zeroBS

Secur|Ty made in Germany

WHITEPAPER

The Art of Defense

Ransomware Operations

Part 1

Whitepaper: RANSOMWARE OPERATIONS

zeroBS

INHALTSVERZEICHNIS

Zusammenfassung

Ransomware-Gangs haben 2020 ihren Gesamtumsatz mit über 350 Millionen $ mehr als verdreifacht. Dabei wurden neue Angriffswege direkt über Sicherheitslücken und Fehlkonfigurationen in der IT-Infrastruktur benutzt, und die Zahl der bekannten Ransomware-Gangs ist explosionsartig von 6 auf 36 gestiegen, Tendenz weiter zunehmend.

Die arbeitsteilig agierenden Gruppen benutzen alle aktuellen Verfahren und Toolchains, um den einmal gewonnenen Zugang (Initial Access) zu einem Unternehmensnetz zu sichern, auszubauen und für ihre Ziele ausnutzen zu können.

Zwar ist die häufig anzutreffende Ausgangslage „zu große Angriffsoberfläche, zu wenig Überblick“ altbekannt, aber erst im Zuge der Ransomeware-Aktivitäten zu einem wirklich drückenden Schuh geworden.

Abwehr und Schutz vor diesen Angriffen über IT-Infrastruktur besteht aus dem Erkennen der eigenen Gefährdungslage (↗ Attack Surface Monitoring) und nachfolgenden organisatorischen Maßnahmen (Reduzieren der Angriffsoberfläche, Netzseparation, MFA, Best-Practices).

Teil I – Einleitung

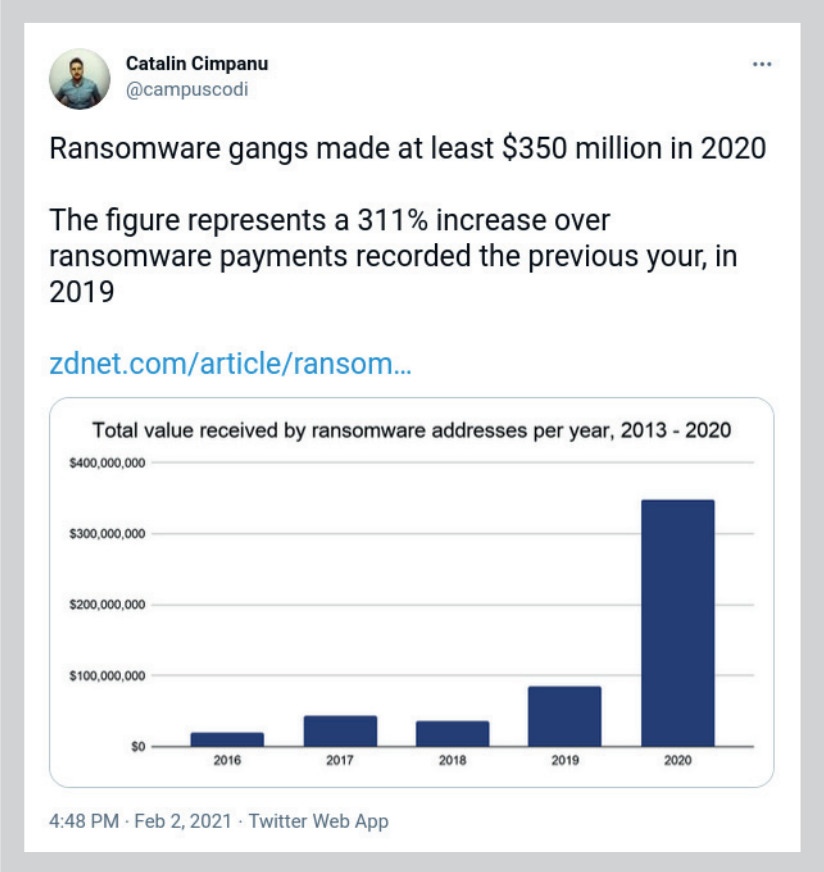
Das Jahr 2020 war extrem erfolgreich für die verschiedenen Ransomware-Gangs.

Einerseits hat sich der geschätzte Gesamtumsatz mit über 350 Mio $ mehr als verdreifacht, andererseits haben einzelne Gruppierungen wie REvil oder Ryuk jeweils mehr als 100 Mio $ eingenommen.

DarkTracer listet für die letzten 12 Monate über 2300 Unternehmen als Ransomware-Opfer; und das sind nur diejenigen, von denen man erfährt – mithin die Spitze des Eisbergs.

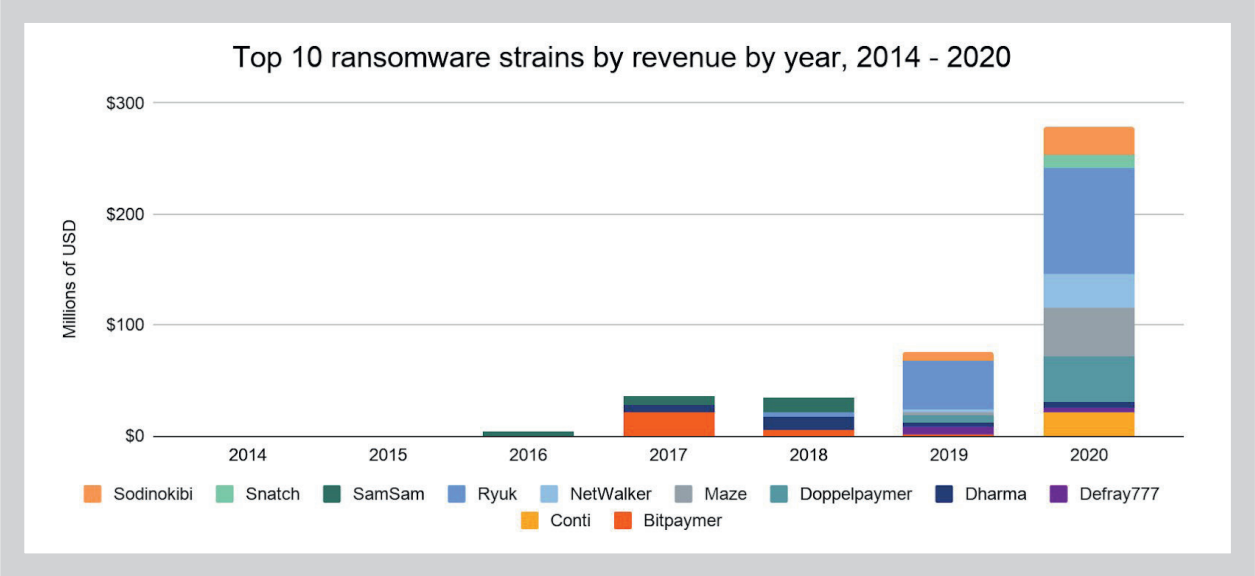
Populäre Fälle (2020/2021)

- ↗ *Colonial Pipeline*
- ↗ *Honda*
- ↗ *Einhell*
- ↗ *Garmin*
- ↗ *University of California*
- ↗ *Ruhr-Uni Bonn*
- ↗ ...



