SANS

Analyst Program

Whitepaper

SANS 2022 Bericht zur Ransomware-Abwehr

Autor: **Matt Bromiley**

März 2022

cisco SECURE

corelight

ExtraHop

Gigamon®

MORPHISEC

Die Ransomware-Ära

Die Jahre 2020 und 2021 waren zweifelsohne die Jahre der Ransomware. Angesichts der anhaltenden COVID-19-Pandemie, der zunehmenden Zahl von remote Arbeitenden und der weit verbreiteten Einführung neuer Technologien mangelte es Angreifern nicht an Möglichkeiten. Diese Änderungen gingen einher mit einer Reihe kritischer, weit verbreiteter Sicherheitslücken und groß angelegter Kompromittierungen der Lieferkette, die viele Unternehmen dem Risiko von Ransomware-Angriffen aussetzten.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) stellte fest, dass Ransomware-Angriffe zwischen April 2020 und Juli 2021 um 150 % zugenommen haben.[1] In dem Bericht wurde auch festgestellt, dass Ransomware-Angreifer im vergangenen Jahr in ihren Forderungen und Vorgehensweisen dreister geworden sind, wobei das Geschäftsmodell Ransomware-as-a-Service (RaaS) neue Trends gesetzt und Rekorde gebrochen hat. RaaS verschärft das Ransomware-Problem nur, da es die Eintrittsschwelle für einen Ransomware-Angriff buchstäblich für jeden ermöglicht, der Zugang zu Kryptowährungen hat.

Auch wenn sich die Situation durch Ransomware-Angreifer und -Angriffe verschlechtert hat, sind Unternehmen und Sicherheitsteams ihnen nicht komplett ausgeliefert. In den letzten zwei Jahren haben sich die Cybersicherheitstechnologien zur Erkennung von und Reaktion auf Vorfälle weiterentwickelt. In der Tat konzentrieren sich viele Unternehmen erfolgreich auf die Verhinderung von Ransomware- und Malware-Angriffen, um Angreifern, die sich der Erkennung entziehen wollen, einen Schritt voraus zu sein. Viele Organisationen setzen derzeit auf Lösungen und Plattformen, die einen ganzheitlichen Blick auf das Unternehmen ermöglichen. Andere Teams nutzen die Veränderungen, die sich durch die Pandemie ergeben haben, um die Sicherheitsausgaben zu erhöhen, neue Tools anzuschaffen oder Projekte voranzutreiben, die bereits als gescheitert galten.

Wie das Sprichwort sagt, ist Erfahrung der beste Lehrmeister. Im Falle von Datenschutzverletzungen und Ransomware möchten wir die Angreifer jedoch lieber schon im Vorfeld studieren und sicherstellen, dass sie niemals ungehinderten Zugang zu unseren Netzwerken haben. Lesen Sie dieses Whitepaper, um potenzielle Sicherheitsrisiken in Ihrer Umgebung zu identifizieren und diese zu eliminieren, bevor ein Angreifer sie ausnutzt.

In diesem Whitepaper befassen wir uns mit diesen beiden übergeordneten Konzepten: Was sind die aktuellen Trends bei Ransomware, und was können Unternehmen tun, um sich zu schützen (oder besser zu schützen)? Das grundlegende Konzept von Ransomware bleibt das gleiche: Daten werden verschlüsselt und es wird Geld für die Entschlüsselung verlangt. Wenn Sie jedoch schon einmal einen Ransomware-Vorfall erlebt haben, wissen Sie, dass es nicht ganz so einfach ist. Es hat den Anschein, dass alles schlimmer geworden ist, vor allem, wenn man bedenkt, dass die Angreifer sich vermehrt gut vorbereiten und ihre Ziele genau kennen.

Genauso wie die Angreifer ihre Techniken verändert haben, haben sich auch die Unternehmen verändert. Sehen wir uns beides an, und versuchen wir Bereich zu finden, in denen Sicherheitsteams erfolgreich agieren können. Gibt es Verfahren oder Tools, um Angriffe auf die Umgebung verhindern oder früher in der Angriffskette erkennen zu können? Gibt es bei Ransomware-Angriffen einen bestimmten „Knackpunkt“, der eine Möglichkeit zur Erkennung bietet? Oder noch besser: Nutzen die Angreifer gleiche Taktiken, und können wir, wenn wir die Taktik eines Angreifers kennen, viele andere Angreifer stoppen?

