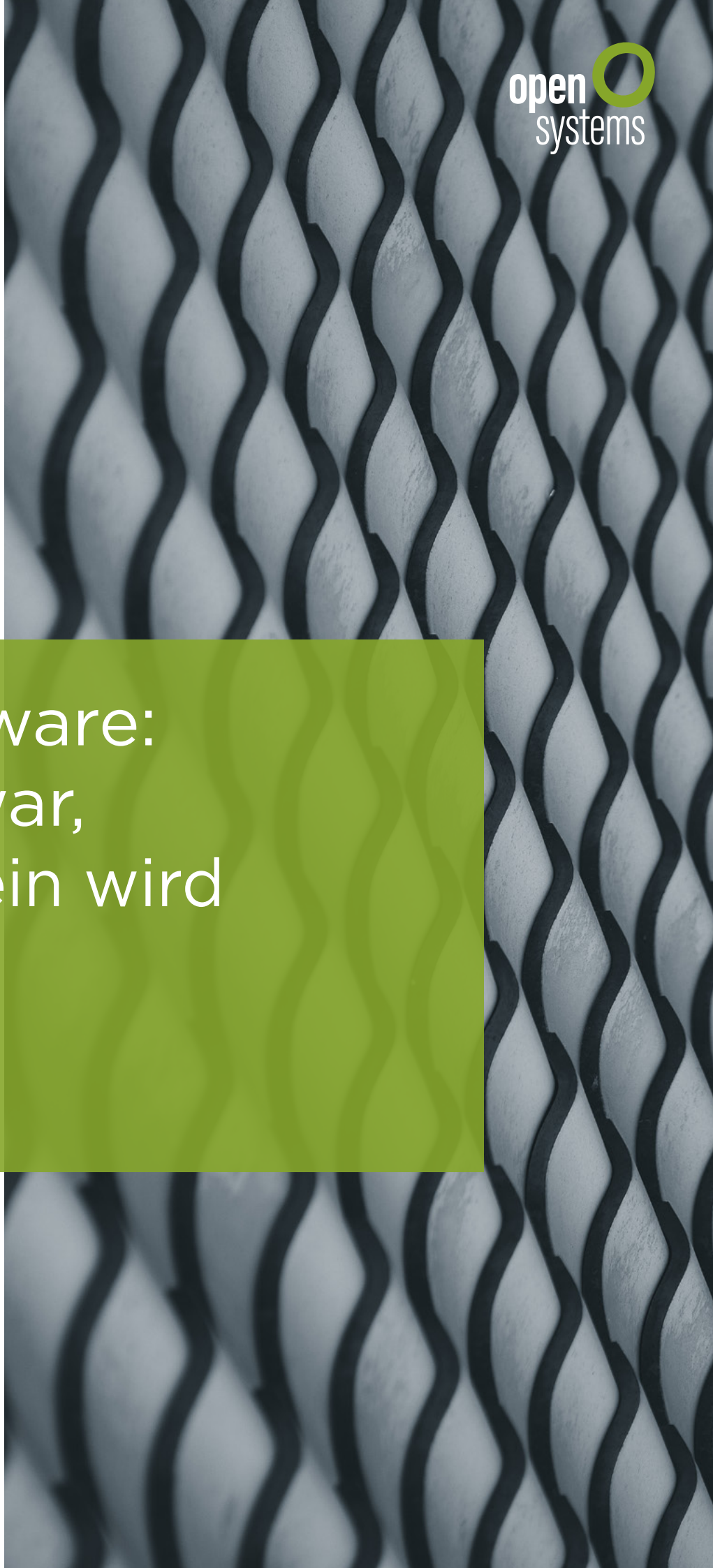

WHITE PAPER

Ransomware: Wie es war, ist und sein wird

Open Systems services are ISO 27001 certified.

Alle 14 Sekunden fällt irgendwo auf der Welt ein Unternehmen einer Ransomware-Attacke zum Opfer. Was ist Ransomware und warum bereitet sie IT-Experten zunehmend schlaflose Nächte?

Einfach erklärt: Ein bösartiger Akteur schleust einen Virus auf ein Gerät ein, oft via Phishing, der entweder Dateien verschlüsselt, versteckt, den Zugriff darauf verweigert oder den Benutzer ganz aus seinem System aussperrt. Der Angreifer fordert dann eine Zahlung für die Wiederherstellung des Daten- oder Systemzugriffs. Bei einem Angriff auf ein Unternehmen kann sich die Malware auch lateral von System zu System bewegen, so lange bis Sie sämtlichen Zugriff auf kritische Daten und Dienste in Ihrer Organisation verlieren.

Ransomware bisher: Von bescheidenen Anfängen zum riesigen Problem

Es handelt sich hierbei um eine Form der Cyberkriminalität, die vor dem Internet bereits aufkam. Die ersten Erpressungsversuche dieser Art gab es mittels AIDS-Trojaner (PC Cyborg Virus) auf Disketten. Ein Biologe erstellte 1989 den bösartigen Code und verteilte 20'000 infizierte «AIDS Information» Disketten an die Teilnehmer einer AIDS-Konferenz der World Health Organization. Diejenigen, die unglücklicherweise die Diskette in ihren Computer einlegten, wurden mit einem Trojaner infiziert. Nachdem der Rechner eine bestimmte Anzahl von Neustarts durchgeführt hatte, versteckte der Virus Adressbücher und verschlüsselte die Namen aller Dateien. Dadurch wurde das System unbrauchbar und auf dem Bildschirm erschien die Aufforderung zur Zahlung einer «Software-Leasing» Gebühr (Abb. 1). Um das Ganze zu entschlüsseln, mussten die Opfer ein Lösegeld von 189 US-Dollar per Post an das Postfach der PC Cyborg Corporation in Panama senden.