Revenues // src

Teil I – Einleitung



Revenues by strain // src

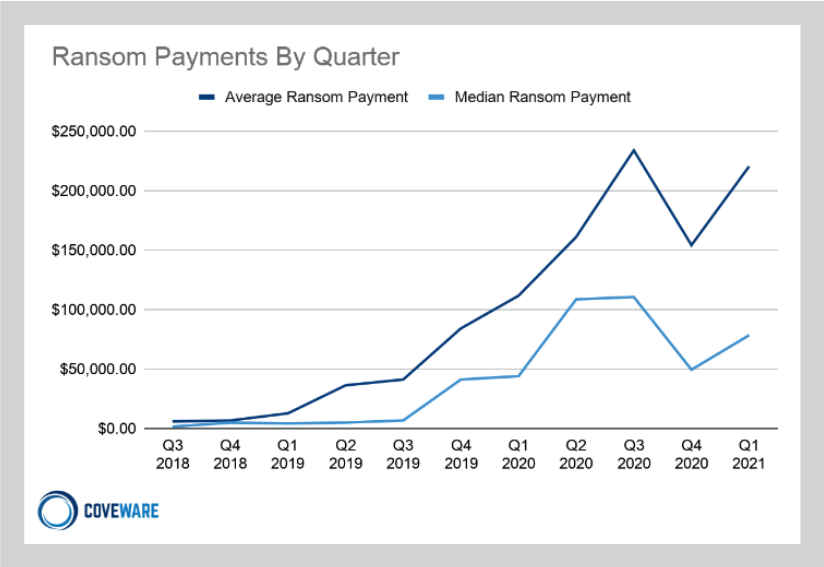
Dieses Erfolgsmodell hat für einen gehörigen Pullfactor gesorgt: waren im Januar 2020 gerade einmal 6 Gruppen aktiv, so zählt man aktuell 36 Ransomware-Gangs; Tendenz weiter zunehmend.

Der durchschnittliche Ertrag pro Vorfall hat sich von 80.000 $ Ende 2019 auf 220.000 $ knapp verdreifacht.

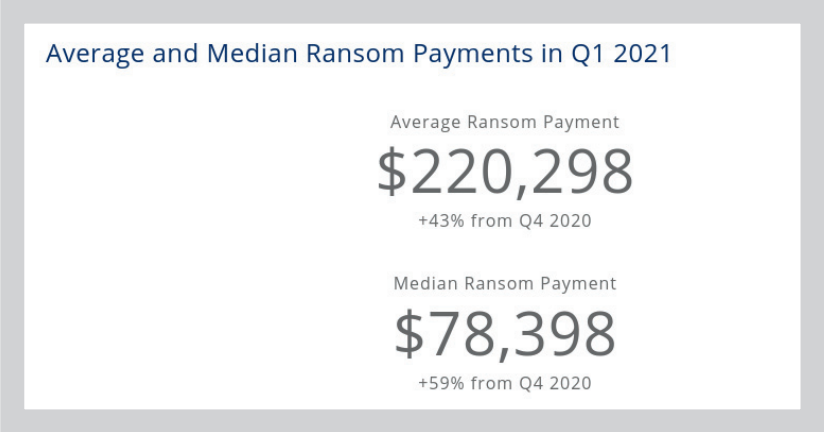
Ein weiterer Trend hat sich 2020 durchgesetzt. Um die Zahlbereitschaft der erpressten Unternehmen zu erhöhen, werden nicht nur die entsprechenden Daten verschlüsselt, sondern vorher kopiert und, sollte das Unternehmen die Erpressungsverhandlungen ablehnen, auf den entsprechenden Leak-Seiten der Gruppe in Auszügen veröffentlicht, zum Teil auch an den Meistbietenden versteigert.

Mehr zu diesem Vorgehen im Teil II.

Teil I – Einleitung



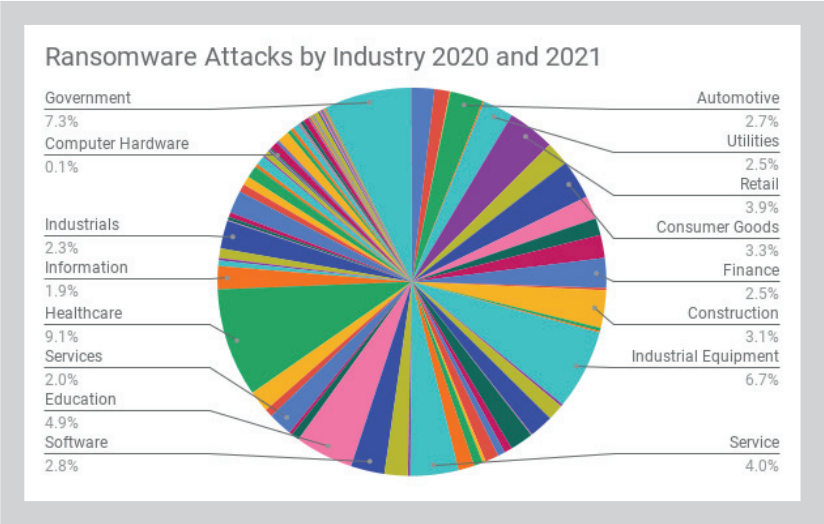
Avg Payment per Incident / Trend // ↗ src



Avg Payment per Incident / Trend // ↗ src

Nach Branchen aufgeschlüsselt läßt sich erkennen, dass es alle und jeden treffen kann.
Gibt es ein Ziel, eine Sicherheitslücke oder leicht mögliches Eindringen, wird zugeschlagen.

Teil I – Einleitung



Ransomware-Vorfälle nach Branchen // ↗ src

Zusammenfassend lässt sich sagen: der Ransomware-Markt wächst weiterhin, und wir sind wahrscheinlich gerade am Anfang der Ransomware-Welle. Wer jetzt seine Hausaufgaben immer noch nicht gemacht hat (siehe Teil III – Schutzmöglichkeiten), bietet sich als Opfer feil.

Um einen ungefähren Eindruck über das weltweite Ausmaß von Ransomware-Vorfällen zu gewinnen, kann man einfach mal die Twitter-Posts von RansomwareMap einer Woche durchscrollen; ein weiterer empfehlenswerter Twitter-Account mit guten Analysen ist DarkTracer.

Teil II: „Operations“ und Verfahren

Ransomware hat sich 2020 als extrem erfolgreiches Businessmodell für Cybercrime erwiesen. Wir wollen das Thema etwas näher beleuchten und dabei auf Hintergründe, Operationsverfahren und potentielle Schutzmöglichkeiten eingehen. Der Fokus liegt dabei auf der IT-Infrastruktur.
Die extreme Zunahme der Ransomware-Aktivitäten geht einher mit einer Verschiebung beim „Initial Acess“, also dem ersten Zugang oder Fuß in der Tür in die betroffenen Unternehmensnetze.