[1] www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Angriffstrends

Leider modernisieren Ransomware-Bedrohungsakteure ihre Operationen ständig und aktualisieren ihre Techniken, Taktiken und Verfahren (auch als „TTPs“ bezeichnet) laufend. Das geht so weit, dass Ransomware-Akteure fast schon auf sarkastische Art und Weise Unternehmen Ratschläge zu ihren Sicherheitsmaßnahmen und -implementierungen erteilen. Das heißt zwar nicht, dass diese völlig falsch sind, aber häufig wurden diese spezifischen Bedrohungsmaßnahmen entweder von Ransomware-Bedrohungsakteuren genutzt oder zur schnellen Durchführung von Ransomware-Angriffen eingesetzt.

Kenntnis des operativen Betriebes und der Angriffsfläche von Umgebungen der Opfer

Lassen Sie nicht zu, dass ein Angreifer mehr über Ihre Perimeter weiß als Ihr Sicherheitsteam. Ob es Ihnen gefällt oder nicht – die Angreifer informieren sich in einer ersten Aufklärungsphase eines Angriffs genau über ihre Opfer. Diese Hintergrundrecherche trägt dazu bei, die Glaubwürdigkeit der Bedrohung zu erhöhen, wenn sie eine Lösegeldzahlung fordern, und ermöglicht es ihnen, potenziell mehr Bereiche der Umgebung zu sperren.

Ransomware-Akteure haben immer wieder, und in den letzten zwei Jahren vielleicht sogar vermehrt, die Umgebungen ihrer Opfer vor einem Angriff genau untersucht und Wissen darüber erlangt. Zu diesem Wissen gehören häufig betriebliche und finanzielle Details wie Jahresbudgets, die Anzahl der Mitarbeitenden und/oder Umsatzstatistiken. So wurde beispielsweise im April 2021 versucht, die öffentlichen Schulen von Broward County in Florida durch einen Ransomware-Angriff als „Geiseln“ zu nehmen. Als die Angreifer eine Lösegeldzahlung in Höhe von 40 Millionen Dollar verlangten, wiesen sie den Schulbezirk darauf hin, dass diese Forderung lediglich 1 % des Jahresbudgets von 4 Milliarden Dollar ausmachte.[2]

Das Wissen der Angreifer über ihre Opfer umfasst oft auch das Wissen über die gesamte Angriffsfläche des Opfers. Die Angriffsfläche einer Organisation kann unter anderem Folgendes umfassen:

- Systeme und Dienste mit Internetzugriff
- Schwachstellen oder nicht gepatchte Systeme
- Nutzung spezifischer Technologien wie etwa von Sicherheitslösungen oder Drittanbietern
- Potenzieller Cloud-Footprint

Wir gehen sogar so weit zu behaupten, dass der Erwerb solcher Informationen durch Angreifer nicht nur äußerst geschickt ist, sondern auch die Wahrscheinlichkeit erhöht, dass ein Angreifer sein „Lösegeld“ erhält (weil er anscheinend mehr über seine Opfer weiß). Außerdem kann der Angreifer das ihm zum Opfer gefallene Unternehmen auf verschiedene Weise erpressen, vor allem, wenn die Sicherheitsvorkehrungen des Unternehmens unzureichend sind, so dass der Angreifer die Möglichkeit eines erneuten Eindringens hat.

Wir möchten Angreifern keinesfalls zu guten TTPs oder Aktionen gratulieren, aber wir müssen zugeben, dass es eine clevere Taktik ist, seine „Hausaufgaben“ in Bezug auf das für einen Angriff anvisierte Unternehmen zu machen.