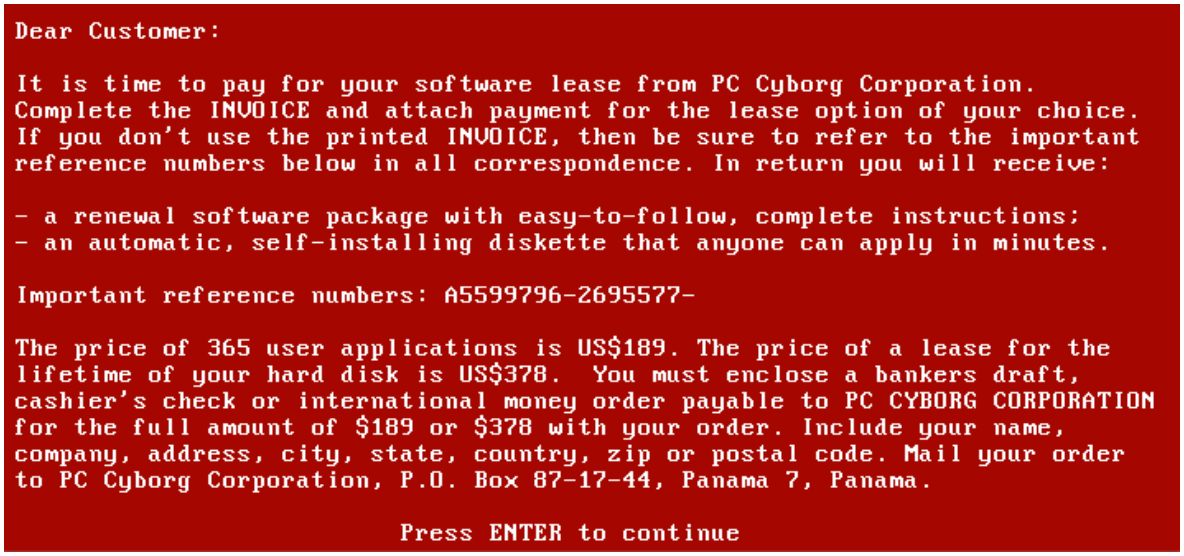

Abb. 1 – Die erste bekannte Ransomware – der AIDS-Trojaner (PC Cyborg Virus)

Dieser Angriff erscheint nach heutigen Massstäben fast schon kurios. Wenn es die Opfer heute immer noch nur 189 Dollar kosten würde, wäre Ransomware keine so grosse Sache. Doch die Zeiten von Disketten und Lösegeldern an Postfächer sind längst vorbei. Die heutigen Cyberverbrecher nutzen ausgeklügelte Online-Angriffsvektoren und Bitcoin als sofortige und meist anonyme Zahlungsmöglichkeit.

Ransomware heute: Smarter, schneller und teurer

In den letzten Jahren haben viele Angriffe Unternehmen und Organisationen des öffentlichen Sektors getroffen, die es einen sechsstelligen Betrag oder mehr kostete. Im Herbst 2020 warnten beispielsweise das FBI und zwei weitere Bundesbehörden in einer gemeinsamen Meldung US-Krankenhäuser und Gesundheitsdienstleister vor einer «erhöhten und unmittelbar bevorstehenden Bedrohung durch Cyberkriminalität». Die Warnung besagte, dass Cyberkriminelle Gruppen den Sektor angreifen, um «Datendiebstahl und Unterbrechung von Gesundheitsdiensten» zu erzielen.

Eine Ransomware Gruppe namens Ryuk hatte innerhalb einer Woche mindestens fünf US-Krankenhäuser infiziert. Im September 2020 legte ein ähnlicher Angriff die Datensysteme aller 250 US-Einrichtungen der Krankenhauskette Universal Health Services lahm. Dieser Angriff führte zu chaotischen Zuständen und wurde von Mitarbeitern als «Beeinträchtigung der Patientenversorgung» beschrieben. Dazu gehörten lange Wartezeiten in der Notaufnahme und der Ausfall von Krankenhaussystemen, wie. z. B. drahtlose Geräte, die zur Überwachung der Vitalwerte von Patienten verwendet werden. In Deutschland starb mindestens eine schwerkranke Person aufgrund Ryuk bedingter Störungen.

Hold Security, die Ryuk verfolgt, sagte zur Zeit aus, dass die Gruppe Lösegelder von weit über 10 Millionen Dollar pro Angriff verlangte. Dieselbe Gruppe wurde dabei erwischt, wie sie im Dark Web Pläne diskutierte, mehr als 400 Krankenhäuser, Kliniken und andere medizinische Einrichtungen zu infizieren.

Eine wachsende Bedrohung für Organisationen jeder Grösse

Die durchschnittlichen Kosten für Ausfallzeiten aufgrund eines Ransomware-Angriffs übersteigen oft den Betrag des Lösegelds um beinahe das 50-fache.

Obwohl der Gesundheitssektor den Löwenanteil der Angriffe ausmacht (45 %), ist keine Organisation sicher vor Ransomware. Im Jahr 2020 wurde beispielsweise Garmin, ein Hersteller von GPS-Software und -Hardware mit einem Jahresumsatz von mehreren Milliarden, von Cyberkriminellen mittels einer grossen Ransomware-Attacke angegriffen. Die Attacke stellte die Dienste offline. Berichten zufolge zahlte das Unternehmen Lösegeldforderungen von mehreren Millionen Dollar an Dritte (sog. Ransomeware Negotiation Business), um die Systeme wieder online zu bringen.

Grosse Unternehmen mit solch tiefen Taschen sind jedoch nicht die einzigen Organisationen, die gefährdet sind. Die Auswirkungen von Ransomware-Angriffen auf kleine und mittelständische Unternehmen nehmen ebenfalls zu. Im Jahr 2019 waren die durchschnittlichen Kosten für Ausfallzeiten bei Angriffen auf kleine und mittlere Unternehmen (KMUs) 94 % höher – und fast sechsmal höher als 2018 – von 46'800 US-Dollar auf 274'200 US-Dollar in 2 Jahren, wie eine erneute Untersuchung von Datto ergab. Heute ist Ransomware die grösste Cyberbedrohung für KMUs.

