INTSIGHTS
A RAPID7 COMPANY

Die Ransomware-Bedrohung:

Was Verantwortliche in Unternehmen über Datenlecks wissen sollten

Das Wort „Ransomware" löst bei den meisten Unternehmen Angst aus – unabhängig von der Größe, dem Standort oder der Branche. Doch das war nicht immer so. Die Firmen begannen erst in den letzten Jahren damit, sich vor Ransomware zu schützen, indem sie sich um Datensicherung kümmerten. Back-ups ermöglichen es ihnen, den Betrieb nach einem Angriff wiederherzustellen.

Doch bei vielen Praktiken im Bereich der Datensicherheit und Schutz vor Ransomware herrscht bei den meisten Unternehmen noch Nachholbedarf. Die heutigen Bedrohungen gehen weit darüber hinaus, Firmen offline zu schalten und eine Zahlung für die Wiederherstellung des Betriebs zu verlangen. Jetzt geht es um die Daten.

In diesem Whitepaper beleuchten wir die Geschichte von Ransomware und wie ihre Varianten und Anwendungsfälle im Laufe der Zeit zugenommen haben. Wir zeigen, wie Datenlecks bereits Auswirkungen auf Unternehmen in aller Welt haben und welche weiteren Bedrohungen auf Organisationen lauern. Außerdem stellen wir praktische Schritte vor, wie Verantwortliche diese Gefahren erkennen und abwehren können.

Die Geburt von Ransomware und ihr Aufstieg (1989–2019)

Seit ihrer **Ausbreitung im Jahr 1989** mittels einer per Post verschickten Diskette hat sich Ransomware enorm weiterentwickelt. Heute zählt Ransomware zu den größten Bedrohungen für jede Firma, die in irgendeiner Form digital präsent ist. Sie stellt eine weitaus größere Gefahr dar als nur die Verschlüsselung von Computern und die Unterbrechung des Betriebs. Wenn Ransomware heutzutage zuschlägt, trifft es Unternehmen in allen Bereichen.

Als Meilenstein in der Entwicklung von Ransomware gilt das Jahr 2013, als Ransomware-Angriffe neben allgemeiner Cyberkriminalität und dubiosen Geschäften mit Kryptowährungen in den Mittelpunkt rückten. Das Aufkommen von Kryptowährungen bot Kriminellen die Möglichkeit, eine Vielzahl von Geschäftstransaktionen durchzuführen und dabei völlig unauffällig zu bleiben. Anonymität hat mit Abstand oberste Priorität bei Bedrohungsakteuren, noch mehr als die Bezahlung. Kryptowährungen (vor allem BTC und Monero) ermöglichen beides.

Doppelte (und dreifache) Erpressung (2019–2021)

Während Firmen früher mit einer einzigen Erpressung konfrontiert waren, betreffen Ransomware-Angriffe heute viele kritische Bereiche: Rufschädigung, Rechtsstreitigkeiten, Verletzungen von Vorschriften, Verlust von geistigem Eigentum. Die Angreifer haben nicht mehr nur eine Methode, um Druck auszuüben. Die Attacken beinhalten oft die Verschlüsselung von Systemen und die Drohung, gestohlene Daten zu veröffentlichen (doppelte Erpressung).

Im Juli 2019 publizierte die Hackergruppe MAZE auf frei zugänglichen Darkweb- und Clearweb-Websites gestohlene Daten aus den Netzwerken, Servern und Endpunkten der Opfer. Mit diesen Informationen sollten die Zielunternehmen unter Druck gesetzt und erpresst werden, das geforderte Lösegeld zu zahlen.

Zur gleichen Zeit erlangte RaaS (Ransomware as a Service) im Darkweb Popularität. Bei RaaS handelt es sich um ein Geschäftsmodell, das selbst unerfahrenen Nutzern die Möglichkeit bietet, ihre eigenen Ransomware-Angriffe zu starten und davon zu profitieren, indem sie eine symbolische Gebühr zahlen und sich für das Programm anmelden. Mit anderen Worten: RaaS ermöglicht es jedem, Unternehmen zu gefährden.

