22] https://securite.developpez.com/actu/313967/Victime-d-un-ransomware-une-entreprise-paie-des-millions-aux-cybercriminels-pour-restaurer-ses-fichiers-L-entreprise-se-fait-attaquer-a-nouveau-par-le-meme-ransomware-et-paie-encore/
[23] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[24] https://www.usine-digitale.fr/article/ransomwares-rembourser-la-rancon-un-jeu-dangereux-dass-die-Versicherer-unter-den-Bedingungen-weiterspielen.N2038932
[25] https://www.linkedin.com/posts/s%C3%A9bastien-viou-b0806861_cybersaezcuritaez-ransomware-activity-6973284015197827073-dAGn?utm_source=share&utm_medium=member_desktop
[26] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[27] https://www.clubic.com/antivirus-securite-informatique/actualite-442272-cybersecurite-faut-il-assurer-les-victimes-de-ransomware-le-senat-dit-oui.html
[28] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf
[29] https://www.lemagit.fr/actualites/252501084/Ransomware-ces-rancons-payees-qui-plaident-en-faveur-de-la-cyberassurance
[30] https://www.numerama.com/cyberguerre/738790-apres-deux-mois-dabsence-le-terrible-gang-revil-fait-un-retour-inattendu.html
[31] https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
[32] https://www.cio-online.com/actualites/lire-experience-de-faux-phishing-au-cern-8%C2%A0-de-compromission-14450.html
[33] https://feedback.sekoia.io/changelog/11222

https://www.lesechos.fr/finance-marches/banque-assurances/
assurance-bercy-donne-son-feu-vert-a-lindemnisation-des-cyber-rancons-1786154
https://www.usine-digitale.fr/article/assurance-un-projet-de-loi-clarifie-le-cadre-
von-der-Entschädigung-der-Franken-im-Fall-eines-Angriffs.N2041292
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/
https://www.cap-com.org/actualit%C3%A9s/20h02-la-web-serie-des-hopitaux-lyonnais-sur-la-covid-19
https://www.stormshield.com/fr/actus/50-nuances-de-ransomwares/
https://www.stormshield.com/fr/actus/vers-une-nouvelle-economie-de-la-vulnerabilite/
https://www.stormshield.com/fr/zero-ransomware/
https://www.stormshield.com/fr/ressourcescenter/ask-ze-expert-ransomware-ne-payez-pas-les-rancons/
https://www.stormshield.com/wp-content/uploads/SES-FR-Ransomware-Infographics-202204.pdf
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.stormshield.com/fr/actus/quel-etat-des-lieux-des-ransomwares-en-2020/
https://www.stormshield.com/fr/actus/alerte-securite-snake-combattre-infection-avec-stormshield-endpoint-security/
https://www.stormshield.com/fr/actus/ransomware-robbinhood-pourquoi-baltimore-se-retrouve-sous-les-projecteurs/
https://www.stormshield.com/fr/actus/tour-dhorizon-des-ransomwares-les-plus-wtf-de-la-planete/
https://www.stormshield.com/fr/actus/les-pirates-seraient-ils-des-juillettistes/
https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
https://www.idc.com/getdoc.jsp?containerId=US48093721
https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
https://www.zdnet.com/article/
ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
https://cyware.com/news/ransomware-sprawl-fbi-finds-over-100-variants-to-be-active-88f659f6
https://youtu.be/azdrKZzyWgg
https://www.nomoreransom.org/fr/decryption-tools.html
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.vadesecure.com/fr/blog/ransomware-as-a-service-raas-une-activite-illicite-qui-a-desormais-pignon-sur-rue
https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
https://www.lemondeinformatique.fr/actualites/lire-4-groupes-de-ransomwares-emergents-dangereux-a-surveiller-83944.html
https://www.darktrace.com/fr/blog/les-9-stades-des-ransomwares-comment-l-ia-repond-a-chaque-etape/

DIE EUROPÄISCHE WAHL FÜR CYBERSICHERHEIT

WWW.STORMSHIELD.COM

STORMSHIELD