LogRhythm®
The Security Intelligence Company

Die Ransomware-Bedrohung

So erkennen Sie einen Angriff, bevor es zu spät ist

DIE RANSOMWARE-BEDROHUNG:
So erkennen Sie einen Angriff, bevor es zu spät ist

LogRhythm
The Security Intelligence Company

INHALTSVERZEICHNIS:

- EINFÜHRUNG
- EINE SCHNELL WACHSENDE BEDROHUNG: EINE GEISSEL NAMENS RANSOMWARE
- DIE ANGRIFFE VERLAGERN SICH VON PRIVATPERSONEN ZU UNTERNEHMEN UND ORGANISATIONEN
- DIE 5 PHASEN EINES RANSOMWARE-ANGRIFFS
- DIE 5 VERTEIDIGUNGSSCHRITTE: UMGANG MIT EINEM RANSOMWARE-ANGRIFF
- FAZIT
- ÜBER LOGRHYTHM

Im Februar 2016 fiel das Computernetzwerk im Hollywood Presbyterian Medical Center (HPMC) in Südkalifornien mehr als eine Woche lang aus, weil das Krankenhaus mit den Folgen eines Ransomware-Angriffs zu kämpfen hatte. Die Krankenhausverwalter riefen den internen Notstand aus, da die Mitarbeiter Schwierigkeiten hatten, auf Krankenakten und Computersysteme zuzugreifen, die für die Patientenversorgung unerlässlich waren. Einige Patienten mussten in andere Krankenhäuser verlegt werden, um ihre kontinuierliche Versorgung zu gewährleisten. Währenddessen hielten die Angreifer die Computersysteme des Krankenhauses als Geisel, bis ein Lösegeld von 40 Bitcoins – etwa 17.000 USD – gezahlt wurde. Erst dann konnte das Krankenhaus seine Dateien wieder nutzen, die heimlich mit Malware verschlüsselt worden waren.

Seitdem haben mindestens drei weitere Gesundheitseinrichtungen Betriebsstörungen durch Ransomware-Angriffe gemeldet. Und es wird weitere geben, da organisierte Cyber-Kriminelle mittlerweile erkannt haben, wie lukrativ diese Art von Angriff sein kann. HPMC ist mit einem Lösegeld von nur 40 Bitcoins vielleicht noch glimpflich davongekommen. Kriminelle wissen, dass viele Unternehmen und Einrichtungen noch deutlich mehr zahlen würden, um ihre Systeme wieder betriebsbereit zu machen. Laut dem Institute of Critical Infrastructure Technology (ICIT) wird es in den Vorstandsetagen von Unternehmen in den USA und weltweit hitzige Diskussionen um die Frage „zahlen oder nicht zahlen“ geben.

Ist Ihr Unternehmen auf einen Ransomware-Angriff vorbereitet? Um Ihr Unternehmen erfolgreich gegen einen solchen Angriff verteidigen zu können, müssen Sie gewappnet sein und wissen, worauf Sie achten müssen, wenn ein Angriff beginnt. Dieser Leitfaden bereitet die gesammelten Erkenntnisse der Experten bei LogRhythm auf und zeigt Ihnen, wie Ransomware-Angriffe beginnen, wie sie sich auf Ihren Endpunkten und im Netzwerk fortpflanzen und wie Sie sie verhindern oder zumindest eindämmen können, um schwere Nachwirkungen zu verhindern.

Das Institute of Critical Infrastructure Technology konstatiert:

“2016 IST DAS JAHR, IN DEM RANSOMWARE AMERIKA ALS GEISEL NEHMEN WIRD”

Eine schnell wachsende Bedrohung: Eine Geißel namens Ransomware

Über die letzten drei Jahre ist Ransomware ins Rampenlicht der IT-Bedrohungslandschaft gerückt. Kaspersky Lab meldet, dass seine Lösungen im Jahr 2015 auf mehr als 50.000 Computern in Unternehmensnetzwerken Ransomware entdeckt haben – das sind doppelt so viele wie 2014. Doch trotz dieser Entdeckungsrate räumt Kaspersky ein, dass die Dunkelziffer um ein Vielfaches über dem liegt, was erkannt und gemeldet wurde.[1] Allein im ersten Quartal 2016 erpressten IT-Kriminelle mittels Ransomware 209 Mio. USD. Das FBI schätzt, dass die Verluste durch Ransomware im Jahr 2016 über 1 Mrd. USD liegen werden.[2] Und wie gesagt - dies ist nur die Spitze des Eisbergs.

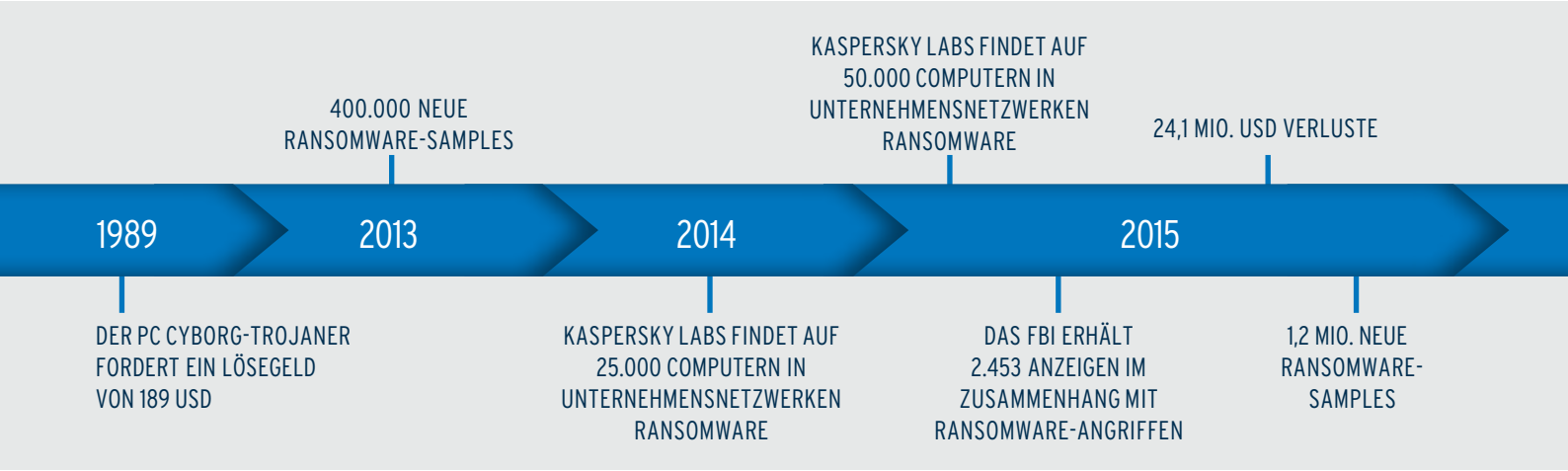
Doch was genau ist diese Geißel namens Ransomware? Es handelt sich um eine bösartige Software, die es einem Hacker erlaubt, den Zugang zu den wichtigen Informationen einer Privatperson oder eines Unternehmens einzuschränken und dann irgendeine Form von Zahlung zu verlangen, um die Einschränkung aufzuheben. Die häufigste Art von Einschränkung ist heute die Verschlüsselung wichtiger Daten auf dem Computer oder Netzwerk, was letztlich bedeutet, dass der Angreifer Benutzerdaten oder ein System in Geiselhaft nimmt. Zahlung in Bitcoins ist die typische Forderung, da die digitale Währung sowohl global als auch anonym ist. Ransomware-Angriffe gewinnen bei IT-Kriminellen aus gutem Grund schnell an Beliebtheit: Es wird geschätzt, dass die Kriminellen mit dieser Art von Angriff 10 bis 50 Mio. USD pro Monat verdienen.[3]