Durch RaaS und die Anonymität von Kryptowährungen operieren mittlerweile mehr als 30 Ransomware-Gruppen nach dem Prinzip der doppelten Erpressung. Dennoch gibt es Unterschiede zwischen diesen einzelnen Gruppierungen. So hat beispielsweise jedes Team seine eigenen Quellen für gestohlene Infos und publiziert Daten individuell (etwa Veröffentlichung von Lecks in mehreren Teilen, Beschreibung des genauen Prozentsatzes des bereits veröffentlichten Lecks, Herausgabe des vollständigen Lecks nach einer einzigen Bedrohung usw.).

Einige Ransomware-Gruppen haben sich auch untereinander (siehe: **MAZE-Kartell**) vernetzt. Zum Beispiel Ryuk und Conti mit TrickBot (wie vom **US-CERT** berichtet) sowie Egregor und ProLock mit QBot (**Bleeping Computer**), wobei sie die von den Mini-Malware-Stämmen bereits geöffneten „Hintertüren" nutzen.

Info-Stealer: Eine Malware-Art, die Informationen von einem System sammelt, hauptsächlich von Endpunkt-PCs oder Mobilgeräten. Die gängigsten Formen häufen Anmeldeinformationen wie Benutzernamen und Kennwörter sowie andere Autofill-Daten an und senden sie an den Betreiber zurück. Andere Arten konzentrieren sich hingegen auf finanzielle und persönliche Daten.

Laut **COVEWARE** sind die Ransomware-Zahlungen um 2.500 Prozent gestiegen, von einem durchschnittlichen Lösegeld von unter 10.000 US-Dollar Ende 2018 auf eine Lösegeldforderung im Schnitt von fast 250.000 Dollar im dritten Quartal 2020. Während einige Unternehmen schnell reagieren, sich mit den Angreifern in Verbindung setzen und diese Lösegelder zahlen, um die Veröffentlichung vertraulicher Daten zu verhindern, reagieren andere nicht so schnell – entweder bewusst oder aus mangelndem Bewusstsein für die Gefahren.

Außerdem haben sich Cyberkriminelle eine weitere Möglichkeit ausgedacht: Während sie mit der Veröffentlichung ergaunerter Firmendaten drohen, starten Hackergruppen DDoS-Angriffe (siehe Abbildung 1) auf die Server der Opfer, um sie von jeglicher Geschäftstätigkeit abzuhalten. In einigen Fällen blockieren sie den Zugang von Kunden und Mitarbeitern, um die Unternehmen zu zwingen, sich mit ihnen an den Verhandlungstisch zu setzen.