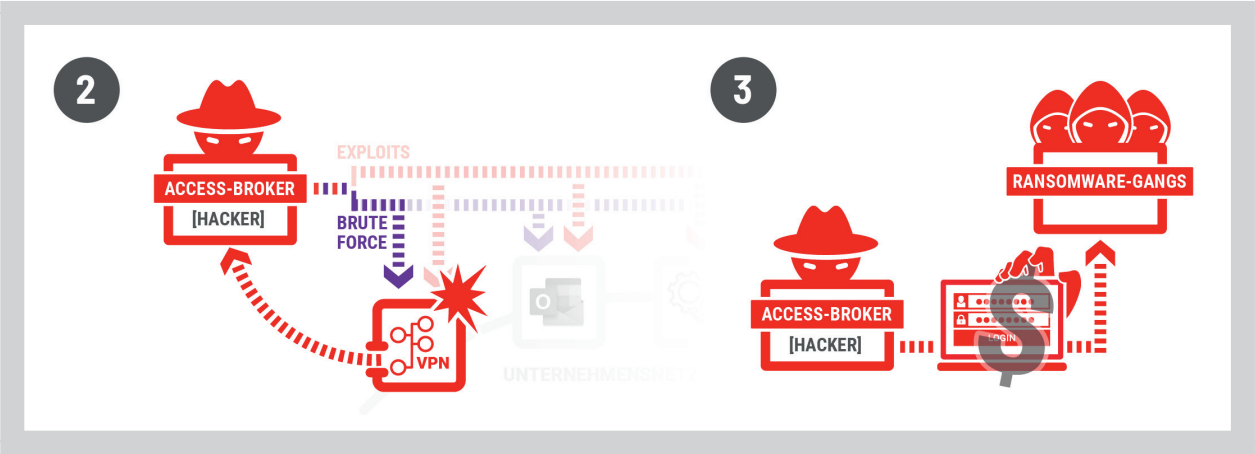
Im Jahr 2019 hat der Trojaner „Emotet“ bei dem Vorfall am Berliner Kammergericht für Schlagzeilen gesorgt; diese Art von Schadsoftware wird meist per Email versandt, benötigt die Interaktion eines Benutzers, und lässt sich mit dem Schuß aus einer Schrotflinte in einen Entenschwarm vergleichen: wenn man Glück hat ist irgendwas getroffen, man weiß aber nie genau, was man trifft.

Diese Situation hat sich im 1. Halbjahr 2020 innert kurzer Zeit geändert. Wir haben im April 2020 schon bemerkt, dass sich Ransomware-Gangs mehr und mehr auf den direkten Netzzugang durch Sicherheitslücken fokussieren, zumal gerade in diesem Zeitraum über 40 kritische Vulnerabilities in Produkten und Appliances publiziert wurden, die vornehmlich in Unternehmensnetzen Einsatz finden (VPN-Gateways, Firewalls, VMware-Management, Automation and Orchestration-Lösungen etc. pp) und bei Exploitation direkten Zugang in das entsprechende Unternehmensnetz gewährten:

- Citrix Sharefile Datenzugriff
- SaltStack RCE
- Fortimail Auth-Bypass
- vCenter RCE
- HAProxy RCE
- Paessler PRTG RCE
- Exchange RCE
- Sophos Firewall RCE
- ...

Im folgenden beleuchten wir etwas genauer die einzelnen Phasen einer erfolgreichen Ransomware-Attacke.

Phase 1 + 2: „Inital Access“ / Zugang legen, Persistenz



Inital Access - Vektoren

Das Ziel der ersten Phase eines Angriffs ist es, überhaupt erst einmal Zugang zu einem Unternehmensnetz zu erhalten.

Wie vorab erwähnt, haben sich die initialen Angriffsvektoren hierfür vom Trojaner-Versand via Email auf den Zugang via RDP oder direktes Ausnutzen von Sicherheitslücken in der IT-Infrastruktur verlagert. Spezialisiert auf den „Initial Access“ haben sich so genannte „Access Broker“, die das Internet kontinuierlich nach Schwachstellen scannen oder via RDP-BruteForce an Zugangsdaten gelangen.

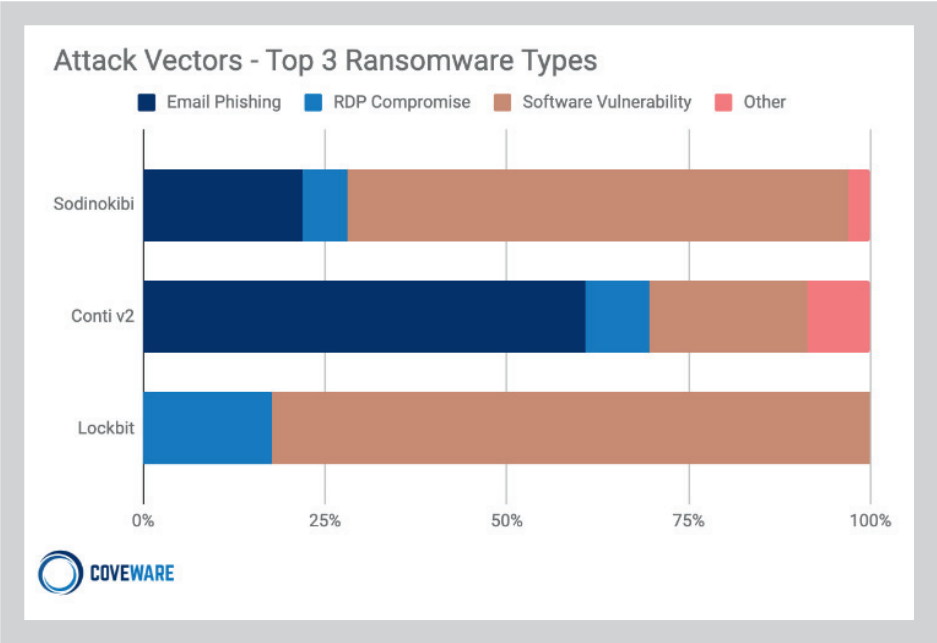
Phase 1 + 2: „Inital Access“ / Zugang legen, Persistenz

Rops-2 // src

Rops-3 // ↗ src

Phase 1 + 2: „Inital Access“ / Zugang legen, Persistenz

Attack Vectors used by the Top 3 Ransomware Variants



Attack-Vectors by Top 3 Gangs // ↗ src

Bestätigt wird dieser Trend durch eine Analyse der NSA as dem Q3/2021, in dem aufgezeigt wurde, auf welche Wege sich Angreifer Zugriff auf Netze zwecks Datenklau und/oder Ransomware verschafft haben.