Tipp zur Verteidigung

Sie können nicht jeden Aspekt Ihres digitalen Footprints kontrollieren – aber sich dessen bewusst zu sein, ist der erste Schritt. In einigen Fällen, in denen das Sicherheitsteam direkt verantwortlich ist, kann das Fehlen von Patches oder die Verwendung veralteter oder anderweitig anfälliger Software ein Unternehmen einem erheblichen Risiko aussetzen. Warten Sie nicht darauf, dass ein Angreifer mehr über Ihre Angriffsfläche in Erfahrung bringt und dies dann ausnutzt, bevor Sie versuchen, einen Angriff zu verhindern oder darauf zu reagieren.

[2] „Large Florida school district hit by ransomware attack“, https://apnews.com/article/technology-fort-lauderdale-florida-ac217a0759194dc3c717b421ae05bd0c

Schnelles „Bewaffnen“

Nach der Bekanntgabe eines neuen Sicherheitsrisikos beginnt oft ein Wettlauf zwischen Angreifern und den sich verteidigenden Unternehmen im Hinblick darauf, wer das Sicherheitsrisiko schneller ausnutzen oder patchen kann. Hierbei hat der Angreifer häufig die Oberhand, weil er einfacher und schneller Exploit-Code schreiben kann, als ein Unternehmen ein Patch anwenden, da Change-Control-Prozesse durchlaufen werden müssen oder, noch schlimmer, gerade ein Änderungsstopp vorliegt. Ein Trend bei Ransomware-Bedrohungsakteuren ist es, den Wettlauf bei dieser „Bewaffnung“ nicht nur zu gewinnen, sondern ihn auch schnell zu gewinnen.

Wir müssen uns nur die Exchange-Sicherheitslücken vom März und April 2021 oder von Log4j im Dezember 2021 ansehen, um zu erkennen, wie schnell die Angreifer von anfälligem Code zu einem funktionierenden Exploit übergehen. Bereits wenige Stunden nach der Bekanntgabe der Sicherheitsrisiken war funktionierender Proof-of-Concept-Code (PoC) im Internet verfügbar, und Angreifer nutzten die Sicherheitsrisiken schnell aus, bevor Sicherheitsteams überhaupt von einem Patch wussten.

Tipp zur Verteidigung

Patching – häufig einfacher gesagt als getan. Leider ist das Patching manchmal der effizienteste Weg, um sich gegen einen bevorstehenden Exploit zu verteidigen, auch wenn dies bedeutet, dass bestehende Change-Controls unterlaufen werden müssen oder jemand mitten in der Nacht geweckt werden muss. Letztendlich ist es besser, ein Notfall-Patch zu erstellen, als auf einen aktiven Eindringungsversuch zu reagieren. Der erste Schritt beim Beheben eines Cybersecurity-Risikos ist der, es zu kennen. Ungepatchte Schwachstellen gehören zu den größten Risiken, und sie sind die ersten Angriffsvektoren, die Angreifer nutzen. Remotearbeit und die digitale Transformation haben die Verwaltung von Sicherheitslücken in wichtigen Softwareanwendungen erschwert. Die besten Lösungen vereinfachen und automatisieren das Management von Sicherheitsrisiken, indem sie die von Ihrem Team am häufigsten genutzten Anwendungen in Verbindung mit nicht gepatchten, bekannten Sicherheitsrisiken priorisieren und so sicherstellen, dass Sie zuerst die größten Risiken auf möglichst effiziente Weise reduzieren können.

Natürlich ist diese schnelle „Bewaffnung“ nicht unbedingt mit einem Ransomware-Angriff gleichzusetzen. Auch fortgeschrittene Bedrohungsakteure aus dem Bereich der State-Nexus-Bedrohungen agieren mit hoher Geschwindigkeit, um Sicherheitsrisiken auszunutzen und sich dauerhaft in einer Umgebung festzusetzen. In einigen Fällen hat dies sogar dazu geführt, dass mehrere Bedrohungsakteure versucht haben, über dasselbe Sicherheitsrisiko in ein Zielunternehmen einzudringen. Dadurch entsteht für diejenigen, die sich verteidigen müssen, eine einzigartige „Einer-gegen-viele“-Situation: Sie müssen nur einen Patch anwenden, um mehrere Bedrohungsakteure auszuschalten.