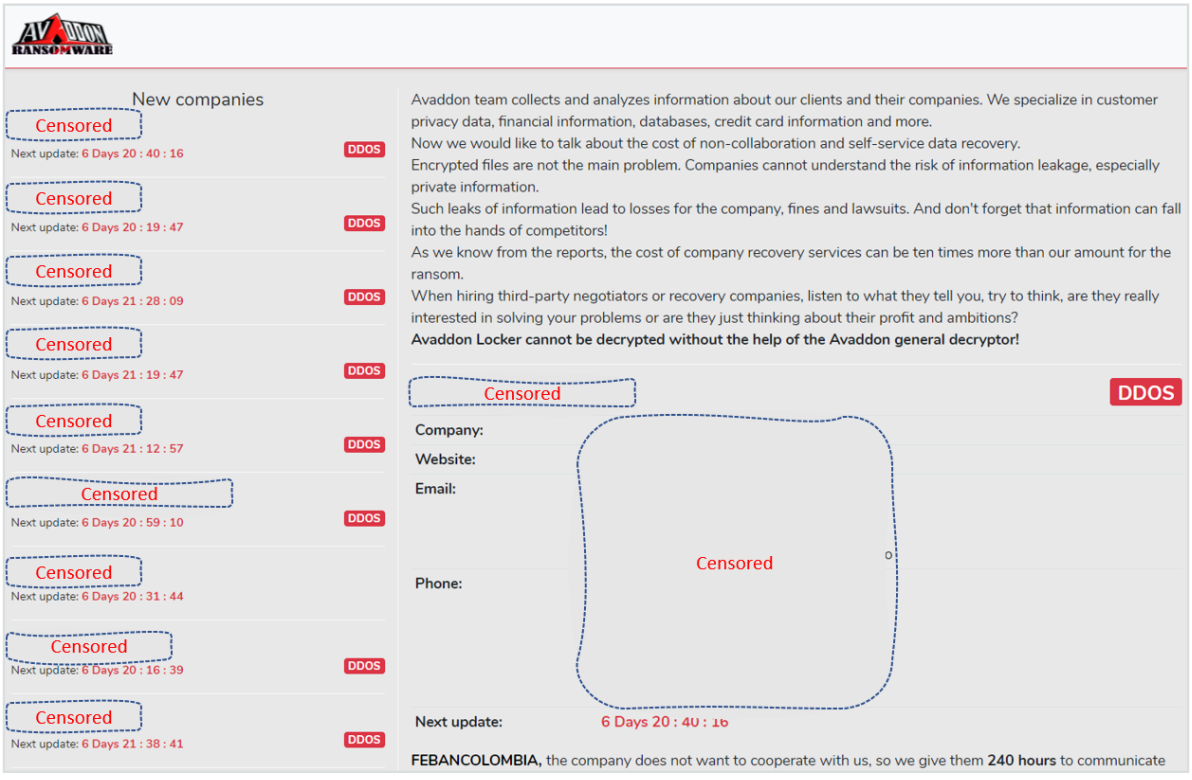


Abbildung 1: Avaddon-Quelle, die Unternehmen auflistet, die derzeit einem DDoS-Angriff ausgesetzt sind

Die Ransomware-Zukunft: Private Daten für jedermann und jeden Zweck (2021–?)

Anfangs galten Ransomware-Gruppen-Quellen als nur ein Mittel zur Erpressung. Opfer, die sahen, dass ihre Daten am seidenen Faden hingen und kurz vor der Veröffentlichung standen, hatten das Exklusivrecht, sich aus der misslichen Lage herauszukaufen. Diese „komfortable" Situation dauerte jedoch nur etwa ein Jahr, bevor die Cyberkriminellen beschlossen, ihren Opfern das Leben noch schwerer zu machen.

Seit Anfang 2021 stellt IntSights fest, dass Ransomware-Gruppen mit zunehmender Dynamik in einem Multichannel-Modus operieren, in dem sie nun einige der vollständigen Datenlecks in verschiedenen Bereichen ihrer bestehenden Websites **versteigern**. IntSights weiß, dass mehrere Hackergruppen ihre gesamte Beute dem Meistbietenden zum Kauf anbieten. Das bedeutet, dass ein Unternehmen, das unter einer Ransomware-Attacke leidet, gegen die Zeit arbeitet, um wieder auf die Beine zu kommen und den Geschäftsbetrieb aufzunehmen. Es läuft zudem Gefahr, seine Daten an Unbekannte zu verlieren und möglicherweise nicht einmal zu wissen, welche Daten kompromittiert wurden und/oder wer nun Zugriff auf sie hat.

Die jüngste Ransomware-Entwicklung geht auf eine Gruppe namens BABUK zurück. Diese vermutlich russische Truppe hat kürzlich einige „Presseerklärungen" auf ihrer Website veröffentlicht. In einer davon erklärt BABUK, dass die Hacker nicht mehr „Netzwerke verschlüsseln", aber immer noch „Ihre Daten mitnehmen" werden, um die angegriffene Partei danach zu benachrichtigen (siehe Abbildung 2).