Die Idee, Ransomware zu entwickeln, ist im Grunde nichts Neues. Im Jahr 1989 verbreitete Dr. Joseph Popp einen Trojaner namens PC Cyborg, bei dem Malware alle Ordner verbarg und die Dateien auf dem C-Laufwerk des PCs verschlüsselte. Ein Skript lieferte eine Lösegeldnachricht, in der die Zahlung von 189 USD an die PC Cyborg Corporation verlangt wurde. Der betroffene Computer funktionierte nicht, bis das Lösegeld gezahlt wurde und die Maßnahmen der Malware rückgängig gemacht wurden. Seither ist dieses System wesentlich verfeinert worden, insbesondere im Hinblick auf stärkere Dateiverschlüsselung. Heute ist es für die Opfer praktisch unmöglich, ihre eigenen Dateien zu entschlüsseln.

Eine andere Art von Ransomware, die sogenannte „Scareware", zeigte auf dem Computer eines Benutzers eine Warnung an, dass das Gerät mit Malware befallen sei, die sich sofort entfernen ließe, wenn das Opfer etwas kaufe, das sich dann als gefälschte Antivirensoftware erwies. Die Scareware-Meldung erschien wiederholt, was viele Opfer veranlasste, die „Antivirensoftware" zu kaufen, nur um die Warnmeldung loszuwerden.

Der Begriff „Ransomware" bezeichnet allgemein ein breites Spektrum von bösartigen Softwareprogrammen, wie CryptoLocker, Locky, CryptoWall, KeyRanger, SamSam, TeslaCrypt, TorrentLocker und weitere. Diese Hauptanwendungen tauchen in verschiedenen Varianten auf und entwickeln sich ständig weiter, um der Erkennung zu entgehen. In der Tat haben Forscher im zweiten Quartal 2015 mehr als 4 Millionen Ransomware-Samples gefunden, einschließlich 1,2 Millionen neuer. Im dritten Quartal 2013 waren es noch weniger als 1,5 Millionen gewesen, darunter weniger als 400.000 neue Samples.[4]

Die große Mehrheit der heutigen Angriffe richtet sich gegen Windows-basierte Systeme. Das liegt hauptsächlich an den Zahlenverhältnissen: Es gibt mehr Windows-basierte Computer als Geräte mit anderen Betriebssystemen. Angreifer setzen oft Exploit Kits ein, um die Ransomware auf das Gerät des Opfers zu bekommen.



[1] Kaspersky Lab, „Kaspersky Security Bulletin 2015"
[2] CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, 15. April 2016
[3] David Common, CBC News, „Ransomware: What You Need to Know", 11. März 2015
[4] Security Magazine, „'Ransomware' Attacks to Grow in 2016", 23. November 2016

Die Angriffe verlagern sich von Privatpersonen zu Unternehmen und Organisationen

Bis vor Kurzem waren die meisten Ransomware-Angriffe einfach opportunistisch und betrafen vor allem die Computer privater Benutzer oder kleinerer Unternehmen. Die Lösegeldforderungen beschränkten sich meist auf den Gegenwert von ein paar Hundert Dollar für einen einzelnen PC. Dies war und ist weiterhin ein lukratives Geschäft für Kriminelle, die die Endbenutzer als leichte Beute ansehen. Aber jetzt sind die größeren Unternehmen in ihr Visier geraten, die größere Budgets haben, um höhere Lösegeldforderungen zu zahlen. Zudem haben sie wichtigere Dateien und Computersysteme, die für den täglichen Geschäftsbetrieb unabdingbar sind.

Eine von Intermedia in Auftrag gegebene und von Researchscape International durchgeführte Umfrage bei knapp 300 IT-Beratern zeigte, dass die Ausfälle für die meisten Unternehmen schädlicher sind als die Lösegeldforderung an sich. Von den Unternehmen, die einen Ransomware-Angriff erlitten, konnten 72% für mindestens zwei Tage nach dem Ausbruch nicht auf ihre Daten zugreifen und 32% verloren den Zugang für fünf Tage oder länger. Außerdem waren von 86% der Angriffe zwei oder mehr Mitarbeiter betroffen und 47% erstreckten sich auf mehr als 20 Personen.[5]

Neben dem Hollywood Presbyterian Medical Center in Los Angeles haben auch viele andere Unternehmen und Einrichtungen Ransomware-Angriffe erlitten. Einige Beispiele sind MedStar Health, der größte Gesundheitsdienstleister in Maryland und Washington, D.C.; das Methodist Hospital in Henderson, Kentucky; der Schulbezirk Swedesboro-Woolwich in New Jersey; und selbst lokale Polizeibehörden in Maine und Massachusetts. All diese Unternehmen und Einrichtungen mussten den Betrieb aussetzen, weil ihre wichtigen Dateien unerreichbar waren.