Vulnerability Identifier	Affected Application	Reported
CVE-2019-0604	Microsoft® SharePoint®[15]	15 May 2019 [8]
CVE-2019-19781	Citrix®[16] Gateway, Citrix® Application Delivery Controller, and Citrix® SD-WAN WANOP appliance	22 Jan 2020 [9]
CVE-2019-3396	Atlassian® Confluence®[17] Server	20 May 2019 [10]
CVE-2019-3398	Atlassian® Confluence Server and Atlassian® Confluence Data Center	26 Nov 2019 [11]
CVE-2019-9978	WordPress®[18] “Social Warfare” Plugin	22 Apr 2019 [12]
CVE-2019-18935 CVE-2017-11317 CVE-2017-11357	Progress® Telerik®[19] UI	7 Feb 2019 [13]
CVE-2019-11580	Atlassian® Crowd and Crowd Data Center	15 July 2019 [14]
CVE-2020-10189	Zoho® ManageEngine®[20] Desktop Central	6 Mar 2020 [15]
CVE-2019-8394	Zoho® ManageEngine® ServiceDesk Plus	18 Feb 2019 [16]
CVE-2020-0688	Microsoft® Exchange®[21] Server	10 Mar 2020 [17]
CVE-2018-15961	Adobe® ColdFusion®[22]	8 Nov 2018 [18]

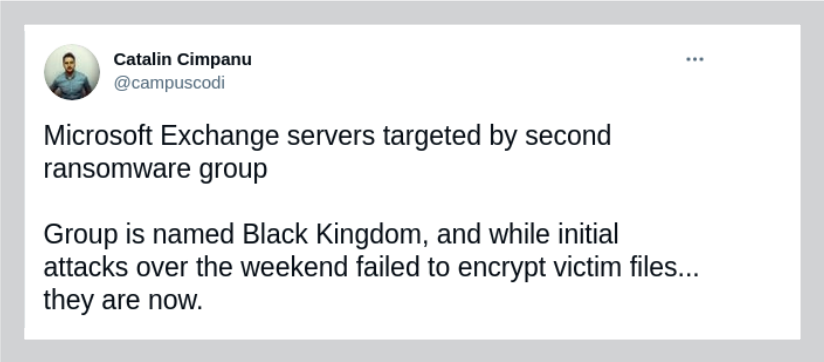
Attack-Vectors, analyzed // ↗ src

Phase 1 + 2: „Inital Access“ / Zugang legen, Persistenz

In der 2. Phase wird dafür gesorgt, dass der langfristige Zugang zum Unternehmensnetz gewährt bleibt (Persistenz); dies kann auf unterschiedliche Wege geschehen:

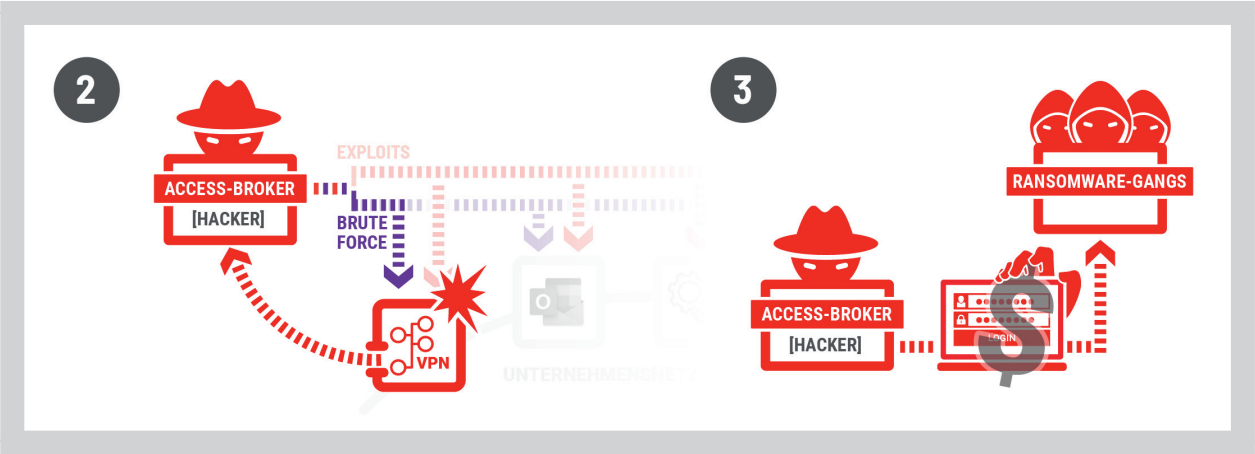
- Anlegen von weiteren privilegierten Accounts (Privilege Escalation)
- Implantieren von Backdoors oder Webshells

Gerade der letzte Fall hat bei der Exchange-Lücke aus dem März 2021 gezeigt, wie schnell die Access-Broker agieren: innerhalb von 3 Tagen nach dem Release des Advisories waren auf einer Großzahl von Systemen Backdoors zu finden.