Hinzu kommen die enormen Kosten für Geschäftsunterbrechungen und die Wiederherstellung von Systemen nach einem Ransomware-Vorfall. So übersteigen die durchschnittlichen Kosten für Ausfallzeiten durch einen Ransomware-Angriff oft den tatsächlichen Lösegeldbetrag um beinahe das 50-fache, ganz zu schweigen von der enormen Beschäftigung der IT-Teams. 34 % der von Malware betroffen Unternehmen benötigen eine Woche oder länger, um wieder Zugriff auf ihre Daten zu erhalten (Quelle: Kaspersky).

Auch Ransomware entwickelt sich ständig weiter. So behauptete der AIDS-Trojaner zwar die Dateien der Opfer zu verschlüsseln, tatsächlich chiffrierte er aber nur die

Dateinamen mit einer rudimentären Verschlüsselung. In den späten 2000er Jahren waren die Schöpfer der Ransomware CryptoLocker in der Lage, starke 2048-Bit-RSA-Verschlüsselungen mit öffentlichen und privaten Schlüsseln zu erzeugen, um Dateien zu sperren. Die Verschlüsselung von CryptoLocker ist so stark, dass ein durchschnittlicher Computer mehr als 14 Milliarden Jahre bräuchte, um ein 2048-Bit-Zertifikat zu knacken.

Darüber hinaus erhöhen Ransomware-Angreifer den Einsatz durch eine Reihe neuer Taktiken, die Folgendes beinhalten:

- Fokus auf gemeinsame Netzlaufwerke
- Einschleusen von Easter Eggs, die für eine bestimmte Zeit lang ruhen, bevor sie aktiviert werden
- Löschen von Windows Shadow Copy Dateien
- Angriffe auf cloudbasierte Infrastructure-as-a-Service gespeicherte Dateien
- Unterbrechung kritischer IT-Infrastrukturen wie Web- und Anwendungsserver
- Lancieren von Angriffen auf Managed Service Provider (MSPs) und Cloud Service Provider, um die Anzahl der Opfer zu maximieren
- Löschen von Backup-Dateierweiterungen

Um Ransomware weiter zu verbreiten, gehen heutige Cyber-Erpresser von den herkömmlichen, ungezielten Phishing-Angriffen über zur organisierten Grosswildjagd. Wie beim «Spear-Phishing» hat diese Praxis den Fokus auf Gemeinden, grosse Unternehmen oder Krankenhäuser. Gut finanzierte Angreifer, motiviert durch die Aussicht auf einen grossen Zahltag, entwickeln Ransomware für genau diese Ziele. Die Verursachung des Maximalschadens dient einzig und allein zur unsäglich erhöhten Lösegeldforderung.

Zum konventionellen Ansatz der Benutzerdatenverschlüsselung, kommt der Datendiebstahl hinzu. Eine erweiterte Strategie des Datendiebstahls ist nicht nur die Verwendung von Malware zur Exfiltration sensibler Daten, sondern auch die Androhung einer Meldung an Aufsichtsbehörden oder sogar Börsen über die Datenverletzung, die das Opfer erlitten hat. Auf diese Weise hoffen die Kriminellen, schnellere und grössere Lösegeldzahlungen zu erzwingen. Diese Technik wurde laut SecureList bereits von Ransomware-Familien wie Maze, REvil/Sodinokibi, DoppelPaymer und JSWorm/Nemty/Nefilim übernommen.

Eine Liste der gängigen Ransomware-Gruppierungen und die jeweiligen Techniken finden Sie im Anhang.

Geschäftsunterbrechungen führen zu Ausfallzeiten oder kompletter Schliessung

Von Compliance-Risiken über Datenverluste bis hin zu Ausfallzeiten: Die Kosten eines Ransomware-Angriffs können richtig wehtun. Oktober 2020 beispielsweise erlitt der Möbelhersteller Steelcase einen Ransomware-Angriff durch die Ryuk-Bande, welcher das Unternehmen zwang beinahe den gesamten Betrieb für zwei Wochen einzustellen.

Während ein grosses Unternehmen wie Steelcase (13'000 Mitarbeiter und 3,75 Milliarden US-Dollar Jahresumsatz) eine grössere Betriebsunterbrechung überstehen kann, können für kleine und mittlere Unternehmen (KMUs) solche Ausfälle mehr als nur ein vorübergehender Schluckauf bedeuten; sie können eine existenzielle Bedro-

hung darstellen. In den letzten Jahren haben sich viele kleinere Unternehmen aus verschiedenen Gründen für die Einstellung ihres Betriebs entschlossen. Entweder ihnen fehlten die Mittel für die Zahlung der Lösegeldforderung zur Wiederbeschaffung ihrer Daten, sie konnten die Ausfallzeit nicht verkraften, oder es fehlte an Ressourcen die IT-Infrastruktur wiederaufzubauen. Im Jahr 2019 war beispielsweise Brookside ENT & Hearing Services mit Sitz in Michigan der erste Gesundheitsdienstleister in den USA, der seinen Betrieb dauerhaft einstellen musste, nachdem Ransomware sein elektronisches Krankenakten-System infiziert hatte.

Compliance-Problem:
Die Zahlung von Lösegeldern kann in den USA zu staatlichen Strafen führen

In einer neuen Wendung haben staatliche Aufsichtsbehörden die Überwachung von Ransomware-Zahlungen verschärft. Unternehmen, die Lösegeldzahlungen leisten und Finanzinstitute, die solche Gelder überweisen, könnten sich Ärger mit zwei Vollstreckungsorganen des US-Finanzministeriums einhandeln. Am 1. Oktober 2020 veröffentlichten das Office of Foreign Assets Control (OFAC) und das Financial Crimes Enforcement Network (FinCEN) eine Mitteilung zu den potenziellen Sanktions- und Anti-Geldwäsche-Risiken bei der Durchführung oder Vermittlung von Ransomware-Zahlungen. Auch wenn viele IT-Führungskräfte noch nie etwas von OFAC oder FinCEN gehört haben, können diese mächtigen Aufsichtsbehörden strenge Strafen verhängen und Unternehmen und Einzelpersonen auf Sperrlisten setzen.