Wenn Sie jedoch ein anfälliges und/oder nach außen gerichtetes System nicht so schnell patchen können, wie Sie es gerne tun würden, sollten Sie als Notlösung Netzwerk- und Endpunktalternativen in Betracht ziehen. Nutzen Sie vorhandene technologische Kontrollen, um nach Möglichkeiten zur Prävention, Erkennung und Reaktion zu suchen. Eine schnell umgesetzte Netzwerkregel oder eine Endpunktsignatur und verhaltensorientierter Schutz sind Beispiele für zuverlässige Schutzmaßnahmen, die Sie zur Überbrückung nutzen können, bis das Unternehmen die Anwendbarkeit von Patches beurteilen kann.

Das jüngste Log4j-Sicherheitsrisiko ist ein sehr gutes Beispiel für die Verwendung von Signaturen, um das Patchen zu minimieren und Zeit zu gewinnen. Es waren mehrere Signaturen verfügbar, sowohl für Netzwerke als auch für Endpunkte. Unternehmen konnten diese zur Erkennung eingehender bösartiger Pakete und Aktivitäten nach der Kompromittierung verwenden. Unternehmen, die diese Signaturen schnell nutzen konnten, hatten die Möglichkeit, dem Anwendungsteam Zeit zu geben, um alle Optionen auszuloten und angemessen zu reagieren.

Angriffe ohne Dateien oder Malware

Ein zunehmender Trend bei Angreifern besteht darin, beim Eindringen so wenig Malware wie möglich zu nutzen. Dies spiegelt die Versuche der Angreifer wider, sich der Erkennung so weit wie möglich zu entziehen, bis sie den eigentlichen Ransomware-Verschlüsseler in die Umgebung eingeführt haben. Einige TTPs der Angreifer nutzen dateilose oder speicherresidente Angriffe und/oder verwenden native Binärdateien, um keine zusätzliche Malware in die Umgebung einzuschleusen. Lassen Sie uns jeweils kurz darauf eingehen:

- **Dateilose Malware** umfasst Malware, die wenig oder gar keine Malware auf Datenträgern hinterlässt und stattdessen auf andere Speicherorte wie Windows Registry oder einen entfernten Speicherort zurückgreift, um bösartigen Code zu speichern. Allgemein gesprochen stellt dateilose Malware einen Versuch dar, der herkömmlichen dateibasierten Erkennung oder Kompromittierungsindikatoren (IoCs) zu entkommen. Dateilose Malware kann auch rein speicherresident sein. Dies bezeichnet Malware und/oder bösartigen Code, die oder der nur im Speicher existiert. Angreifer laden den Code direkt in den Speicher herunter und stellen ihn dort bereit, wobei sie auch hier dateibasierte oder herkömmliche Erkennungsmaßnahmen umgehen.
- Die Verwendung von **nativen Binärdateien** in einem System ist eine weitere Angriffstechnik, mit der herkömmliche Erkennungsmaßnahmen umgangen und der Angriff während des Eindringens verborgen werden sollen. „Living-off-the-Land"-Binärdateien (auch als „LOLBINS" bezeichnet) sind ausführbare Dateien, die bereits in einem Betriebssystem vorhanden sind. Angreifer haben Dutzende von Möglichkeiten aufgedeckt, diese Dateien zu manipulieren, um bösartige Ziele zu erreichen, wie etwa das Laden von Code in den Speicher, das Herunterladen einer Datei oder das Ausführen eines benutzerdefinierten Skripts.

Ebenso können Angreifer auf kompilierte Binärdateien verzichten und sich stattdessen auf benutzerdefinierte Skripte oder Exploit-Kits auf einem System des Opfers verlassen. In den letzten Jahren haben Angreifer zunehmend PowerShell und Post-Exploitation-Frameworks wie Cobalt Strike genutzt, um ihre Ziele zu erreichen. Obwohl Skripte und Exploit-Kits immer noch Artefakte auf Datenträgern hinterlassen können, bieten sie einem Angreifer eine Vielzahl von einfach auszunutzenden Möglichkeiten, mehrere Systeme zu kompromittieren und im Speicher zu verbleiben.