Viele der Angriffe auf Privatpersonen und kleinere Unternehmen finden über Ramsomware statt, die massenhaft verbreitet wird. Die Opfer sind meist Gelegenheitsziele (d.h. diese Personen/Unternehmen wurden nicht aufgrund ihrer Identität gezielt anvisiert). Sie haben sich die Malware meist über eine Phishing-E-Mail, einen Drive-by-Download oder von einer befallenen Website eingefangen. So wurden beispielsweise Websites der New York Times, der BBC, von AOL und der NFL allesamt im Rahmen einer bösartigen Kampagne „gekapert", die darauf abzielt, auf den Computern der Besucher Ransomware zu installieren.[6]

„Die Bedrohung verschiebt sich", so Ryan Sommers, Manager of Incident Response bei LogRhythm. „Wir sehen, wie Kriminelle ihre Taktiken auf gezielte Ransomware-Angriffe verlagern. Sie wählen ein spezifisches Unternehmen aus, das große Finanzreserven hat und mit höherer Wahrscheinlichkeit eine hohe Lösegeldforderung zahlen würde, um die Ausfallzeit zu minimieren", erklärt Sommers. So zahlte das Hollywood Presbyterian Medical Center fast 17.000 USD, um seine Dateien entsperren zu lassen und zum Normalbetrieb zurückkehren zu können. Einer Schätzung zufolge war dies noch ein gutes Geschäft, da das Krankenhaus sage und schreibe 100.000 USD pro Tag allein dadurch verlor, dass es keine CTs an Patienten durchführen konnte.[7] Und auch die Täter können rechnen. Gezielt ausgewählte Unternehmen könnten deutlich höhere Lösegeldforderungen erhalten, je nachdem, wie viel sie vermutlich zu zahlen bereit sind.

Auf den ersten Blick scheinen Massenverbreitung und gezielte Angriffe einander zu ähneln, aber es gibt ein paar grundlegende technische Unterschiede, die wir in den nächsten Abschnitten untersuchen werden. Massenangriffe sind typischerweise automatisiert, sehr schnell in ihrer Ausführung – oft nur 15 Minuten von der anfänglichen Infektion bis zu einer Lösegeldforderung – und aus Sicht des Angreifers gut abgestimmt.

Gezielte Angriffe ähneln dagegen stark Advanced Persistent Threats (APTs). Sie werden normalerweise von einem Menschen und nicht einem automatisierten System betrieben und ihre Ausführung kann deutlich mehr Zeit in Anspruch nehmen. Die Tools, die für die beiden Angriffsarten verwendet werden, können ebenfalls unterschiedlich sein. Für Massenangriffe werden oft speziell angepasste oder Einmal-Tools verwendet. Gezielte Angriffe setzen für die Erkundungsphase mehr serienmäßige Tools ein, während der Verschlüsselungsprozess meist speziell angepasst ist.

[5]Blogpost von Intermedia, „When ransomware strikes your business, are you prepared? Our new report findings may surprise you.", 17. März 2016
[6]The Guardian, „Major sites including New York Times and BBC hit by 'ransomware' malvertising", 16. März 2016
[7]Venturebeat, „Next wave of ransomware could demand $millions", 26. März 2016

Die 5 Phasen eines Ransomware-Angriffs

Ransomware-Angriffe haben klar unterscheidbare Phasen, unabhängig davon, ob es sich um eine Massenverbreitung oder einen gezielten Angriff handelt. „Wenn man weiß, was in jeder Phase geschieht, und die Indicators of Compromise [IOCs] (Befallanzeichen) kennt, nach denen man Ausschau halten sollte, steigt die Wahrscheinlichkeit, dass man einen Angriff erfolgreich abwehren oder zumindest seine Folgen mindern zu kann“, erläutert Sommers.

Diese Phasen sind:

1. **Ausnutzung und Infektion**
2. **Bereitstellung und Ausführung**
3. **Vernichtung von Sicherungskopien**
4. **Dateiverschlüsselung**
5. **Benachrichtigung des Benutzers und Cleanup**

Abbildung 1: Der typische zeitliche Ablauf eines Ransomware-Angriffs über Massenverbreitung

Wir werden im Folgenden angeben, wo die Aktivitäten in den einzelnen Phasen sowie die IOCs je nach Angriffstyp unterschiedlich ausfallen. So besteht zum Beispiel einer der Unterschiede zwischen einem Angriff über Massenverbreitung und einem gezielten Angriff darin, wie lange es dauert, alle Schritte vollständig auszuführen.

Wie in Abbildung 1 gezeigt, ist der zeitliche Ablauf eines Massenangriffs sehr konzentriert – oft nur 15 Minuten von der Ausnutzung und Infektion bis zum Erhalt einer Lösegeldforderung durch das Opfer. Ein Grund für diesen schnellen Verlauf besteht darin, dass der Angriff nicht versucht, über das erste System hinauszugehen, das er erfasst.

Dagegen verhält sich ein gezielter Angriff eher wie eine APT: Er versucht, auf so breiter Ebene wie möglich so viel Schaden wie möglich anzurichten. Die Angreifer versuchen, das gesamte Unternehmen zu befallen statt nur einen einzelnen Benutzer, da sie dann das Unternehmen erpressen und versuchen können, wesentlich mehr Geld zu bekommen. Da gezielte Angriffe meistens von einer Person betrieben werden und nicht von einem automatisierten System, spielt die Reaktionszeit eine etwas weniger kritische Rolle als bei Ransomware über Massenverbreitung. Leider bedeutet das auch, dass es schwieriger sein kann, den Angriff zu erkennen.

Sehen wir uns die typischen Phasen eines Angriffs einmal im Detail an.

1 Phase 1: Ausnutzung und Infektion

Damit ein Angriff erfolgreich ist, muss die bösartige Ransomware-Datei auf dem Computer ausgeführt werden. Dies geschieht oft über eine Phishing-E-Mail oder ein Exploit Kit – eine Art von bösartigem Werkzeugkasten, der verwendet wird, um Sicherheitslücken in Softwareanwendungen auszunutzen und so Malware zu verbreiten. Diese Kits zielen auf Benutzer ab, die auf ihrem Computer unsichere oder veraltete Software nutzen.