Die OFAC-Sanktions- und AML-Compliance-Vorschriften sind äusserst kompliziert. Dennoch lassen sie sich im Wesentlichen auf zwei Punkte reduzieren:

Erstens verlangen die AML-Gesetze in den USA bei Finanztransaktionen ab einem bestimmten Dollarbetrag sowohl Angaben zum Absender als auch zum Empfänger. Jeder, der grössere Banküberweisungen tätigt, hat diese Anforderung schon einmal gesehen. Das Problem ist: Cyberkriminelle wollen offensichtlich anonym bleiben. Dies ist ein Hauptgrund dafür, dass Datenentführer die Bezahlung in Kryptowährung wie Bitcoin verlangen. Die pseudo-anonyme Natur der Blockchain macht die Informationen des Empfängers in einer Kryptowährungstransaktion unerkennbar – zumindest ohne Anwendung ausgefeilter Blockchain-Analysen.

Während neue Richtlinien von Finanzinstituten und Kryptowährungsbörsen verlangen, die sogenannte «Geld-Reise-Regel» einzuhalten, hat die Branche noch keinen technologisch machbaren Weg gefunden, Sender- und Empfängerinformationen über die Blockchain zu teilen. Nichtsdestotrotz sollte jede Organisation, die eine Lösegeldzahlung in Bitcoin in Erwägung zieht, die rechtlichen Implikationen einer anonymen Zahlung prüfen.

Zweitens werden viele Ransomware-Schemata von Personen verübt, die versuchen, Terrorismus, Massenvernichtungswaffenprogramme und andere ruchlose Aktivitäten zu finanzieren. In der OFAC-Beratung wird darauf hingewiesen, dass die Behörde eine Reihe von Ransomware-Angreifern als «Specially Designated Nationals» (SDNs) und «Blocked Persons» eingestuft hat. US-Bürgern ist es generell untersagt, mit SDNs zu handeln. Das bedeutet, dass Sie zivilrechtlich haftbar gemacht werden können, auch wenn Sie nicht wussten oder keinen Grund hatten zu wissen, dass Sie eine Transaktion mit einem SDN oder einer gesperrten Person durchführen. Interessanterweise betrachtet die OFAC die Meldung des Angriffs an die Strafverfolgungsbehörden als strafmildernden Faktor.

All dies veranschaulicht nur einen Teil der Schwierigkeiten, mit denen Unternehmen im Umgang mit einem Ransomware-Angriff konfrontiert sind. Es mag auch erklären, warum Unternehmen wie Garmin auf Dritte zurückgreifen, um mit Kriminellen zu verhandeln. Die Opfer stehen vor einem schwierigen Dilemma: Sie zahlen das Lösegeld nicht und verlieren den Zugriff auf wichtige Daten und Systeme, oder sie zahlen das Lösegeld und geraten möglicherweise in Konflikt mit der US-Regierung, weil sie gegen US-Sanktions- und AML-Gesetze verstossen.

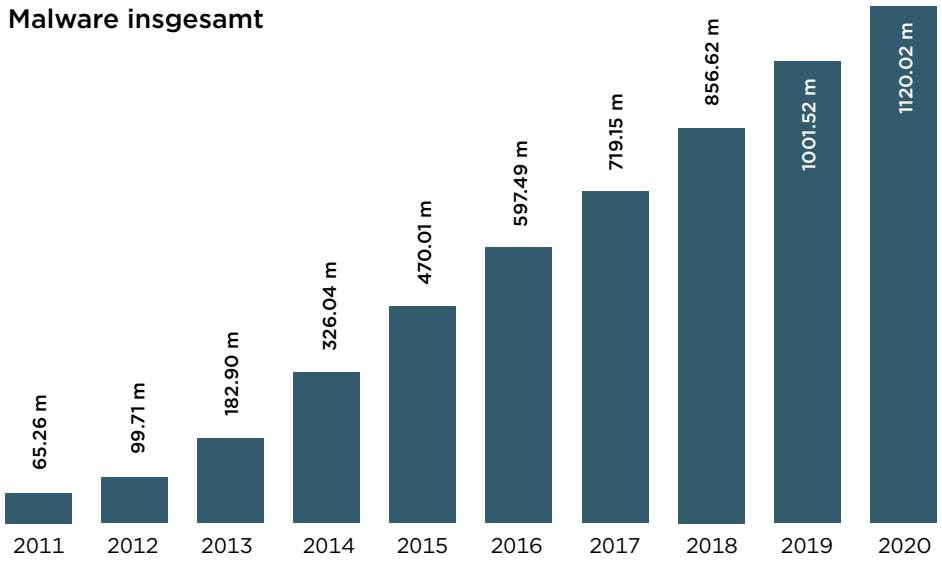

Abb. 2 – Quelle: AV-Test, www.av-test.org
Stand: 23. November 2020

Ransomware-Risiko verläuft parallel zur wachsenden Bedrohung durch Malware

Das unabhängige AV-TEST-Institut überwacht neue Schadprogramme (Malware) und potenziell unerwünschte Anwendungen (PUA). Nach ihren Daten sind die Sichtungen dieses riskanten Codes in freier Wildbahn auf über 350'000 pro Tag gestiegen, was ein explosives Wachstum der gesamten Malware in den letzten zehn Jahren darstellt (Abb. 2). Darüber hinaus handelt es sich bei 85 % der Malware-Infektionen bei Organisationen im Gesundheitswesen um Ransomware.