Tipp zur Verteidigung

Sich auf veraltete Schutzmaßnahmen wie die Analyse und Erkennung von Dateien auf Datenträgern zu verlassen, kann dazu führen, dass ein Angreifer leicht durch die Maschen schlüpft. Wenn ein Angreifer erst einmal die richtigen Anmeldedaten erlangt hat, gibt es nur noch wenig, was er nicht damit tun kann. Um sich gegen diese fortschrittlichen Techniken zu schützen, müssen Unternehmen präventive Funktionen für speicherinterne Analysen und Schutzmaßnahmen in Betracht ziehen.

Mithilfe von Technologie können wir heute starke Präventionsfunktionen implementieren, die eine In-Memory-Analyse von Code, geladenen Bibliotheken und anderen Aktivitäten ermöglichen. Indem wir Präventions- und Erkennungsfunktionen im Speicher unterbringen, kommen wir Angreifern näher als je zuvor. Dies bietet einen höheren Grad der sicheren Erkennung, aber auch eine Möglichkeit für gerissene Angreifer, die Endpunktüberwachung zu umgehen. Passen Sie Ihre Regeln entsprechend an und untersuchen Sie, wie mehrere Warnungen so zusammenspielen, dass sich ein umfassendes Bild ergibt.

In-Memory-Schutzmaßnahmen sind eine Möglichkeit, den Erfolg dieser Techniken zu begrenzen. Runtime-Analyse und In-Memory-Codeprüfung sind nur zwei der technologischen Entwicklungen, die Unternehmen bei der Verteidigung gegen fortschrittliche Angreifer helfen. Wir empfehlen Ihnen, die Möglichkeiten Ihrer aktuellen Tools zu prüfen und sich schlau zu machen, ob sie in der Lage sind, dateilose Malware aufzuhalten oder die Verwendung von LOLBINS zu analysieren, um bösartige Aktivitäten zu identifizieren.

Obwohl es sich nicht um eine Angreifertaktik handelt, ist eine weitere bemerkenswerte Veränderung in den letzten zwei Jahren (wie bereits erwähnt) die explosionsartige Zunahme von Ransomware-as-a-Service (RaaS). Durch das Anbieten kompletter Ransomware-Lösungen haben einige Angreifer als Mittelsmänner inzwischen mehr Geld verdient, als sie es als Angreifer getan hätten. Auch wenn die Explosion von RaaS die Ransomware-Angriffe an sich nicht verändert hat, so kann sich jedoch ändern, wer an der Tastatur sitzt oder welche TTPs verwendet werden.

Verstärkte Automatisierung

Ein weiterer Bereich, in dem Ransomware-Angreifer erfolgreich sind und/oder dem als Opfer auserkorenem Unternehmen voraus sind, ist der Grad der Automatisierung, den sie nutzen. Und dies ist äußerst ernst. Früher haben wir die Geschwindigkeit, mit der ein Angreifer agiert hat, in Tagen gemessen – heute messen wir dies in Stunden oder Minuten. In einem Blog-Beitrag von „The DFIR Report“ vom November 2021 wird ein Eindringen beschrieben, bei dem die Angreifer innerhalb von 42 Stunden die volle Kontrolle als Domänenadministrator übernommen und Ransomware eingeschleust hatten.[3] In einem anderen Beitrag wurde ein Angriff beschrieben, bei dem innerhalb von zwei Stunden die volle Kontrolle übernommen wurde.[4] Man kann gar nicht oft genug betonen, wie schnell Angreifer anhand der Fülle von Open-Source-Tools und automatisierten Prozessen ihre „Aufgabe“ erledigt haben, bevor ein Sicherheitsteam sie überhaupt entdeckt.

Zum Glück führt diese Automatisierung durch Angreifer aber auch zu einer vorhersehbaren und daher leicht zu entdeckenden Abfolge von Ereignissen. Angreifer schreiben Angriffsskripte in der Regel in betriebssystembasierten Programmiersprachen wie PowerShell oder Bash mit wiederholbaren Befehlen. Sicherheitsteams können viele davon zur Erstellung von Signaturen für die Erkennung verwenden. Darüber hinaus verwenden Angreifer zunehmend offensive Sicherheitstools, einschließlich Open-Source-Toolkits und -Skripte. Obwohl sie dem Angreifer einen Zeitvorteil für eine schnelle Bereitstellung verschaffen, hinterlassen sie jedoch auch vorhersehbare Spuren, die ein Unternehmen zum frühzeitigen Unterbinden eines Eindringungsversuchs nutzen kann.