src

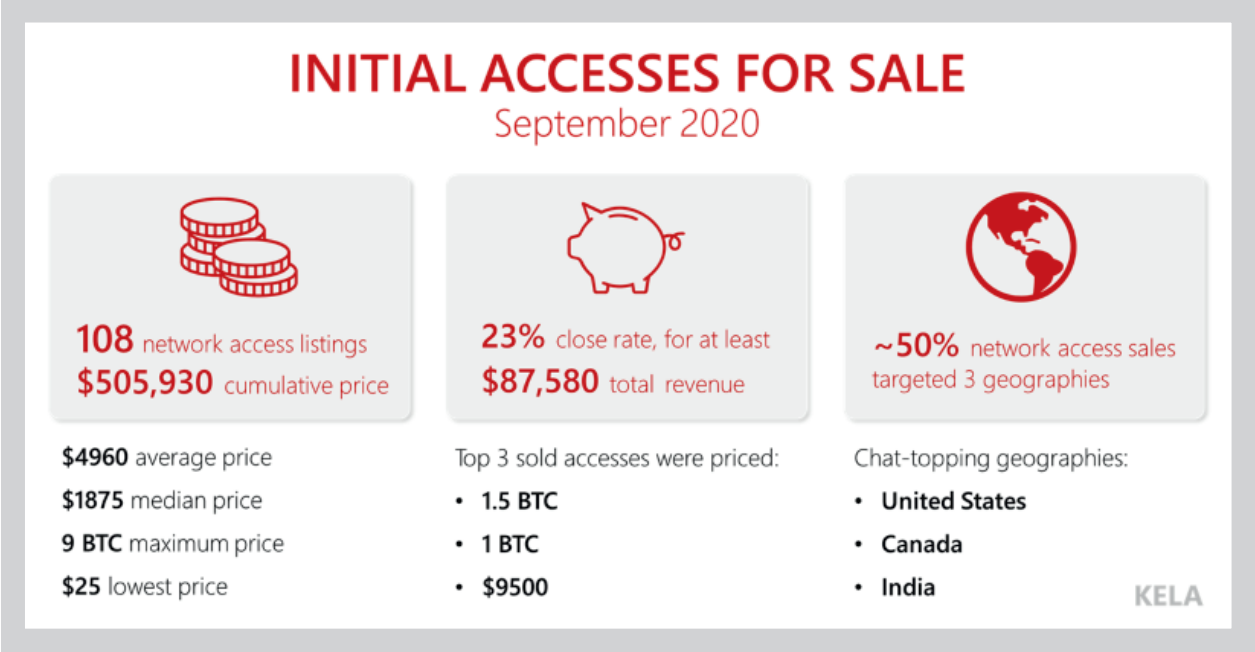
Phase 3: Verkauf an Ransomware-Gangs



Verkauf der Zugänge

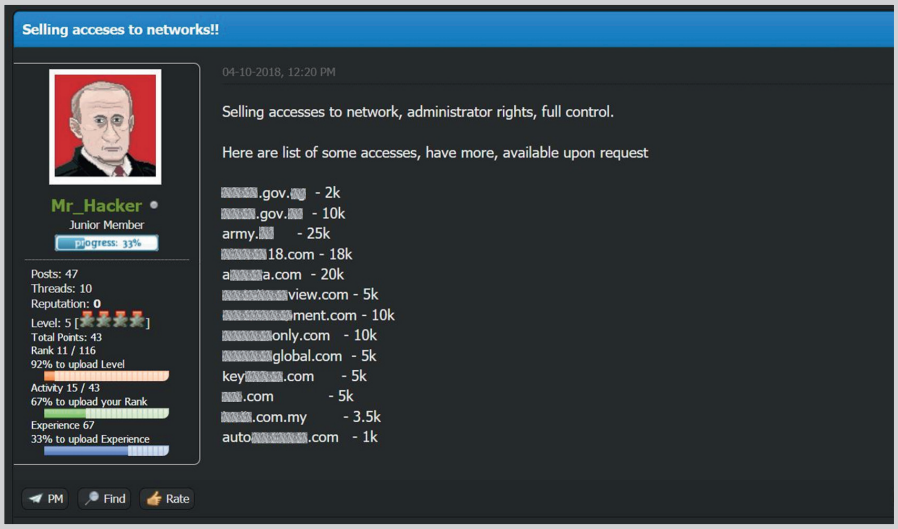
Im Phase 3 wird der mit Persistenz versehene Zugang in speziellen Darknet-Foren verkauft.

Aufgrund der Vielzahl an Sicherheitslücken und der explosionsartig gestiegenen Nachfrage stehen jederzeit hunderte Systeme zur Auswahl; der UAS-Market, auf dem RDP- und VPN-Zugänge gehandelt werden, listed für die Jahre 2019 + 2020 1.3 Mio Accounts zu vorwiegend Firmennetzen, die dort gehandelt wurden.



Initial-Access-Market // ↗ src

Phase 3: Verkauf an Ransomware-Gangs



Broker-Ad in einem Darknet-Forum // ↗ src

UAS-RDP-Darkent-Forum // ↗ src

Phase 4: Ausleiten der Daten (Data-Exfil)

Daten kopieren

Nachdem der persistente Zugang zum Unternehmensnetz vom Access-Broker an eine Ransomware-Gang verkauft wurde, kann diese zu einem späteren Zeitpunkt auf das Unternehmensnetz zugreifen und den Zugang „monetarisieren“.

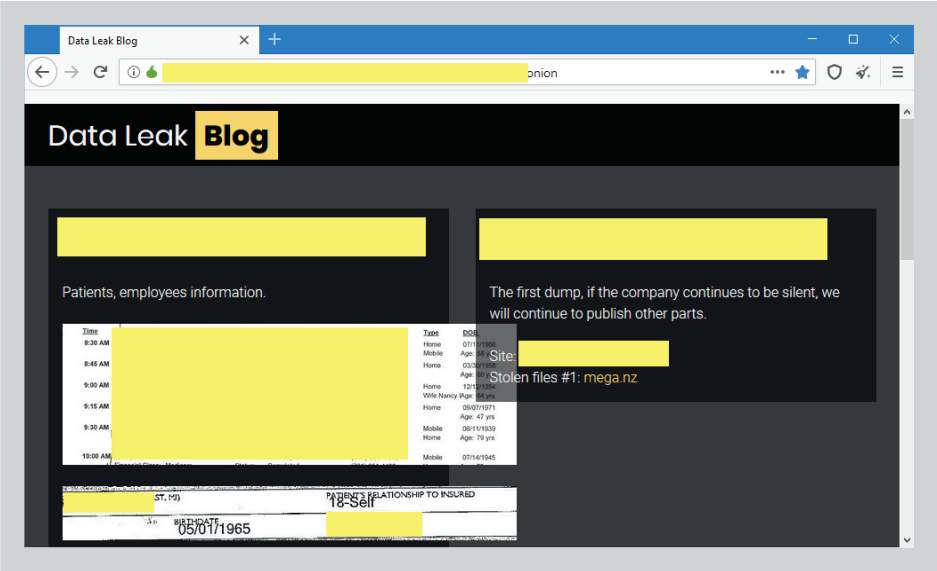
Die Zeitspanne zwischen dem „Initial Access“ und der eigentlichen Ransomware-Operation beträgt im Schnitt 3-6 Monate, kann aber in ↗ ausgewählten Fällen auf wenige Wochen schrumpfen.

Wenn die Angreifer sich etwas im Unternehmensnetz umgesehen und die datentechnischen Krownjuwelen gefunden haben, werden diese kopiert und auf Systeme der Angreifer übertragen.

Diese Methode hat sich im Laufe des Jahres 2020 etabliert. Die betroffenen Unternehmen werden neben der eigentlichen Verschlüsselung zusätzlich damit erpresst werden, dass so erbeutete, sensitive Daten veröffentlicht werden.

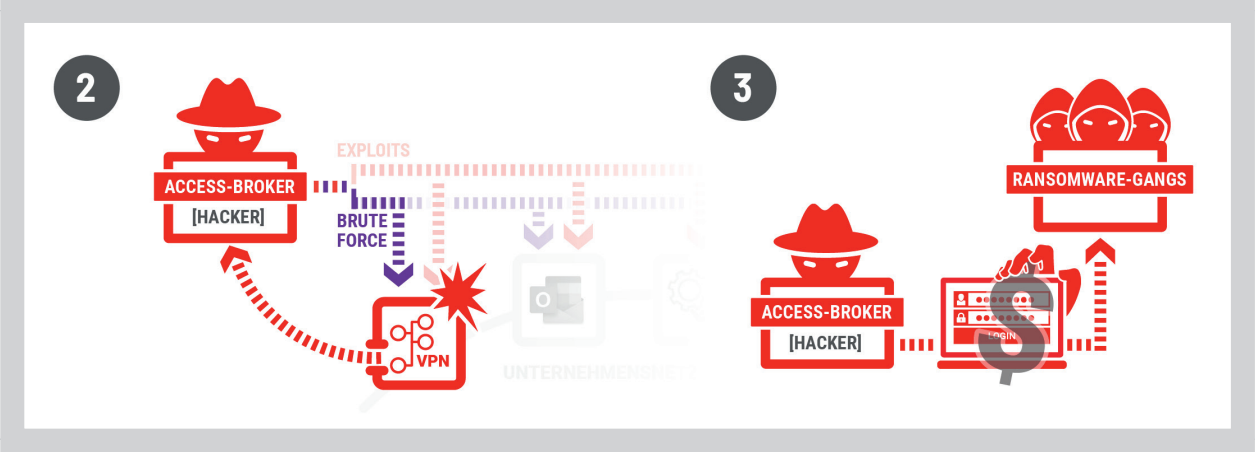
Dieser Zwischenschritt wurde eingefügt, um einen Hebel gegen Unternehmen zu haben, die ihre Daten und Systeme aus Backups wiederherstellen können und nicht auf die Erpressung reagieren.