Infolgedessen müssen sich IT-Organisationen gegen Malware zur Wehr setzen. Ransomware ist nicht nur eine der teuersten Formen von Malware, sondern auch eine der am schwierigsten abzuwehrenden.

Wie Ransomware funktioniert

Ransomware verwendet eine Reihe von Angriffsvektoren, um auf einen Computer zuzugreifen. Phishing-Scams sind jedoch die häufigsten Übertragungswege. Diese gefälschten E-Mails enthalten oft bösartige Anhänge oder URLs, die sich beim Empfänger als vertrauenswürdig ausgeben. Sobald die ahnungslosen Opfer draufklicken, können die bösen Akteure ihren Computer übernehmen. Einige der raffinierteren Schemata, wie z. B. das Big Game Hunting, nutzen Social Engineering, um Benutzer dazu zu bringen, administrativen Zugriff zu erlauben.

Andere, aggressivere Formen von Ransomware nutzen Brute-Force-Angriffe, die Schwachstellen in der Cyberabwehr ausnutzen und Computer infizieren, ohne dass Benutzer ausgetrickst werden müssen. Ryuk beispielsweise verbreitet sich in erster Linie durch andere Malware, die sie auf einem bereits infizierten System ablegen. Das Auffinden des Droppers auf einem System zur Analyse ist schwierig, da die Hauptnutzlast nach der ersten Ausführung gelöscht wird.

Im Allgemeinen läuft ein Ransomware-Angriff in fünf Phasen ab.

Phase 1: Einschleusung

Im ersten Schritt eines Ransomware Angriffs verwendet der Erpresser in der Regel Techniken wie Social Engineering, um den Rechner mit einem kleinen Codeschnipsel zu infizieren, einem sogenannten Dropper. Dafür gibt es folgende Methoden:

- **Phishing E-mails:** 93 % der Phishing-E-Mails enthalten Ransomware. Wenn ein ahnungsloser Benutzer auf einen Anhang in einer dieser gefälschten E-Mails klickt, beginnt der Angriff oft mit dem Öffnen einer ausführbaren Datei, z.B. einer Word- oder Excel-Datei mit eingebetteten Makros. Die Makros können dann gegebenenfalls das PowerShell-Skript verwenden, um die Malware herunterzuladen.

- **Drive-by Downloads:** Benutzer können auch unabsichtlich einen Virus oder Malware auf einen Computer oder ein mobiles Gerät herunterladen. Angreifer nutzen in der Regel eine Schwachstelle in einem veralteten Webbrowser, einer veralteten App oder einem Betriebssystem mit einer Sicherheitslücke aus.

- **Watering Hole Angriff:** Bei dieser Art der strategischen Webkompromittierung laden die Angreifer bösartigen Code auf harmlos aussehende Websites, die von einer Zielgruppe von End-Usern besucht werden. Das Gerät des Opfers wird allein durch den Besuch der Website infiziert.

- **USB-Laufwerke und tragbare Geräte:** USB-Speichersticks, tragbare Computer und Mobiltelefone sind gängige Übertragungswege für Ransomware. Durch das Anschliessen eines infizierten Geräts kann die Ransomware nicht nur den lokalen Rechner verschlüsseln, sondern die Malware möglicherweise auch über das Netzwerk verbreiten.

Phase 2: Installation

Sobald die Ransomware installiert ist, beginnt der Angriff. Der Dropper kommuniziert über die Kommandosteuerung des Kriminellen, und wenn er einen Befehl erhält, lädt er die eigentliche Malware herunter und installiert sie.

Phase 3: Erkundung

In dieser Phase erkennt die Malware Merkmale des Zielsystems – sowohl des Hosts als auch des Netzwerks. Diese Erkundung kann die Identifizierung des Betriebssystems, der installierten Anti-Malware-Software, des Browsers, des Domain-Namens und der IP-Adresse sowie der Art der Dateien, die der Kriminelle verschlüsseln möchte, beinhalten.

Die Erpresser bauen dann mit der Ransomware einen Befehls- und Kontrollkanal auf, um die Vorgänge auf dem Rechner des Opfers zu steuern. Sie können die gleichen

Protokolle wie bei der webbasierten Kommunikation verwenden, indem sie ein unverschlüsseltes HTTP unterstützen oder eingebettete Tor-Dienste nutzen, um eine verdeckte Kommunikation aufzubauen.

Phase 4: Verschlüsselung

In der Verschlüsselungsphase wird die Ransomware aktiv und beginnt, Dateien zu verschlüsseln oder den autorisierten Benutzer aus dem System auszusperren. Die gefährlicheren Ransomware Gruppen verschlüsseln nicht nur Dateien, sondern verschlüsseln auch Dateinamen, um deren Wiederherstellung zu verhindern. Bei einem Angriff auf Unternehmen verwenden sie auch das SMB-Protokoll für Netzwerkfreigaben und bewegen sich lateral, wo sie sowohl Server als auch Hosts infizieren. Einige der verheerendsten Ransomware-Angriffe in der Geschichte wiesen dieselben Selbstverbreitungsmechanismen auf, darunter WannaCry, Petya und SamSam (siehe Anhang A für weitere Informationen).

Phase 5: Lösegeld

Sobald die Verschlüsselung erfolgreich durchgeführt wurde, fordern die Erpresser eine Zahlung. Sie geben dreisterweise sogar Tipps, wie man Kryptowährung für die Lösegeldzahlung kaufen kann. Ein aktueller Bericht von Gartner gibt drei Empfehlungen, wie Sicherheits- und Risikomanagementverantwortliche, die für Endpunkt- und Netzwerksicherheit zuständig sind, sich auf alle Phasen von Ransomware-Angriffen konzentrieren müssen:

- Bereiten Sie sich auf Ransomware-Angriffe vor, indem Sie eine Strategie zur Vorbereitung auf einen Vorfall entwickeln. Diese Strategie sollte Backups, Asset-Management und die Wiedereinschränkung von Benutzerrechten beinhalten. Bestimmen Sie, ob die Organisation letztendlich bereit ist, ein Lösegeld zu zahlen oder nicht.