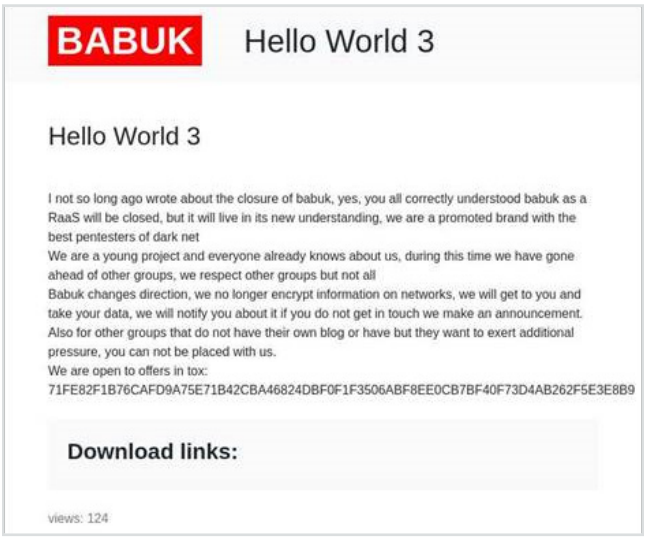


Abbildung 2: BABUK-Presseerklärung vom 30. April 2021

BABUK erklärt uns im Wesentlichen, dass sich die Netzwerkverschlüsselung als bloße Verschlüsselung nicht mehr lohnt. Mit anderen Worten: Für Firmen mit Back-up-Programmen ist diese früher bewährte Taktik nicht mehr schädlich genug.

Diese neue Realität wirkt sich mehrfach aus:

- **Veraltete Back-ups** - Sie sollten immer noch schnelle, von Ihren Netzwerken getrennte Back-ups einsetzen. Diese ermöglichen es Ihrem Unternehmen jedoch nur, schnell wieder in Betrieb zu gehen, bewahren Sie aber nicht unbedingt vor Geschäftsschäden durch Ransomware.

- **Lähmende Ungewissheit** - Nur weil Ihr Netzwerk noch funktioniert und die Endgeräte einwandfrei arbeiten, heißt das nicht, dass Sie nicht **bereits** mit übler Malware infiziert sind, die Daten entwendet.

- **Ethische Grenzen überschritten** - Einige Hackergruppen vermieden es früher, kritische Infrastrukturen und Einrichtungen des Gesundheitswesens wie Krankenhäuser anzugreifen. Sie wollten keine Menschenleben gefährden. Nun gehen Cyberkriminelle aktiv auf Medizin- und Bildungseinrichtungen los, wobei sie ihnen erlauben, ihre Funktionsfähigkeit aufrechtzuerhalten. In einigen Fällen werden die **Patienten, deren Daten gestohlen wurden,** sogar erpresst. Die Opfer müssen „nur" ein saftiges Lösegeld zahlen, sonst landen ihre Daten bei anderen Ransomware-Gruppen, privaten Käufern, feindlichen Ländern oder im Internet.

Im Zusammenhang mit diesem Trend hat IntSights eine neue Art von Quelle in der Landschaft der Datenlecks identifiziert: Schwarzmärkte für Datenlecks (siehe Abbildung 3). Obwohl das Konzept des Handels und der Versteigerung von Datenlecks schon länger existiert, entsteht durch die neue Entwicklung eine Plattform, die es vorher so nicht gab. Einige der Betreiber behaupten sogar, überhaupt keine Cyberkriminellen zu sein. Diese Märkte beruhen im Wesentlichen – neben anderen Faktoren – auf der Zusammenarbeit zwischen Angreifern und Verkäufern.