Phase 4: Ausleiten der Daten (Data-Exfil)



Leak-Blog // ↗ src

Phase 5 + 6: Verschlüsselung und Erpressung



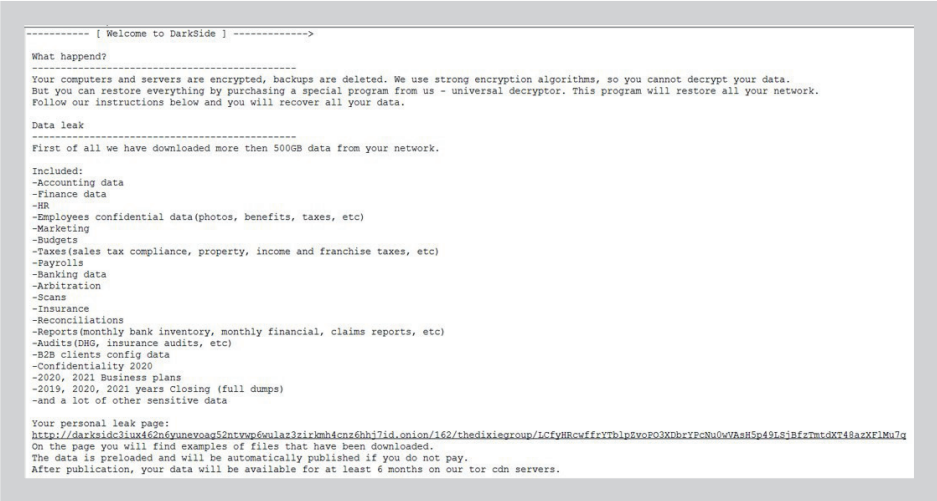
Daten kopieren

Im finalen Phase werden die Unternehmensdaten und teilweise auch komplette Systeme verschlüsselt, was häufig zu einem sofortigen Systemstillstand führt. Gleichzeitig wird dem Unternehmen die Erpressungsnachricht zugeleitet, oder diese werden von den infizierten Systemen selber angezeigt.

Ransomware gangs are abusing VMWare ESXI exploits to encrypt virtual hard disks

Ransomware goes ESXi // ↗ src

Phase 5 + 6: Verschlüsselung und Erpressung



```
---------- [ Welcome to DarkSide ] ------------>

What happend?
---------------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
---------------------------------------------------
First of all we have downloaded more then 500GB data from your network.

Included:
-Accounting data
-Finance data
-HR
-Employees confidential data(photos, benefits, taxes, etc)
-Marketing
-Budgets
-Taxes(sales tax compliance, property, income and franchise taxes, etc)
-Payrolls
-Banking data
-Arbitration
-Scans
-Insurance
-Reconciliations
-Reports(monthly bank inventory, monthly financial, claims reports, etc)
-Audits(DHG, insurance audits, etc)
-B2B clients config data
-Confidentiality 2020
-2020, 2021 Business plans
-2019, 2020, 2021 years Closing (full dumps)
-and a lot of other sensitive data

Your personal leak page:
http://darksidc3iux462n6yunevoag52ntvwp6wulaz3zirkmh4cnz6hhj7id.onion/162/thedixiegroup/LCfyHRcwffrYTblpZvoPO3XDbrYPcNuOwVAsH5p49LSjBfzTmtdXT48azXFlMu7q
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
```

Ransom-Nachricht

Sollte das Unternehmen nicht innerhalb einer gesetzten Frist auf die Erspressungsnachricht reagieren und Kontakt aufnehmen (meist 3 – 7 Tage), veröffentlicht die Ransomware-Gang auf ihrem Blog mindestens eine Nachricht, dass das Unternehmen erfolgreich angegriffen wurde – meist auch einen Auszug der erbeuteten Daten, um den Druck auf das Unternehmen zu erhöhen.

Diese Leak-Blogs, die mittlerweile Standard in der Ransomware-Szene sind (siehe auch hier) kann man nur über das TOR-Netzwerk erreichen.

Eine alternative Zweitverwertung ist die Versteigerung der Unternehmensdaten.

Die eigentlichen Verhandlungen finden über anonyme Chats statt. Hierbei gehen die meisten Gangs methodisch vor, da sie vor allem ein Ziel haben: mit diesem Kunden Geld zu verdienen und mit dem nächsten auch. Sollten die Verhandlungen nicht innerhalb einer Woche zum Erfolg führen bzw. das betroffene Unternehmen weder Willens noch in der Lage sein, die geforderte Summe aufzubringen, werden diese abgebrochen und die Unternehmensdaten wie angedroht veröffentlicht. Bei erfolgreicher Verhandlung bekommt das Unternehmen den passenden Decryptor, um den regulären Betrieb wieder herzustellen. Die illegalerweise kopierten Dateien werden auf Seiten der Erpresser gelöscht.

Dieser letzte Schritt, das Löschen der Dateien, geschieht natürlich auf Vertrauensbasis. Bisher sind aber bei den größeren Ransomware-Gangs noch keine Vorfälle bekannt, dass kopierte Daten an anderer Stelle aufgetaucht sind. Entsprechende Fälle mögen bei kleineren, eher unbekannten, Gangs möglich sein, entsprechend nicht funktionierende Decryptoren, sind aber eher nicht zu erwarten, da die Ransomware-Gangs ihr ansonsten erfolgreiches Businessmodell selbst torpedieren würden.