- Implementieren Sie Erkennungsmassnahmen, indem Sie Verhaltensanomalie-basierte Erkennungstechnologien einsetzen, um Ransomware-Angriffe zu identifizieren.

- Erstellen Sie Reaktions-Prozesse für die Zeit nach einem Vorfall, indem Sie Mitarbeiter schulen und regelmässige Tests durchführen.

Best Practice zur Verhinderung oder Einschränkung eines Ransomware-Angriffs

Ransomware zählt zu der schwierigsten Form der Attacke für diejenigen, die mit dem Schutz kritischer Datensysteme, Dienste und Netzwerke betraut sind. Laut Sophos haben 90 % der Unternehmen, die mit Ransomware infiziert wurden, einen aktuellen Endpoint-Schutz installiert.

Eine wichtige erste Abwehrlinie ist der Mensch. E-Mail-Kampagnen für Spear-Phishing und ähnliche Methoden Opfer zu täuschen, werden zur Verbreitung von Ransomware als Hauptmittel genutzt. Laut Symantecs aktuellem Internet Security Threat Report (ISTR) sind jedoch 80 % der Unternehmen nicht davon überzeugt, dass ihre Mitarbeiter via E-Mail verbreitete Ransomware erkennen und abwehren können.

90 % der mit Ransomware infizierten Unternehmen verwendeten zum Zeitpunkt der Attacke einen aktuellen Endpoint-Schutz.

Sophos, Januar 2020

Implementieren Sie Erkennungsmass-nahmen, indem Sie auf Anomalien basierende Erkennungs-technologien einsetzen, um Ransomware-Angriffe zu identifizieren.

Gartner

Zukunft der Ransomware: Von Risiko nach Widerstandsfähigkeit

Laut Cybersecurity Ventures könnten Ransomware-Angriffe Auswirkungen von gesamthaft über 20 Milliarden Dollar nach sich ziehen – und die Gesamtverluste durch Cyberkriminalität überhaupt sogar bis zu 6 Billionen Dollar.

Sicherheits- und Risikomanagement (SRM) Experten müssen wissen, wie sie die fortschreitende Bedrohung durch Malware verhindern können. Gartner erklärt, dass «Sicherheitshygiene entscheidend ist für den Schutz vor ‚menschengesteuerter' Ransomware, was eine ganzheitliche Betrachtung des Unternehmens erfordert».

Gartner empfiehlt das MITRE ATT&CK®-Framework zu verwenden, um die Ransomware-Bedrohung je nach Unternehmen einzuschätzen. Diese weltweit zugängliche Sammlung aus realen Taktiken und Techniken von Angreifern kann zur Entwicklung spezifischer Bedrohungsmodelle und -methoden verwendet werden.

Für die Vorbeugung, Schadensbegrenzung und Wiederherstellung nach Ransomware-Angriffen gibt es Massnahmen, die vom gesunden Menschenverstand bis hin zu fortschrittlichen Technologien reichen. Einige bewährte präventive Massnahmen sind:

- Sichern Sie zuallererst alle kritischen Daten mit einer Offline-Lösung.
- Verbessern Sie die Cybersicherheitsschulung Ihrer Mitarbeiter – insbesondere in Bezug auf Phishing-Betrug und die Raffinesse der heutigen Social-Engineering-Techniken.
- Halten Sie Betriebssysteme und Anwendungen auf dem neusten Stand.
- Installieren Sie die neusten Sicherheits-Patches, da Ransomware oft auf ungepatchte Systeme zurückgreift.
- Gehen Sie davon aus, dass die Bedrohung 24x7 eintreffen kann, d. h. suchen Sie rund um die Uhr nach Malware.
- Ziehen Sie in Erwägung, Ihre Sicherheitsexperten und Incident Response Teams durch Managed Detection and Response (MDR) zu ergänzen, um Ihre Umgebung von reaktionsfähigen Experten überwachen zu lassen, die mögliche Schäden sofort eingrenzen können.
- Verwenden Sie verschlüsselten Transport, um Remote Access auf Unternehmensressourcen zu schützen.
- Erwägen Sie die Implementierung einer Richtlinie gegen die Ausführung von Makros in nicht vertrauenswürdigen Excel- oder Word-Dateien.
- Implementieren Sie eine starke Authentifizierung für «Privileged Users».
- Protokollieren Sie die Aktivitäten in Ihrer Umgebung, um böswillige Akteure daran zu hindern bekannte Malware zu verwenden und Zugriff auf Zugangsdaten mit höheren Privilegien zu erhalten.

- Verwenden Sie eine moderne Endpoint Detection and Response (EDR) Lösung für Verhaltenserkennung und einer Remediation-Engine, die einen automatischen Rollback von Dateien ermöglicht.
- Fügen Sie Ihrer Endpoint Security Lösung einen EDR-Agenten hinzu, für erweiterte Analysen, Forensik und Bedrohungseindämmung.
- Aktivieren Sie das Remote Desktop Protokoll nur, wenn es notwendig ist oder ändern Sie den RDP-Port vom Standard auf Port 3389.
- Installieren Sie keine Software und geben Sie keine administrativen Rechte, wenn Sie nicht genau wissen, welche Implikationen es hat.
- Setzen Sie Blocklisting-Software ein, die verhindern kann, dass nicht autorisierte Anwendungen ausgeführt werden.
- Stellen Sie sicher, dass Sie den ursprünglichen Bedrohungsvektor des Angriffs verstehen und aktualisieren Sie die Sicherheitskontrollen entsprechend. Wenn Sie nicht verstehen, wie der Angreifer das Ziel ursprünglich kompromittiert hat, wird er zurückkehren und denselben Vektor wieder nutzen.