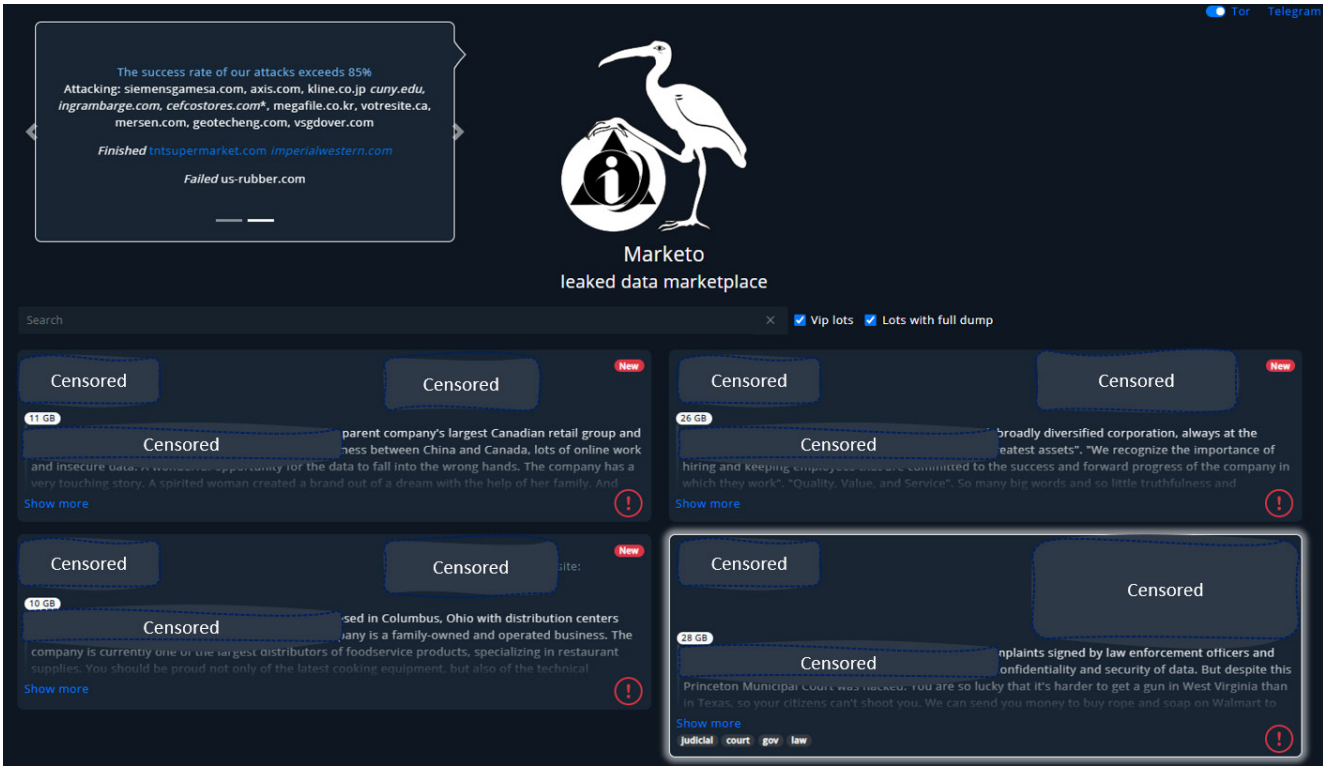


Abbildung 3: Durchgesickerter Daten-Marktplatz von Marketo (Mai 2021)

Die Angreifer müssen die Daten nicht mehr selbst zum Verkauf anbieten, sparen Zeit und Mühe und brauchen sich so nicht der Gefahr aussetzen, enttarnt zu werden. Jetzt können sie mit dieser neuen Plattform von Schwarzmärkten, die sich ausschließlich auf Datenlecks spezialisiert haben, mehr Opfer erpressen. Eine Ransomware-Gruppe kann sich in ein Unternehmen hacken, alle benötigten Informationen klauen und sie an einen Dritten verkaufen, der einen Schwarzmarkt betreibt. Erst dann erfährt das Opfer, was geschah – wenn überhaupt.

Am 1. Juni 2021 erfüllte BABUK sein Versprechen und startete seine „Plattform für unabhängige Leaks". Bei der Eingabe der bekannten Domain stießen die Nutzer auf eine neue Website. Anstelle des bekannten BABUK-Blogs fanden sie eine Entität, die unter dem Namen „Payload.bin" firmiert (siehe Abbildung 5 auf der nächsten Seite). Die Abschnitte „Über uns" und „Unsere Regeln" auf der Website sind aber noch leer.