Phase 5 + 6: Verschlüsselung und Erpressung

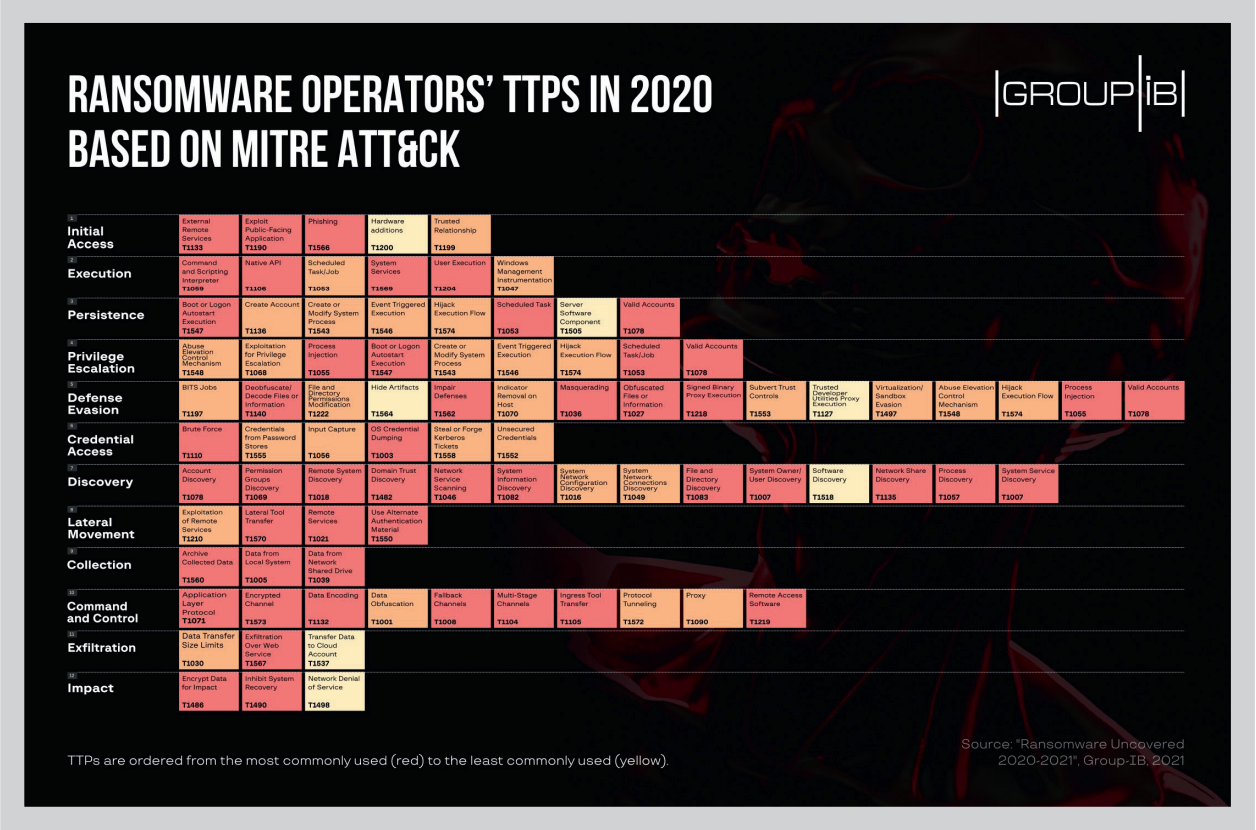
Daten kopieren

Dass die meisten Ransomware-Gangs mittlerweile hochprofessionell agieren, zeigen nicht nur die gestiegenen Umsätze, sondern auch die folgende Übersicht über jeweils beobachtete Methoden, basierend auf der MITRE ATT&CK-Matrix.

Wer darüber hinaus Interesse an Interna hat, dem seien an dieser Stelle mehrere Artikel empfohlen, die detaillierten Einblick in die Szene geben:

- ↗ Alleged REvil member spills details on group's ransomware operations
- ↗ „I through the trash heaps… now I'm a millionaire:" An interview with REvil's Unknow
- ↗ Million-dollar deposits and friends in high places: how we applied for a job with a ransomware gang
- ↗ Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Phase 5 + 6: Verschlüsselung und Erpressung



Operations matched to MITRA ATT&CK // src

Teil III – Schutzmöglichkeiten

Den 3. Teil der Ransomware-Serie, der sich mit möglichen Schutzverfahren beschäftigt, möchten wir mit einem Statement von ↗ Florian Roth beginnen:

Why we lose it // ↗ src

Ein Teil des Problems, warum Ransomware über den Angriffsvektor IT-Infrastruktur so erfolgreich ist und aktuell nur partiell, aber nicht in der Fläche einzudämmen sein wird, liegt sicherlich u.a. an dem Punkt, dass die besten Methoden dazu (Asset- und Patchmanagement, Überwachen der Angriffsoberfläche, Hardening, Defense in Depth, Durchsetzen von Best-Practice-Emfpehlungen) viel Disziplin in ihrer stetigen Durchführung benötigen und somit von den aktuell angepriesenen Vorgehensweisen ThreatIntel, ThreatHunting, AI-Driven-Defense eher in den Schatten gedrängt werden.

Teil III – Schutzmöglichkeiten

Gegenmaßnahmen // ↗ src

Die wichtigsten Punkte, um sich gegen Infrastruktur-basierte Ransomwareattacken zu schützen, an dieser Stelle kurz zusammengefasst:

- ↗ Reduzierung und Monitoring der externen Angriffsoberfläche, z.B. über ein Tool wie LUUP
- ↗ reibungsloses Patch-Management und unverzügliches Einspielen von Sicherheitspatches
- ↗ 2FA für alle Accounts, die von aussen auf das Unternehmensnetz zugreifen müssen (VPN, ApplicationManagement, Mail, ...)
- ↗ Web/Application-Proxies für ausgehenden Traffic
- ↗ Application-Whitelists auf allen Systemen
- ↗ Inspiration: ↗ **1**, ↗ **2**, ↗ **3**

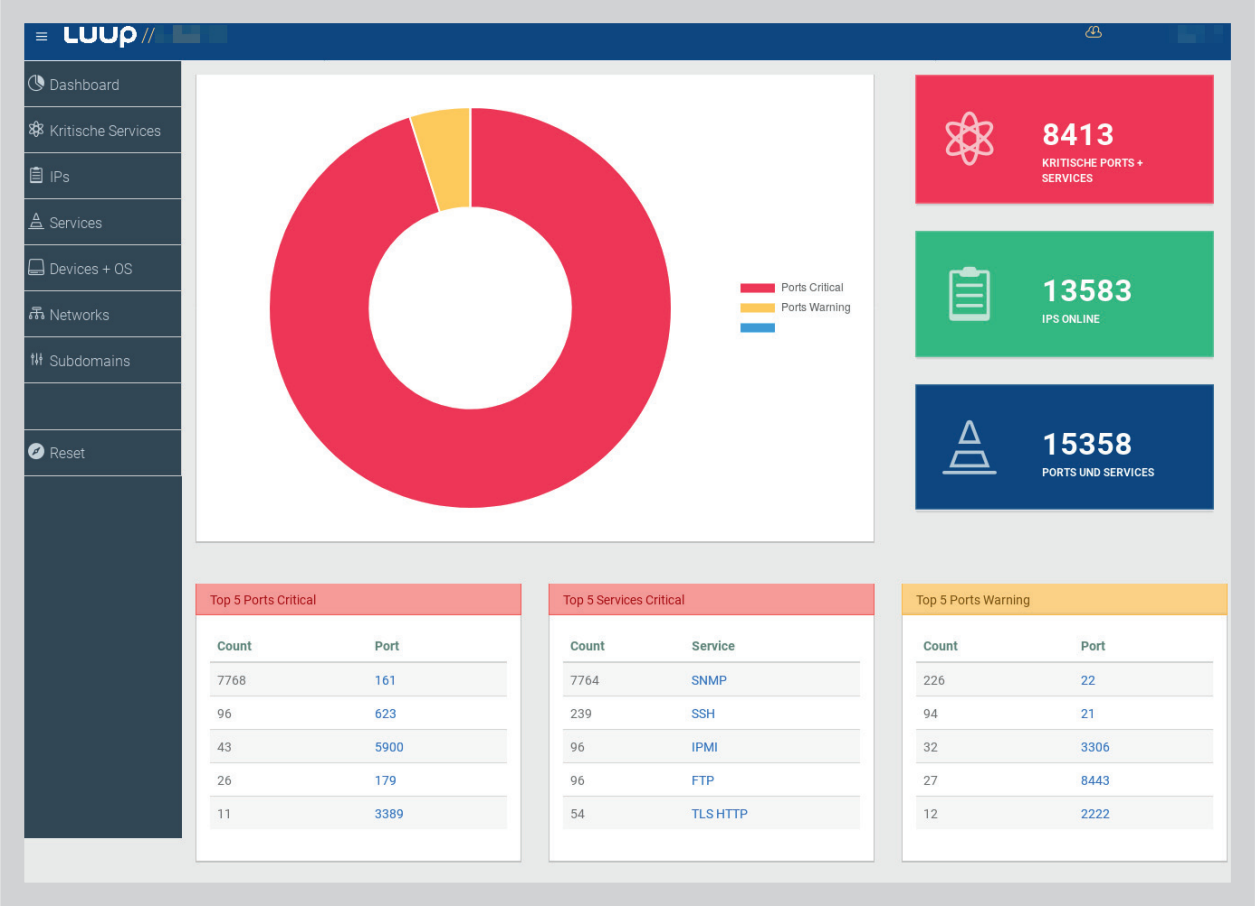
Ziel muss es sein, die externen Angriffspunkte soweit zu reduzieren, dass das Risiko einer potentiellen Attacke minimiert wird.