Zusammenfassung

Ransomware ist eine der am schwierigsten zu stoppenden Cyberbedrohungen. Da die Kosten für Ausfallzeiten und Problembehebungen die Lösegeldkosten oft weit übersteigen, sollten Sie zuallererst sicherstellen, dass alle kritischen Systeme über zuverlässige und automatische Backup-Verfahren verfügen. Ausserdem sollten diese Backup-Systeme vollständig vom Netzwerk isoliert sein.

Es zahlt sich aus, alarmbereit zu sein. Nutzen Sie die Möglichkeiten eines MDR-Services, um Ihre Umgebung rund um die Uhr zu überwachen. Indem Sie die verräterischen Anzeichen einer Ransomware-Bedrohung frühzeitig erkennen, können Sie den Angriff nach der Dropper-Infektion stoppen und die Ausführung verhindern. Wenn Sie Ransomware früh in der Cyber Kill Chain erkennen, können Sie auch das weitere Einschleusen von Ransomware stoppen und die Auswirkungen maximal eingrenzen.

Es ist sehr unwahrscheinlich, dass die Auswirkungen eines Ransomware-Angriffs rückgängig gemacht werden können, sobald die Verschlüsselung oder Systemsperrung ausgeführt wurde. Daher ist es von entscheidender Bedeutung, dass Experten das verfügbare aber sehr kleine Zeitfenster ausnutzen, um Ransomware rechtzeitig zu erkennen.

Wenn Sie Ihr Sicherheitsteam mit dem MDR Service von Open Systems ergänzen, können Sie die wichtigsten Phasen von Ransomware-Angriffen abdecken – von der Vorbereitung eines Vorfalls über die Erkennung bis hin zur Reaktion. Noch wichtiger aber ist die Chance, den Schaden zu verhindern oder zu begrenzen. Die Lösung bietet Experten, die Ihre Umgebung rund um die Uhr überwachen und ergänzt diese menschliche Intelligenz mit fortschrittlichen Tools wie SOAR und auf Verhaltensanomalien basierenden Erkennungstechnologien. Das Ergebnis ist eine kontinuierliche, ganzheitliche Sicht auf Ihr Netzwerk und Ihre Endpunkte, die eine frühzeitige Erkennung von Ransomware zulässt. Diese Transparenz ermöglicht eine schnelle und effektive Reaktion, entweder durch Ihr Incident Response Team oder unsere erfahrenen SOC Analysten.

Anhang: Wichtige Ransomware Gruppen

Der Einfallsreichtum von Kriminellen scheint unbegrenzt zu sein. Das erklärt, warum immer wieder neue und erfinderische Ransomware Gruppen in Netzwerke eindringen. Die nachfolgende Auflistung ist keineswegs vollständig, aber sie gibt einen Eindruck der Strategien und Auswirkungen von Ransomware.

Ryuk

Ryuk-stämmige Ransomware wurde erstmals im August 2018 entdeckt. Sie wurde für massgeschneiderte Angriffe auf Unternehmen entwickelt und verfügt über einige ausgeklügelte Funktionen, wie z.B. das Verschlüsseln und unwiderrufliche Verbergen wichtiger Dateien («unwiderruflich» ohne die Hilfe der Angreifer versteht sich). Diese Fähigkeit ermöglicht es den Bedrohungsakteuren, hohe Lösegeldzahlungen zu verlangen, in der Regel mehrere hunderttausend Dollar.

Zu ihren fortschrittlichen Techniken gehören auch Netzlaufwerke und Ressourcen zu identifizieren und zu verschlüsseln. Ryuk kann Schattenkopien löschen, die auf Endpunkten gespeichert sind und die Windows-Systemwiederherstellungsoption deaktivieren. Infolgedessen können IT-Mitarbeiter die verschlüsselten Dateien nicht wiederherstellen, es sei denn, sie verfügen über ein Offline-Backup. Sie vermeiden auch eine Entdeckung, indem sie alle Dateien löschen, die von dem «Dropper» verwendet wurden. Die forensische Untersuchung der Ursache des Vorfalls wird dadurch erheblich erschwert.

WannaCry

Der WannaCry-Wurm führte zu einem der kostspieligsten und am weitesten verbreiteten Ransomware-Angriffe der Geschichte. Er verbreitete sich im Jahr 2017 schnell auf Computern rund um den Globus (der britische Nationale Gesundheitsdienst war unter anderem erheblich betroffen) und ist heute noch zu sehen.

Der Wurm scheint eine Windows-Schwachstelle ausgenutzt zu haben, von der viele glauben, dass sie zuerst von der US National Security Agency (NSA) entdeckt wurde. Die Sicherheitslücke mit dem Namen EternalBlue nutzt den Microsoft Server Message Block (SMB) 1.0. SMB ist ein Netzwerkprotokoll zur Dateifreigabe, das es Anwendungen auf einem Computer ermöglicht, Dateien zu lesen und zu schreiben sowie Dienste im selben Netzwerk zu suchen. Nach der Infizierung eines Windows-Rechners verschlüsselt WannaCry alle Dateien auf der Festplatte, so dass der Benutzer nicht mehr darauf zugreifen kann, und fordert dann eine Lösegeldzahlung in Bitcoin, um die Daten des Benutzers wieder zu entschlüsseln. Microsoft hat diese Sicherheitslücke inzwischen gepatcht.

CryptoLocker und CryptoWall

Ransomware gibt es in der einen oder anderen Form schon seit zwei Jahrzehnten, aber so richtig bekannt wurde sie erst 2013 mit CryptoLocker. Die Täter des CyrptoLocker-Schemas erpressten Millionen an Lösegeldzahlungen von den Opfern, und der Name wurde fast zum Synonym für Ransomware. Nachdem das ursprüngliche CryptoLocker-Botnet im Mai 2014 abgeschaltet wurde, erschien sein Cousin CryptoWall im Jahr 2014 unter verschiedenen Namen und Varianten, wie z.B. CryptoWall 2.0. Die inzwischen weit verbreitete Verschlüsselungs-Malware, die Dateien gegen Lösegeld sperrt, zeigte 2020 eine aktualisierte Version. Sobald sie sich auf dem Gerät eines Opfers installiert hat, verschlüsselt sie Dateinamen und löscht Systemwiederherstellungspunkte, wodurch es fast unmöglich wird, die Daten in ihrem zuvor gespeicherten Zustand wiederherzustellen.