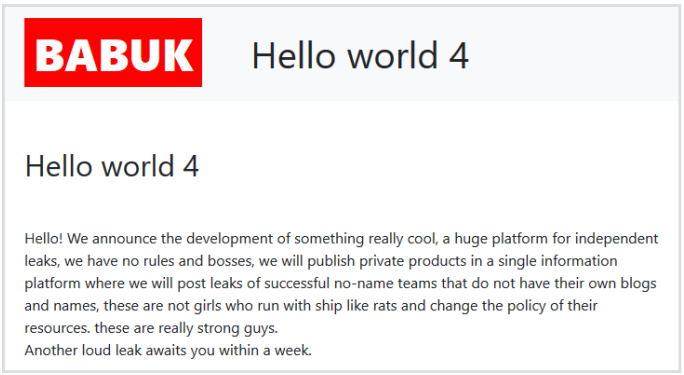
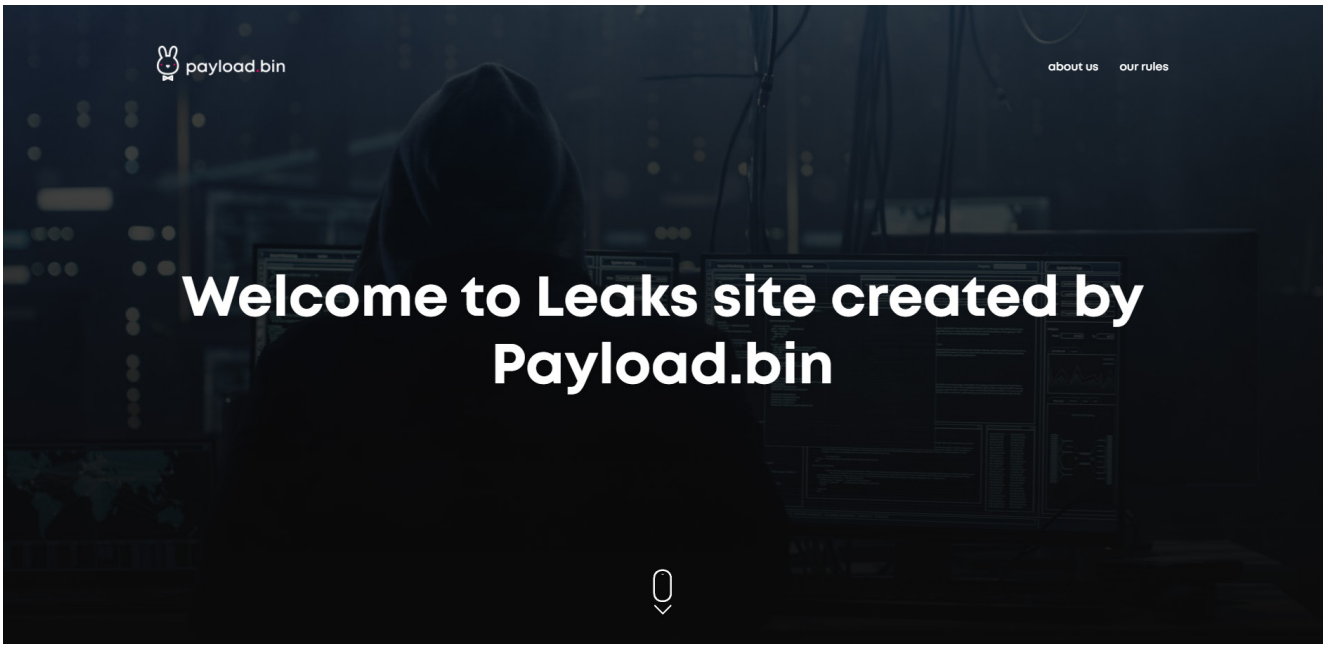


Abbildung 4: Einige Wochen nach „Hello world 3" erklärte die BABUK-Gruppe der Welt in der nächsten Mitteilung, dass sie sich offiziell dem Trend anschließt



Der erste Beitrag betrifft den „CD Projekt all Source Code", den Quellcode des mit Spannung erwarteten Videospiels „Cyberpunk 2077". **Berichten zufolge** brachte dieser im Februar in einer Darkweb-Auktion einen Millionenbetrag ein, nachdem er durch einen Ransomware-Angriff illegal beschafft worden war.