Im Fall der CryptoLocker-Malware ist das Angler-Exploit Kit eine bevorzugte Methode, um die Ausführung zu erreichen. Die Schwachstellen, die das Angler Exploit Kit bevorzugt, finden sich typischerweise in Adobe Flash und Internet Explorer.

2 Phase 2: Bereitstellung und Ausführung

Nach dem Ausnutzungsprozess wird die eigentliche ausführbare Ransomware auf dem System des Opfers bereitgestellt. Nach der Ausführung setzt sich die Ransomware mittels Persistenz-Mechanismen im System fest. Typischerweise dauert dies ein paar Sekunden, je nach Netzwerkgeschwindigkeit.

Leider werden die ausführbaren Dateien meist über einen verschlüsselten Kanal bereitgestellt – statt SSL wird eine maßgeschneiderte Verschlüsselungsschicht zur normalen HTTP-Verbindung hinzugefügt. Da die Malware eine sichere Verschlüsselung verwendet, ist es schwer, die ausführbare Datei in der Leitung aufzuspüren. „Meistens werden die ausführbaren Dateien entweder im %APPDATA%- oder im %TEMP%-Ordner unter dem Profil des Benutzers abgelegt“, erläutert Sommers. „Zum Zweck der Erkennung ist es gut, das zu wissen, da Ihr Unternehmen dann auf solche Ereignisse achten kann, um Abwehrmechanismen einzurichten.“

Die meiste Crypto-Malware wendet Persistenz-Techniken an: So kann sie, falls der betroffene Rechner während des Verschlüsselungsprozesses neu gestartet wird, anschließend einfach weitermachen und ihn vollends verschlüsseln.

3 Phase 3: Vernichtung von Sicherungskopien

Ein paar Sekunden, nachdem die Malware ausgeführt wurde, macht sich die Ransomware an die Sicherungsdateien und -ordner auf dem System und entfernt sie, um eine Wiederherstellung zu verhindern. Das ist eine Besonderheit von Ransomware. Andere Arten von krimineller Software und sogar APTs machen sich nicht die Mühe, Sicherungsdateien zu löschen.

Die meisten Ransomware-Varianten setzen alles daran, dem Opfer jede Chance zu nehmen, sich von dem Angriff zu erholen, ohne das Lösegeld zu zahlen. Auf Windows-Systemen wird sowohl bei gezielten als auch bei Massenangriffen oft das vssadmin-Tool verwendet, um die Volumeschattenkopien vom System zu entfernen. So führen zum Beispiel CryptoLocker und Locky einen Befehl aus, alle Volumeschattenkopien vom System zu löschen. „Die gute Nachricht ist, dass dabei Ereignisprotokolleinträge erstellt werden, wodurch auslösbare Ereignisse von einem SIEM oder Host-basierten Produkt erkannt werden können“, erklärt Sommers.

Einige Varianten, insbesondere bei den gezielten Angriffen, gehen sogar so weit, dass sie nach Ordnern suchen, die Sicherungskopien enthalten, und diese Dateien dann mit Gewalt entfernen. Selbst wenn ein Programm diese Dateien sperrt, werden sie den Prozess abbrechen, sodass sie diese Ordner mit Sicherungskopien löschen können, um die Wiederherstellung noch schwieriger zu machen.

4 Phase 4: Dateiverschlüsselung

Sobald die Sicherungskopien vollständig entfernt wurden, führt die Malware mit dem Command-&-Control-Server (C2) einen sicheren Schlüsselaustausch durch und richtet damit die Verschlüsselungsschlüssel ein, die auf dem lokalen System verwendet werden sollen. Häufig kennzeichnet die Malware das lokale System mit einer eindeutigen Kennung, die dem Benutzer am Ende in den Anweisungen genannt wird. Damit unterscheidet der C2-Server auch zwischen den Verschlüsselungsschlüsseln, die für verschiedene Opfer verwendet wurden. Leider verwenden die meisten Varianten heute sichere Verschlüsselung wie AES 256, sodass das Opfer die Verschlüsselung nicht selbst brechen kann.

Nicht jede Art von Ransomware muss einen C2-Server kontaktieren, um Schlüssel auszutauschen. So nimmt etwa bei der SamSam Malware die Softwareanwendung die gesamte Verschlüsselung lokal vor, ohne überhaupt ins Internet zu gehen. Dies ist gut zu wissen, da die Kommunikation mit einem C2-Server ein IOC ist, der überwacht werden sollte, Umgekehrt bedeutet das Fehlen eines solchen Ereignisses allerdings noch nicht, dass keine Ransomware vorhanden ist.

Während der Dateiverschlüsselungsphase gehen verschiedene Ransomware-Varianten bei der Dateibenennung und -verschlüsselung unterschiedlich vor. So verschlüsselt zum Beispiel CryptoWall Version 3 den Dateinamen nicht, während CryptoWall Version 4 den Dateinamen und die Erweiterung randomisiert. Locky randomisiert die Dateinamen, fügt ihnen aber die Dateierweiterung .locky hinzu. Mit diesem Wissen kann Ihr Unternehmen manchmal anhand der Art und Weise der Dateibenennung die genaue Ransomware-Variante erkennen.

Je nach Netzwerkverzögerung, der Anzahl der Dokumente und der Anzahl der angeschlossenen Geräte kann der Verschlüsselungsprozess von ein paar Minuten bis zu einigen Stunden dauern. Es hat Fälle gegeben, in denen die Ransomware in einem weit verteilten Netzwerk versucht, die Dateien im gesamten Netzwerk zu verschlüsseln. Für ein einzelnes Endgerät ist der Verschlüsselungsprozess jedoch meist eine Frage von Minuten.

5 Phase 5: Benachrichtigung des Benutzers und Cleanup

Nachdem die Sicherungskopien entfernt wurden und die Verschlüsselung abgeschlossen ist, werden die erpresserische Forderung und die Zahlungsanweisungen präsentiert. Häufig wird dem Opfer eine Zahlungsfrist von ein paar Tagen gesetzt, nach deren Ablauf die Lösegeldforderung steigt.