GrandCrab

GrandCrab ist eine weniger berüchtigte Gruppe, machte aber im Jahr 2020 fast 8 % der gesichteten Ransomware aus. Merkwürdig daran ist, dass am 31. Mai 2019 die Erpresser hinter der Malware ankündigten, dass sie ihren Betrieb einstellen. «Alle guten Dinge kommen zu einem Ende», hiess es in einem Beitrag in einem Cybercrime-Forum. Seit dem Start im Januar 2018 haben die GrandCrab-Autoren nach eigenen Angaben mehr als 2 Milliarden US-Dollar eingenommen, und es war Zeit für den «wohlverdienten Ruhestand».

MedusaLocker

MedusaLocker stellt sicher, dass gemappte Netzlaufwerke zugänglich sind, löscht Schattenvolumenkopien, entfernt Backups und deaktiviert die automatische Startup-Reparatur von Windows. Nach der Verschlüsselung schläft das Programm, bevor es nach weiteren zu verschlüsselnden Dateien sucht. Ausserdem erstellt es geplante Prozesse, die das Programm jede halbe Stunde neu starten.

Petya und NotPetya

Wired bezeichnete Petya als die verheerendste Cyberattacke der Geschichte. Die Ransomware begann sich am 27. Juni 2017 rund um den Globus zu verbreiten, und schon bald waren 76 Häfen weltweit geschlossen und fast 800 Seeschiffe sassen auf dem Trockenen – fast ein Fünftel der weltweiten Schifffahrtskapazität. Ganze Rechenzentren wurden innerhalb von Sekunden nach dem Auftreten der Malware ausgelöscht und legten Unternehmen und Regierungen lahm.

Petya zielt auf Windows-Server, PCs und Laptops ab und nutzt dabei dieselbe Server Message Block-Schwachstelle, die auch von WannaCry genutzt wurde, um sich auf ungepatchten Geräten zu verbreiten. Nachdem sie die Schwachstelle ausgenutzt hat, verschlüsselt Petya den Master Boot Record und andere Dateien. Anschliessend sendet sie eine Nachricht an den Benutzer, um einen Systemneustart durchzuführen, woraufhin das System unzugänglich wird. Petya verwendet auch eine Technik zum Diebstahl von Anmeldeinformationen, um auch ungefährdete Rechner zu infizieren.

Während die Petya-Malware eine lange Geschichte hat, brachte der Angriff 2017 eine neue Variante hervor – NotPetya. Diese Ransomeware verhielt sich anders, war aber genauso zerstörerisch.

RobinHood

RobinHood machte von sich reden, als sie die Stadt Baltimore dazu veranlasste, zahlreiche Server und Netzwerke herunterzufahren, um die Verbreitung der Ransomware zu verhindern. Die Erpresser forderten die Stadt auf, ein Lösegeld von 100'000 US-Dollar in Bitcoin zu zahlen. Ähnlich wie andere Ransomware enthielt sie einen Timer und verlangte von den Opfern, bis zu einem bestimmten Datum zu zahlen, sonst würden die Kosten für die Wiederherstellung der Dateien um 10'000 Dollar pro Tag steigen. Sie wird über unsichere Remote-Desktops oder Trojaner verbreitet und verschlüsselt jede Datei mit einem einzigartigen Schlüssel.

Locker Gaga

Im Jahr 2019 warnte das FBI US-Organisationen vor Locker-Gaga-Ransomware-Angriffen. Die Malware kontrolliert das Netzwerk einer Organisation über Exploits, Phishing-Angriffe, SQL-Injections und gestohlene Anmeldedaten. Anschliessend versucht sie, alle Netzwerkgeräte zu verschlüsseln. Cyberkriminelle infizieren das Gerät eines Opfers in der Regel mit LockerGaga-Code, warten dann aber mehrere Monate, bevor sie die Ransomware tatsächlich einsetzen. Sobald ein Angriff beginnt, stoppen die Kriminellen die Sicherheitsprogrammprozesse und -dienste eines infizierten Geräts und deaktivieren die Windows Defender-Scanfunktionen und alle sicherheitsbezogenen Dienste.

SamSam

Die Kriminellen hinter SamSam haben den Einsatz mehrerer Software-Tools – manchmal über Tage hinweg – verfeinert, um so viele Computer wie möglich in einer Organisation zu infizieren. Während dieser langen Zeitspanne setzt die Ransomware ausgeklügelte Techniken ein, um im Netzwerk des Opfers unbemerkt zu bleiben, sich also quasi zu verstecken. Während die meisten Angriffe auf den Gesundheitssektor abzielen, ist SamSam der Übeltäter hinter einer Reihe bemerkenswerter Angriffe auf Kommunalverwaltungen, wie z. B. der berüchtigten City of Atlanta Siege.

Forensische Untersuchungen zeigten, dass SamSam sich über anfällige JBoss-Hostserver Zugang zu den Netzwerken verschafft hat. Sobald die SamSam-Gruppe auf dem Host ist, nutzt sie ausgiebig die Taktik des «living off the land»: die Verwendung von Betriebssystemfunktionen oder legitimen Netzwerkadministrations-Tools, um die Netzwerke der Opfer zu kompromittieren. Diese Taktik wird häufig von Spionagegruppen verwendet, um sich im Zielnetzwerk unauffällig zu verhalten. Indem sie ihre Aktivitäten wie legitime Prozesse aussehen lassen, hoffen sie, nicht entdeckt zu werden.