Die wahre Cyberbedrohung der Zukunft besteht also nicht nur im Verlust von Funktionen oder physischen Schäden, sondern auch im **Datendiebstahl** und den zahlreichen Möglichkeiten, diesen auszunutzen. Die Prognosen von IntSights deuten darauf hin, dass in den kommenden Jahren immer mehr Erscheinungsformen von Datendiebstahl, -lecks und -handel auftauchen – möglicherweise bis zu einem Punkt, an dem Firmen alle Geheimnisse verlieren. Die Aufrechterhaltung einer abhörsicheren Infrastruktur scheidet als realistische Option aus.

Weitere Ransomware-Prognosen von IntSights

In nicht allzu ferner Zukunft werden Ransomware-Gruppen, bösartige Einzelakteure und sogar „normale" Benutzer wahrscheinlich die folgenden Möglichkeiten nutzen:

- **Ransomware für Mobilgeräte** - Die kleinen Begleiter könnten bald zu einem weiteren fruchtbaren Boden für Datendiebstahl werden (etwa Nachrichten, Bilder oder Passwörter), zum Beispiel durch Verschlüsselung der Geräte – oder indem dieser Schritt ganz übersprungen und direkt zur Erpressung übergegangen wird.

- **Ransomware für IoT- und OT-Geräte** - Sie kommen zu Hause an, Ihre Tür ist durch ein WiFi-basiertes Schloss verriegelt. Beim Versuch, die Tür mit der entsprechenden Anwendung zu öffnen, sehen Sie ein Vendetta-Symbol, das das alte Lied singt: Bezahlen oder draußen bleiben. Doch was, wenn es sich um die Zimmertür Ihres Kindes handelt? Was, wenn es ein elektrisches Gerät, eine medizinische Apparatur oder ein Bauwerkzeug betrifft? Hier lauern Gefahren, auch bei schweren Maschinen oder Produktionsanlagen. Die Kontrollübernahme über mit dem Internet verbundene Geräte führt zwar nicht unbedingt zu einem Datenverlust, kann aber eine ernsthafte Bedrohung für private und industrielle Umgebungen darstellen.

- **Ständig steigende Lösegeldbeträge** - Solange die Opfer zahlen, steigen die Lösegeldbeträge weiter. Aus diesem Grund raten alle Behörden davon ab, Cyberkriminelle zu belohnen. Es gibt keine Garantie dafür, dass sie ihre Zusagen einhalten, wenn Sie einen Deal mit Dieben eingehen. Aber leider möchte niemand derjenige sein, der ein starkes Zeichen setzt und gleichzeitig seine Daten, seinen Ruf und noch viel mehr verliert.

- **Strafverfolgung** - Cyberkriminelle verhalten sich immer dreister, schlauer und raffinierter, wodurch sich die Strafverfolgungsbehörden einschalten. Bislang waren diese Behörden in den meisten Bereichen der Darkweb-Kriminalität kaum beteiligt, doch das ändert sich in letzter Zeit. Als DarkSide die Verantwortung für den Angriff auf Colonial Pipeline übernahm, verschickte die Hackergruppe innerhalb einer Woche eine Presseerklärung, in der sie angab, dass sie **Druck „aus den USA"** erhalte. Die Vereinigung hat seitdem in einer weiteren Nachricht mitgeteilt, dass sie den Zugang zu ihrer Infrastruktur verloren hat, wobei sie sich auf eine Störung durch eine Strafverfolgungsbehörde und anhaltenden Druck aus den USA beruft.

Im Januar beschlagnahmte das FBI in Zusammenarbeit mit dem nationalen bulgarischen Ermittlungsdienst und einigen anderen Parteien die Quelle von NetWalker, einer der aktivsten Ransomware-Gruppen (siehe Abbildung 6). Nach der Zerschlagung der Infrastruktur verhafteten die Behörden auch eine kanadische Person, die angeklagt wurde, die Ransomware benutzt zu haben, um zehn Millionen Dollar zu verdienen. Diese Verhaftung sowie die erfolgreiche Razzia der ukrainischen Polizei in einer Wohnung, die von den Vertreibern des berüchtigten Banking-Trojaners Emotet genutzt wurde, macht all jenen Hoffnung, die sich wünschen, dass offizielle Stellen Cyberkriminalität unterbinden.