Anhand der Art und Weise, wie die Anweisungen erfolgen, können Sie möglicherweise feststellen, welche Ransomware das System angegriffen hat. Die Zahlungsanweisungen werden normalerweise auf der Festplatte gespeichert, manchmal in denselben Ordnern wie die verschlüsselten Dateien. In anderen Fällen werden sie an sehr spezifischen Orten auf der Festplatte gespeichert. So verwendet zum Beispiel CryptoWall Version 3 die Datei HELP_DECRYPT, um die Anweisungen zu speichern. In CryptoWall V4 heißt die Datei dagegen HELP-YOUR-FILES. Es gibt eine Reihe von verschiedenen Anweisungen und Varianten, doch in der Regel können Sie anhand dieser Leitlinie im Internet suchen und die genau Variante herausfinden.

Locky verfolgt einen anderen Ansatz: Diese Malware legt nicht nur Dateien auf dem System ab, sondern verändert auch den Bildschirmhintergrund des Benutzers so, dass die Anweisungen für die Entschlüsselung der Dateien dort angezeigt werden. Unübersehbarer kann die Zahlungsforderung wohl kaum sein.

Und ähnlich wie bei den Nachrichten in „Mission Impossible“, die sich selbst zerstören, entfernt sich die Malware schließlich selbst vom befallenen System, um keine nennenswerten Spuren zu hinterlassen, die helfen würden, bessere Abwehrmechanismen gegen sie zu entwickeln. Aufgrund der Selbstentfernung des Schadcodes sollten keine bösartigen Dateien auf dem System zurückbleiben und somit auch keine Bedrohungen, wenngleich sich die Experten da nicht sicher sind. „Obwohl die Ransomware sich selbst entfernt, empfehlen wir Ihnen, die betroffenen Computer wenn möglich zu ersetzen und nicht nur zu reinigen“, rät Sommers.

Die 5 Verteidigungsschritte: Umgang mit einem Ransomware-Angriff

Nachdem wir nun verstanden haben, wie Ransomware typischerweise agiert, sehen wir uns an, was Sie tun können, um einen solchen Angriff abzuwehren. Wir orientieren uns dabei an den einzelnen Schritten, die das SANS Institute, das NIST und die US-Marine in ihren Frameworks zur Behandlung von Sicherheitsereignissen vorsehen: Vorbereitung, Entdeckung, Eindämmung, Ausmerzung und Wiederherstellung.

1

Schritt 1: Vorbereitung

Ransomware-Angriffe nehmen an Häufigkeit und Schwere zu. Sie müssen Ihr Unternehmen auf die sehr reale Möglichkeit eines Angriffs vorbereiten.

Patchen Sie offensiv

Weil Malware oft über bekannte Sicherheitslücken ins System gelangt, besteht die beste Abwehrmaßnahme darin, Ihre Systeme offensiv zu patchen. Das ist im Übrigen nichts anderes als eine der Sicherheitskontrollen aus den „Top 20 Critical Security Controls for Effective Cyber Defence" des SANS Institutes: kontinuierliche Bewertung und Beseitigung von Sicherheitslücken. Wenn Sie Sicherheitslücken beseitigen, hat die Malware möglicherweise keine Chance, überhaupt auf Ihre Computer zu gelangen.

Erstellen Sie Backups und schützen Sie sie

Ransomware vernichtet Sicherungsdateien und verschlüsselt normale Dateien, und dies setzt Ihr Unternehmen einem großen Schadenspotenzial aus. Daher sollten Sie unbedingt häufig alle Dokumente an einem Ort sichern, der von Ransomware nicht befallen werden kann (z.B. Offline-Speicher), und dann prüfen, ob diese Dateien bei Bedarf leicht wiederhergestellt werden können. Selbst Netzwerkfreigaben oder Cloud-Speicher sind möglicherweise nicht völlig sicher, da Dateien, die von der Ransomware bereits verschlüsselt oder beschädigt wurden, womöglich automatisch im Netzwerk oder in der Cloud gesichert werden, sodass die Dateien an diesen Speicherorten dann ebenfalls beschädigt sind.

Erstellen Sie einen Notfallplan

Ihr Unternehmen sollte einen Notfallreaktionsplan entwickeln, der speziell auf einen Ransomware-Angriff abgestimmt ist. Dieser Schritt ist besonders wichtig, um sich auf gezielte Angriffe vorzubereiten, die große Teile Ihres Unternehmens betreffen können. Der Plan sollte die spezifischen Maßnahmen ausführen, die die Mitarbeiter ergreifen sollten, sobald deutlich wird, dass ein Angriff im Gang ist. Dies wird eine zügige Reaktion erleichtern in einer Situation, in der schnelles Handeln die entscheidende Voraussetzung ist, um eine gravierende Bedrohung zu stoppen oder einzudämmen. In ähnlicher Weise sollten Sie speziell für diese Art von Angriff einen Notfallwiederherstellungsplan entwickeln. „Mit einer guten Planung und einer bestimmten Handlungsweise kann die Auswirkung eines Angriffs auf Ihr Unternehmen minimiert werden", so Sommers.

Vergeben Sie möglichst wenige Berechtigungen

Ein entscheidender Aspekt der Verteidigung gegen Ransomware ist die Vergabe von möglichst wenigen Berechtigungen, insbesondere wenn es um den Austausch von Dateien geht. Viele Unternehmen verfügen über ein Filesharing-System, das allen im Unternehmen zugänglich ist. Bestimmte Orte sind vielleicht schreibgeschützt oder nur bestimmten Benutzern zugänglich, doch viele Unternehmen arbeiten mit einer monolithischen Filesharing-Struktur. Der Wechsel zur Vergabe einer minimalen Anzahl von Zugriffsberechtigungen nach Bedarf kann den Schaden, den eine Ransomware-Infektion verursacht, deutlich verringern.