Tipp zur Verteidigung

Interessanterweise ist die Automatisierung gleichzeitig das Problem als auch die Lösung. Genauso, wie es für Angreifer von Vorteil ist, Teile ihrer Angriffe und ihrer Infrastruktur zu automatisieren, kann dies auch für Sicherheitsteams Vorteile haben. Kurz gesagt könnten Sicherheitsteams von der Automatisierung der folgenden Aspekte profitieren:

- Informationsbasierte Erkennung über verschiedene Tools hinweg
- Erkennungsaktionen und -reaktionen, basierend auf Schweregrad, Kritikalität und System
- Response-Playbooks, die Aktionen auf niedriger Ebene automatisieren, so dass mehr Zeit für Analysen zur Verfügung steht, um sich mit wirklich wichtigen Problemen zu befassen

Ihre Möglichkeiten zur Automatisierung sind wahrscheinlich schneller greifbar, als Sie denken. Sie sollten sich die Automatisierungsfunktionen ansehen, die Ihnen Ihre aktuellen Controls und Plattformen bieten, oder sich erkundigen, welche Maßnahmen zu den bereits vorhandenen Controls hinzugefügt werden können. Wie in der Einleitung erwähnt, profitieren sowohl Angreifer als auch die sich verteidigenden Unternehmen von technologischen Fortschritten.

[3] „Exchange Exploit Leads to Domain Wide Ransomware“, https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/

[4] „From Zero to Domain Admins“, https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/

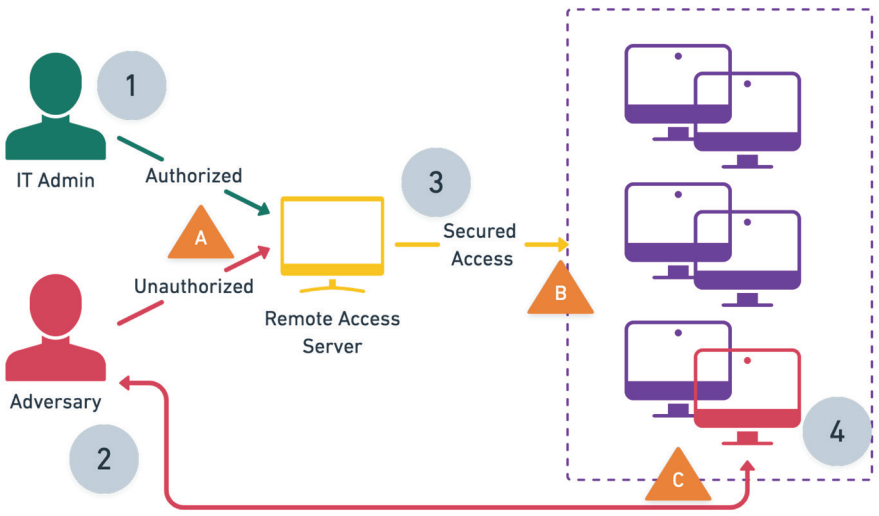
Ransomware-Abwehrmaßnahmen

Auch wenn wir beobachten, dass sich die Taktiken und Techniken von Ransomware-Angriffen ändern – dies bedeutet nicht, dass Unternehmen keine Chance haben, sich gegen diese Art von Angriffen zu wehren. Ganz im Gegenteil: Je mehr „Lärm“ Ransomware-Angreifer machen, desto mehr Möglichkeiten zur Erkennung gibt es. Ja, je mehr „Lärm“ sie machen, desto leichter ist es sogar, sie frühzeitig zu erkennen. In den folgenden Fallstudien werden einige Beispiele für Abwehr- und Gegenmaßnahmen beschrieben, und es wird erläutert, wie sich damit Ransomware-Angriffe abwehren lassen oder das Ransomware-Risiko mindern lässt.