Abbildung 6: Die Quelle von NetWalker, nachdem sie von den Strafverfolgungsbehörden beschlagnahmt wurde

Empfehlungen zur Vermeidung von Ransomware-Schäden

IntSights empfiehlt die folgenden Schritte zur Verhinderung von Datenverlusten, die aus einem erfolgreichen Ransomware-Angriff resultieren:

- **Richtlinie für geschlossene Ports** - Führen Sie eine Richtlinie für geschlossene Ports ein oder einen strengen Leitfaden für die Änderung von Anmeldeinformationen – insbesondere für Ports, auf denen RDP läuft. Der RDP-Zugang zu einem einzigen Netzwerkknoten reicht aus, um einem Angreifer die Kontrolle zu ermöglichen.

- **Phishing-Betrügereien um jeden Preis verhindern** - Phishing und seine Varianten (Spear-Phishing, Smishing, Whaling usw.) gehören zu den ältesten Tricks der Welt und sind immer noch äußerst erfolgreich. Hier empfehlen sich Sicherheitsschulungen für alle Mitarbeiter sowie der Einsatz verschiedener Firewalls und E-Mail-Schutzlösungen.

- **Patches für bekannte Schwachstellen und Software-Updates** - Halten Sie Ihre Software auf dem neuesten Stand und schützen Sie Ihr Netzwerk vor Attacken. Obwohl es sich um die einfachste und offensichtlichste Schutzmaßnahme handelt, halten sich einige Benutzer und Administratoren nicht an diese simple Regel. Wenn eine Sicherheitslücke öffentlich gemacht wird, dauert es nicht lange, bis böswillige Akteure sie zu ihrem eigenen Vorteil ausnutzen – im Falle von Zero-Day-Schwachstellen sogar schon vor der Veröffentlichung. Deshalb müssen Sie immer Patches und Updates bereitstellen.

Schlussfolgerung

Morgen könnten Ihre Daten bereits im Internet stehen, zur Schau gestellt von erfahrenen Kriminellen oder von gelegentlichen RaaS-Nutzern, kostenlos oder für den Meistbietenden. Dabei spielt es keine Rolle, ob es sich um einen direkten Angriff oder um ein Leck bei Dritten handelt. Wer Daten besitzt, kann in die Schusslinie geraten.

Es gibt viel zu bedenken, wenn es um die möglichen Auswirkungen von Ransomware auf Ihr Unternehmen geht. Die Bedrohung verschwindet nicht, im Gegenteil: Die Ransomware-Gefahr wächst und verändert sich, Datenverluste avancieren zum größten Geschäftsrisiko unserer Zeit. Geschäftsführer müssen am Ball bleiben und wachsam sein, indem sie externe Bedrohungsdaten-Protokolle für eine wirksame Erkennung, Verhinderung und Reaktion auf Datenverluste implementieren.

Über IntSights

IntSights ermöglicht es Unternehmen jeder Art und Größe, den vollen Nutzen aus externen Bedrohungsdaten zu ziehen, unabhängig vom Umfang oder dem Entwicklungsstand ihrer Threat-Intelligence-Programme. Im Gegensatz zu allen anderen Lösungen auf dem Markt reduziert IntSights die Komplexität von Threat Intelligence und liefert sofortigen Nutzen – ohne den großen Aufwand oder die beträchtliche Ressourcenzuweisung, die herkömmliche Threat-Intelligence-Lösungen erfordern. IntSights ist skalierbar und eignet sich für jede Firma, und die reibungslose Integration unserer Echtzeit-Cyber-Bedrohungsdaten in die bestehende Sicherheitsinfrastruktur unterstützt Betriebe dabei, ihre Investitionsrendite zu maximieren.

IntSights verfügt über Niederlassungen in Amsterdam, Boston, Dallas, New York, Singapur, Tel Aviv und Tokio. Wenn Sie mehr erfahren möchten, besuchen Sie bitte **intsights.com** und treten Sie in Kontakt mit uns über **LinkedIn**, **Twitter** oder **Facebook**.