Nutzen Sie relevante Informationsquellen

Ein weiterer wichtiger Schritt in der Vorbereitungsphase besteht darin, Branchen- und Bedrohungsinformationen aus geeigneten Quellen oder Branchenlisten zu nutzen, die sich speziell auf Crimeware oder Ransomware konzentrieren, und diese Indikatoren regelmäßig in Erkennungsmechanismen wie Intrusion Detection Systeme (IDS) einzuspeisen.

Schützen Sie Ihre Endpunkte

Ihr Unternehmen kann Tools zum Schutz der Endpunkte einsetzen, die in der Lage sind, Infektionen frühzeitig zu erkennen und automatisch darauf zu reagieren. Tools wie LogRhythm System Monitor können solche Infektionen frühzeitig erkennen und schnell und automatisch auf sie reagieren, damit sie nicht zu großen Problemen werden.

Klären Sie die Benutzer auf

Benutzersensibilisierung ist ein effektives Mittel, um den Nutzern zu zeigen, wie sie es von vornherein vermeiden, auf Phishing-Mails hereinzufallen, die Malware einschleusen. Viele Angreifer stützen sich auf Social Engineering-Taktiken, die immer ausgefeilter werden. Die Endbenutzer müssen wissen, womit sie rechnen und worauf sie in ihren Nachrichten achten müssen, um eine Infektion zu vermeiden.

Schließen Sie eine Versicherung ab

Die Kosten eines Ransomware-Angriffs können ziemlich hoch sein – nicht nur das Lösegeld an sich verursacht Kosten, sondern auch der Geschäftsausfall während der Zeit, in der Dateien und Dokumente nicht verfügbar sind. So war etwa das Hollywood Presbyterian Medical Center komplett lahmgelegt, als es im Februar 2016 den Ransomware-Angriff erlitt. Die Abteilung für Strahlenonkologie wurde geschlossen und CTs und Laborarbeit waren nicht verfügbar. Betroffene Patienten wurden in andere Einrichtungen überstellt oder einfach abgelehnt.[8] Dass das Krankenhaus mehr als eine Woche lang seine normalen Dienste nicht erbringen konnte, war für seine Finanzen eine enorme Belastung.

James Carder, CISO bei LogRhythm und Vice President von LogRhythm Labs, rät Unternehmen, eine gute Cyber-Versicherung abzuschließen, die ausdrücklich Verluste durch Ransomware abdeckt. „Wenn Sie Umsatzeinbußen durch eine Ransomware-Infektion erleiden, können Sie möglicherweise Ihre Cyber-Versicherung in Anspruch nehmen, um diese Verluste zu decken", so Carder. „Von der reinen Risikomanagementperspektive aus gesehen, ist eine wirklich gute Cyber-Versicherung in solchen Fällen wahrscheinlich Gold wert."

2 Schritt 2: Entdeckung

Wird Ihr Unternehmen von einem Angriff getroffen, können Sie den Schaden minimieren, wenn Sie die Malware frühzeitig entdecken.

Vorbereiten Ihrer Abwehrmechanismen

Im Hinblick auf die anfängliche Ausnutzung und Infektion besteht eine gute Abwehrmaßnahme darin, Signaturen und IOCs in Ihrem IDS und anderen Netzwerkgeräten einzurichten. Verwenden Sie Ihre Bedrohungsinformationsquellen, um Anomalien, die mit Ransomware zusammenhängen können, in Ihrem Netzwerktraffic zu blockieren oder zumindest Warnungen auszulösen. Die meisten großen IDS-Anbieter verfügen über zahlreiche Signaturen für CryptoWall- und Locky-Traffic. Sie hängen aber meistens von der Malwareversion ab und können sich ändern. Daher brauchen Sie mehr Abwehrmaßnahmen als nur die Erkennung. Trotzdem können diese Signaturen eine gute Informationsquelle für die Tools sein, die die meisten Unternehmen nutzen.

Prüfen Sie E-Mails auf bösartige Links und Schadwirkung

Ihre beste automatisierte Abwehr gegen Phishing-Mails, die Ransomware enthalten oder die Benutzer zu solcher Malware leiten, sind Tools, die bösartige Anhänge erkennen oder E-Mails auf ausführbare Anhänge überprüfen.

Verwenden Sie Regeln zur Blockade ausführbarer Dateien

Zwei Bereiche, von denen aus Ransomware typischerweise ausgeführt wird, sind die Order %APPDATA% und %TEMP% auf Ihrem System. Nach Dateien Ausschau zu halten, die von dort aus ausgeführt werden, ist ein gutes Mittel, um Ransomware zu erkennen, bevor sie überhaupt eine Gelegenheit hat, Dateien zu verschlüsseln. LogRhythm hat Regeln entwickelt, mit denen unsere Tools Dateiausführungen von diesen Ordnern überwachen sowie prüfen können, wo im System Dateien ausgeführt werden und ob Anweisungen erstellt werden.

Ähnlich wie in der Ausnutzungsphase können Netzwerkregeln auch eingesetzt werden, um die Bereitstellung und Ausführung der ausführbaren Datei zu erkennen, insbesondere in Fällen wie CryptoLocker, in denen es eine sehr vorhersehbare Sequenz von Ereignissen gibt, um den Diffie-Hellman-Schlüsselaustausch zu organisieren. Sie können dafür sorgen, dass diese in Ihrem IDS eine Blockade auslösen. Wenn Sie zum Beispiel bei CryptoLocker in der Lage sind, den Schlüsselaustausch zu blockieren, dann könnten Sie tatsächlich verhindern, dass Dateien verschlüsselt werden, da die Malware über den Versuch, diesen Schlüssel einzurichten, nicht hinauskommen wird.

Die Vernichtung von Sicherungskopien ist ein weiteres zentrales Merkmal, an dem sich die Ransomware CryptoLocker erkennen lässt, bevor sie überhaupt die Möglichkeit zur Ausführung hat. Achten Sie besonders auf die Ausführung des Befehls vssadmin. Dieser Ansatz wird sehr häufig verwendet, und falls Sie über die Tools oder die Protokollierung verfügen, um eine Warnung auszulösen, wenn das admin-Tool ausgeführt wird, können Sie Maßnahmen ergreifen und vielleicht verhindern, dass die Laptop- oder die Netzwerkfreigaben verschlüsselt werden.