Missbrauch beim Remotezugriff

Die erste Fallstudie befasst sich mit einem der beliebtesten Zugangsvektoren, der von Ransomware-Bedrohungsakteuren missbraucht wird: offene Tools und Lösungen für den Remotezugriff. Der Remotezugriff auf eine Umgebung ist nicht per se schlecht – viele Unternehmen nutzen Remotezugriff, um Verwaltungsfunktionen für eine Umgebung bereitzustellen. Dies ist häufig bei Zweigniederlassungen an anderen Standorten oder bei Mitarbeitenden erforderlich, die remote arbeiten (was in letzter Zeit ja stark zugenommen hat).

Problematisch wird es, wenn ein Unternehmen den Remotezugriff mit minimaler oder gar keiner Sicherheitskonfiguration, standardmäßigen oder leicht zu erratenden Anmeldeinformationen oder Ein-Faktor-Authentifizierung einrichtet. Schlimmer noch: Wenn eine Remotezugriffslösung anfällig wird und leicht ausgenutzt werden kann, können Angreifer dies ausnutzen, um die Kontrolle über eine legitime Installation zu übernehmen, selbst wenn die Sicherheitsimplementierungen ordnungsgemäß durchgeführt wurden.



Weg des Angreifers

1. Ein legitimer, autorisierter Benutzer greift auf die Umgebung über Ein-Faktor-Anmeldeinformationen zu.
2. Ein Angreifer erhält dieselben Anmeldeinformationen und kann sich ohne größere Probleme in der Umgebung anmelden.
3. Ist der Angreifer erst einmal eingedrungen, kann er sich problemlos zwischen Perimeter und internen Systemen bewegen und dabei dieselben Routen benutzen.
4. Mit Remotezugriff und erfolgreicher C2-Kommunikation kann der Angreifer problemlos Ransomware einsetzen und die Umgebung als „Geisel“ nehmen.

Ransomware-Abwehr

A. Das Perimeter ist nicht immer ganz einfach zu sichern. Manchmal müssen Dienste zugänglich bleiben. Ziehen Sie Folgendes in Betracht:

- **a.** Multi-Faktor-Authentifizierung
- **b.** VPN- oder Zero-Trust-Architektur zur Sicherung des Benutzerzugriffs

B. Das Springen zwischen das Perimeter und den internen Netzen benötigt eine eigene Schutzschicht. Defense-in-Depth-Strategien können dabei helfen, den unbefugten Zugriff auf diese Segmente zu sichern.

C. Netzwerk- und Endpunktprävention, -erkennung und -reaktion können dazu beitragen, die Möglichkeiten zur Installation von Malware, zum Aufbau ausgehender C2-Kommunikation und zum Einsatz von Ransomware einzuschränken oder zu beseitigen.

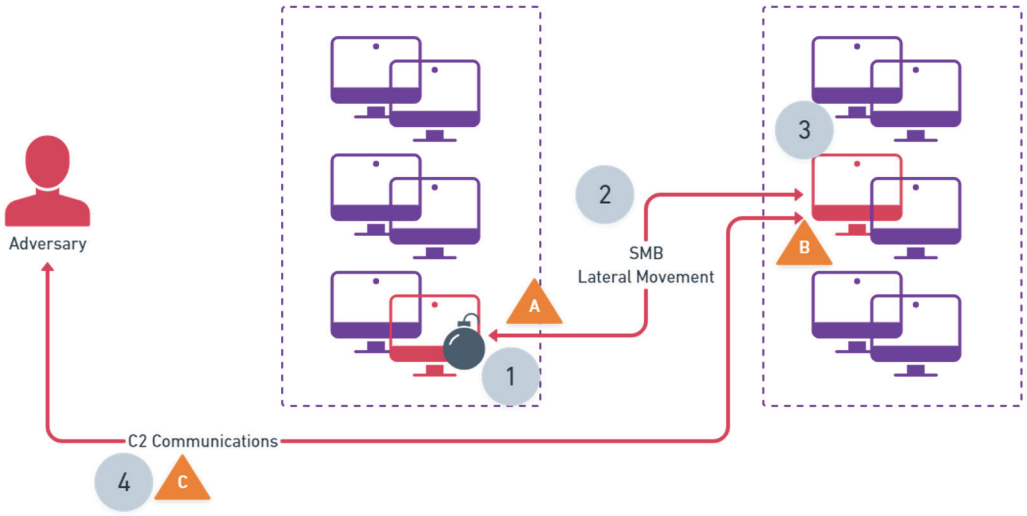
Abbildung 1: Remotezugriff-Implementierung zur Abwehr von Ransomware