An den Punkten, an denen externe Dienste angeboten werden müssen, führen bewährte Praktiken, die man unter dem Oberbegriff „Defense in Depth“ zusammenfassen kann, meist zur Eindämmung einer potentiellen Kompromittierung (DMZ, Netzsegmentierung, Least-Priviledge-Prinzip, Application-Whitelists, Logging, SIEM etc.).

Teil III – Schutzmöglichkeiten

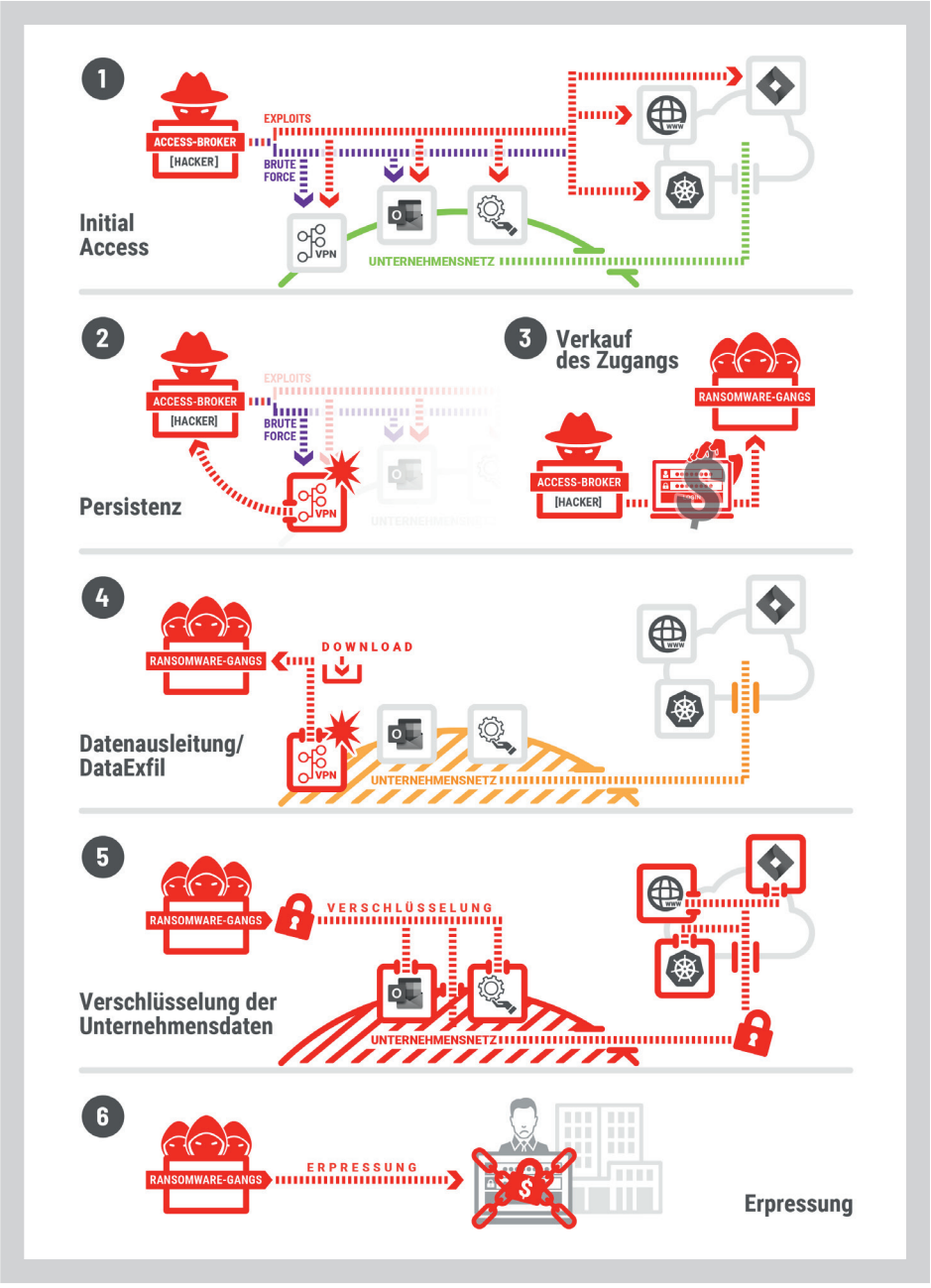
Wie im Teil 2 herausgearbeitet, operieren die Ransomware-Gangs professionell und effizient. Und da mehr als genug Ziele vorhanden sind, reicht es statistisch gesehen aus, wenn man keine von außen potentiell angreifbaren Systeme betreibt oder diese, sofern sie notwendig sind, im Falle von Exploitwellen, so schnell wie möglich patcht.

Die Ransomware-Gangs werden immer den Weg nehmen, der schnell und direkt zum Erfolg führt.



AttackSurfaceMonitoring mit LUUP // ↗ src

Teil IV – Addendum



Ransomware-Angriff - Ablauf

Teil IV – Addendum

Populäre Vorfälle

- Colonial Pipeline
- Honda
- Einhell
- Garmin
- University of California
- Ruhr-Uni Bonn
- ...

Links und Informationen

- TheRecord/Number of victims
- Ransomware goes Infrastruktur: eine Analyse
- DarkTracer - Ransomware - Monitoring
- RansomMap - Ransomware - Monitoring
- Million-dollar deposits and friends in high places: how we applied for a job with a ransomware gang
- The Week in Ransomware - September 25th 2020 - A Modern-Day Gold Rush
- REvil ransomware deposits $1 million in hacker recruitment drive
- CISA RANSOMWARE GUIDE
- Sophos: The State of Ransomware 2021
- Accellion data breaches drive up average ransom price
- Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound
- Berlins Kammergericht muss nach einem Cyber-Angriff vom Netz
- Exchange-Lücke für Ransomware-Angriffe ausgenutzt
- Hackers Breached Colonial Pipeline Using Compromised Password
- Hacker verteilen Ransomware über Sicherheitslücke in Citrix-Servern
- ‚Network access' sold on hacker forums estimated at $500,000 in September 2020
- Ransomware gangs are abusing VMWare ESXi exploits to encrypt virtual hard disks
- The Secret Life of an Initial Access Broker
- Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay

Teil IV – Addendum

- Group-IB Ramsonware-Report 2020/2021
- Alleged REvil member spills details on group's ransomware operations
- 'I scrounged through the trash heaps… now I'm a millionaire:' An interview with REvil's Unknown
- Million-dollar deposits and friends in high places: how we applied for a job with a ransomware gang
- Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom
- Ransomware Prevention | Practical Steps to Reducing Your Attack Surface
- ReadTeam defensive Settings
- Low Level Malware Protection
- True costs of Ransomware