[8]Venturebeat, „Next wave of ransomware could demand $millions", 26. März 2016

Halten Sie nach Hinweisen auf Verschlüsselung und Benachrichtigungen Ausschau

Die Dateiverschlüsselungsphase beginnt normalerweise mit einem Schlüsselaustausch, der über Netzwerksignaturen, Dateinamenmuster und Registry-Änderungen auf dem lokalen System erkannt werden kann. Die Suche nach Dateien mit der Erweiterung .locky ist eine gute Methode, um zu erkennen, dass Locky dabei ist, Dateien auf einem System zu verschlüsseln. In ähnlicher Weise ist bei CryptoWall die Suche nach den zufälligen Dateinamenmustern eine weitere Methode, um Ransomware beim eigentlichen Ausführen zu erkennen.

Und schließlich: Wenn Sie erkennen können, dass Dateien zur Benachrichtigung der Benutzer im System abgelegt werden, sind die Malware-Aktivitäten zwar leider schon weit fortgeschritten, doch sind Sie dann in der Regel zumindest über die Verschlüsselung informiert, auch wenn Sie sie nicht blocken konnten. Eine schnelle Erkennung in diesem Stadium kann Ihnen helfen, die Situation einzudämmen.

3 Schritt 3: Eindämmung

Wenn die Ransomware ihre Arbeit bereits auf einem Gerät erledigt hat, gibt es Maßnahmen, die Sie ergreifen können, um sie lokal einzudämmen, sodass die Netzwerkdateien nicht befallen werden.

Unterbrechen Sie die laufenden Prozesse und isolieren Sie den befallenen Endpunkt

Ein Endpunktschutzsystem, das nach der Ausführung Ausschau halten und den Prozess abbrechen kann, ist meistens die beste Eindämmungsmethode. Doch viele Unternehmen verfügen nicht über eine solche Lösung. Aus diesem Grund hat LogRythm Technologien entwickelt, die den lokalen Host blockieren und vom Netzwerk isolieren, sobald eine Infektion - beispielsweise mit CryptoWall - entdeckt wird. „Wenn LogRhythm die Ransomware erkennt, können wir diese Netzwerkverbindung kappen, sodass CryptoWall zwar vielleicht den Endpunkt erreicht, aber nicht in der Lage ist, die Dateien im Netzwerk zu verschlüsseln“, erklärt Sommers. „Man müsste sich also höchstens um die Dateien auf dem lokalen System Sorgen machen, aber man kann versuchen, dieses System so schnell wie möglich herunterzufahren, sodass so wenig Dateien wie möglich verschlüsselt werden.“

Im Falle eines gezielten Angriffs stellen Sie sicher, dass Sie den gesamten Vorfall erfasst haben, und entwickeln Sie dann schnell einen Eindämmungsplan. Im Unterschied zu einer Massenverbreitung, bei der man es meistens mit einem, zwei oder vielleicht ein paar infizierten Hosts zu tun hat, sind von einem gezielten Angriff meist mehr Systeme betroffen. Daher müssen Sie das gesamte Ausmaß des Angriffs erfassen. Sie müssen den Angreifer aus dem gesamten System bekommen, anstatt ihn in mühsamer Kleinarbeit von einem Rechner nach dem anderen zu entfernen. Dies ist ein Fall, in dem wir sehr empfehlen, das System neu aufzubauen, statt es zu reinigen. Möglicherweise haben die Angreifer latente Tools eingerichtet, die Ihnen entgehen könnten, wenn Sie versuchen, das System zu reinigen. Wenn Sie es neu aufbauen, haben Sie deutlich bessere Chancen, neu anzufangen und den Angriff vollständig rückgängig zu machen.

Wenn LogRhythm die Ransomware erkennt, können wir diese Netzwerkverbindung kappen, sodass CryptoWall zwar vielleicht den Endpunkt erreicht, aber nicht in der Lage ist, die Dateien im Netzwerk zu verschlüsseln“, erklärt Sommers.
„Man müsste sich also höchstens um die Dateien auf dem lokalen System Sorgen machen, aber man kann versuchen, dieses System so schnell wie möglich herunterzufahren, sodass so wenig Dateien wie möglich verschlüsselt werden.

4 Schritt 4: Ausmerzung

Sobald Sie einen Ransomware-Vorfall erkannt und erfolgreich eingedämmt haben, müssen Sie die Malware in Ihrem Netzwerk ausmerzen.

Ersetzen, Neuaufbauen oder Reinigen der Geräte

Wir empfehlen normalerweise, die Geräte zu ersetzen, statt nur zu reinigen. Denn wie bei jeder Art von Malware ist es schwierig herauszufinden, ob Restdateien auf dem System versteckt sind und die Geräte wieder infizieren können. Doch für Netzwerkbereiche wie E-Mail-Fächer oder Filesharing ist es manchmal sinnvoller, sie zu reinigen und die bösartige E-Mail-Nachricht aus dem E-Mail-Fach oder die Ransomware-Anweisungen aus den gemeinsam nutzbaren Dateien zu entfernen. Wenn Sie sich entscheiden, Geräte zu reinigen statt zu ersetzen, achten Sie weiterhin auf Signaturen und andere IOCs, um ein erneutes Auftreten des Angriffs zu verhindern.

5 Schritt 5: Wiederherstellung

Folgen Sie Ihrem Notfallwiederherstellungsplan, um alle Systeme wieder zum Laufen zu bringen und zum normalen Geschäftsablauf zurückzukehren.

Wiederherstellen von einer sauberen Sicherungskopie

Die wichtigste Aufgabe, um zum Normalzustand zurückkehren zu können, wird die Wiederherstellung von der Sicherungskopie sein. Wenn Sie gute, geprüfte Backups haben, können Sie jedes Ransomware-Ereignis leicht bewältigen, indem Sie einfach Ihre Systeme ersetzen oder reinigen und aus Sicherungskopien die Dateien wiederherstellen. Sie werden vielleicht einen Ausfall von ein paar Stunden haben, da Sie Zeit brauchen, um die Wiederherstellung aus der Sicherungskopie vorzunehmen, aber es sollte kein Riesenproblem sein, das Sie mehrere Tage beschäftigt.

Suchen Sie nach dem Infektionsvektor

Bei den meisten Ransomware-Untersuchungen sollten Sie die Wiederherstellungsphase abschließen, indem Sie gründlich untersuchen, welcher spezifische Infektionsvektor gegen das System verwendet wurde. War es eine Phishing-E-Mail oder ein webbasiertes Angriffskit? Wenn es ein webbasiertes Angriffskit war, wie ist der Benutzer dann zu dieser Website gelangt?

Die Analytiker bei LogRhythm erleben immer wieder, dass Opfer nichts anderes getan haben, als via Google nach Antworten auf IT-Fragen zu suchen. „Als die Leute auf eine scheinbar harmlose Antwortseite gingen, wurden sie auf strategisch manipulierte Websites weitergeleitet, die sie dann mit dem Angler-Exploit-Kit infizierten. Zu wissen, wie die Ransomware auf Ihr System gelangt ist, kann Ihnen helfen, Ihre Abwehrmechanismen besser zu trimmen und Ihre Erkennungsmechanismen in Zukunft zu lenken“, so Sommers.

Informieren Sie gegebenenfalls die Strafverfolgungsbehörden

Das United States Computer Emergency Readiness Team (US-CERT) des U.S. Department of Homeland Security fordert Benutzer und Administratoren, die eine Ransomware-Infektion erleiden, dazu auf, den Vorfall über das Internet Crime Complaint Center unter http://www.ic3.gov/default.aspx an des FBI zu melden. Schließlich stellt das Verbreiten und Ausführen bösartiger Software in den Vereinigten Staaten und vielen anderen Ländern eine Straftat dar.

> *Zu wissen, wie die Ransomware auf Ihr System gelangt ist, kann Ihnen helfen, Ihre Abwehrmechanismen besser zu trimmen und Ihre Erkennungsmechanismen in Zukunft zu lenken, so Sommers.*

FAZIT

Ransomware-Angriffe gegen Unternehmen gewinnen zunehmend an Dynamik. Im ersten Quartal 2016 wurden Krankenhäuser und andere Gesundheitseinrichtungen in den gesamten USA von einer Flut von Angriffen heimgesucht. IT-Sicherheitsexperten rechnen damit, dass es noch deutlich schlimmer wird. Weil diese Angriffe für die Täter so lukrativ sind, werden sie sicherlich häufiger, noch schädlicher und deutlich teurer werden. Außerdem ist fast jedes Unternehmen – ob groß oder klein – anfällig für Ransomware-Angriffe.

Die Auswirkungen eines erfolgreichen Angriffs auf ein Unternehmen gehen weit über die Kosten hinaus, die das Lösegeld verursacht. Zu den möglichen Folgen zählen Produktivitätsverluste, Geschäftsausfälle, Unannehmlichkeiten für Kunden und potenziell dauerhafte Datenverluste.

Der Erfolg Ihres Unternehmens bei der Abwehr von Ransomware-Angriffen hängt stark von Ihrer Vorbereitung und den Tools ab, die Sie einsetzen, um Ihre Systeme zu überwachen und verdächtige Aktivitäten zu erkennen, zu beenden und einzudämmen. Wir laden Sie ein, Ihren lokalen LogRhythm-Vertreter zu kontaktieren, um zu erörtern, inwieweit Ihr Unternehmen vorbereitet ist. LogRhythm kann Ihnen die Tools und das Fachwissen liefern, die Ihnen helfen können, Ihr Unternehmen gegen Ransomware und andere IT-Sicherheitsangriffe zu verteidigen.

Über LogRhythm

LogRhythm, ein führendes Unternehmen für Security Intelligence und Analysen, unterstützt Unternehmen weltweit dabei, gefährliche Cyber-Bedrohungen aufzuspüren, abzuwehren und zu entschärfen. Die patentierte und preisgekrönte Plattform des Unternehmens vereint auf einzigartige Weise SIEM der nächsten Generation mit Protokollverwaltung, Netzwerk- und Endpunktforensik sowie fortschrittlichen Sicherheitsanalysen. LogRhythm schützt Kunden nicht nur vor den Risiken in Zusammenhang mit Cyber-Bedrohungen, sondern bietet darüber hinaus einzigartige Funktionalitäten zur Automatisierung und Gewährleistung der Compliance sowie erweiterte IT-Intelligence.

Die marktführende Rolle von LogRhythm spiegelt sich auch in vielen Auszeichnungen wider. Das Unternehmen ist im Magic Quadrant-Bericht von Gartner zum Thema SIEM seit vier Jahren in Folge als „Leader" positioniert, wurde im SIEM Vendor Landscape-Bericht 2014/15 der Info-Tech Research Group als „Champion" ausgezeichnet und im SIEM Appliance Buyer's Guide von DCIG 2014/15 als „Best-in-Class" (Nr. 1) eingestuft. Darüber hinaus erhielt LogRhythm drei Jahre in Folge den SIEM Global Market Penetration Leadership-Preis von Frost & Sullivan und wurde von der Denver Post als hervorragender Arbeitgeber ausgezeichnet. LogRhythm hat seinen Hauptsitz in Boulder, Colorado (USA), und verfügt über Niederlassungen in Nord- und Südamerika, Europa und der Region Asien-Pazifik.

Zusätzliche Ressourcen

- LogRhythm hat ein Webinar zur Verteidigung Ihres Unternehmens gegen Ransomware aufgezeichnet: https://logrhythm.com/resources/webcasts/protecting-your-business-from-ransomware/
- Weitere Informationen zu CryptoLocker finden Sie hier: https://www.us-cert.gov/ncas/alerts/TA13-309A.
- US-CERT-Warnung zu Crypto-Ransomware: https://www.us-cert.gov/ncas/alerts/TA14-295A
- Veröffentlichung des SANS Institute zur Identifizierung und Abwehr von Crypto-Ransomware (und zerstörerischer Malware):
- https://digital-forensics.sans.org/blog/2015/04/03/identifying-and-disrupting-crypto-ransomware-and-destructive-malware

© Copyright 2016, LogRhythm, Inc. Alle Markenzeichen, Dienstleistungsmarken und Handelsnamen, die hier aufgeführt werden, sind Eigentum ihrer jeweiligen Inhaber.