Der einfachste Weg, den Missbrauch des Remotezugriffs einzudämmen, besteht darin, ihn erst gar nicht zu ermöglichen. Wenn ein Unternehmen den Remotezugriff jedoch für unerlässlich hält und er für den Betrieb notwendig ist, besteht der nächste Schritt darin, ihn umfassend zu schützen, damit Angreifer ihn nicht als Einfallstor in das Unternehmen ausnutzen können. Abbildung 1 zeigt eine Remotezugriffsbereitstellung, die Unternehmen nutzen können, um Trends bei Ransomware-Angriffen zu entschärfen.

Dateilose Malware

Die zweite Fallstudie befasst sich mit einem Angreifer, der wenig bis gar keine Beweise auf dem Datenträger hinterlässt. Durch den Einsatz von dateiloser Malware, speicherinternen Skripten und systemeigenen Binärdateien kann der Angreifer unbemerkt schädliche und folgenschwere Ransomware-Angriffe durchführen. Diese Techniken stellen eine große Herausforderung für Sicherheitsteams dar, die sich bei der Erkennung von Malware auf veraltete oder dateibasierte Erkennungsmethoden verlassen.

Ein Hauptproblem bei dateiloser Malware oder dem Missbrauch systemeigener Binärdateien ist die Leichtigkeit, mit der sich Angreifer im Verborgenen halten können. Native System-Binärdateien werden ständig ausgeführt. In der Tat ist es nicht gar nicht so ungewöhnlich, dass ein System seine eigenen ausführbaren Dateien ausführt. Schließlich sind sie für die Runtime erforderlich. Die Angreifer machen einfach etwas anders, als es von der Binärdatei vorgesehen war (sie laden beispielsweise mit BITSAdmin eine Datei von einer bösartigen Remote-Ressource herunter).



Pfad des Angreifers (Endzustand)

1. Die Infiltration in die Umgebung kann mit einem Spear-Phish, einem Drive-by-Download oder einem anderen Ereignis beginnen, um eine erste Kompromittierung zu erreichen. Dies kann eine Methode sein, bei der systemeigene Binärdateien und Skripte verwendet werden, so dass nur wenig Malware im System verbleibt.
2. Laterale Bewegungen können auch automatisch über Skripte und systemeigene Tools erfolgen, wobei sich der bösartige Datenverkehr mit dem normalen Umgebungsdatenverkehr vermischt.
3. Der Wechsel von einem System zu einem anderen ist nicht schwer – systemeigene Protokolle, gemeinsam genutzte Kennwörter und Administratorkonten sowie offene Ports in vertrauenswürdigen Netzwerken ermöglichen Angreifern, problemlos von einem zu vielen Systemen zu wechseln.
4. Einmal hergestellt, können Angreifer die Verbindung zu einer Umgebung aufrechterhalten.

Ransomware-Abwehr

A. Die erste Abwehrmaßnahme erfolgt durch den Einsatz von Endpoint- und Network-Detection-and-Response-Tools, um die böswillige Verwendung systemeigener Dateien zu erkennen. Systemdateien weisen ein spezielles Verhalten auf. Controls sollten nach Anomalien suchen, also nach abweichendem Verhalten. Die Analyse des Benutzerverhaltens kann ebenfalls zur Erkennung solcher Anomalien beitragen.

B. Der laterale Wechsel zu einem anderen System ermöglicht einem Angreifer, seine Operationen auszuweiten und seine Ziele zu erreichen – gleichzeitigt schafft er jedoch auch mehr Möglichkeiten für die Erkennung.

C. Letztendlich hat auch die C2-Kommunikation des Angreifers häufig ein bestimmtes Muster. Obwohl sie sich in den normalen ausgehenden Datenverkehr einfügt, weist sie Merkmale auf, die es ermöglichen, Angreifer zu erkennen und daran zu hindern, einen notwendigen bidirektionalen Kanal aufrechtzuerhalten.

Abbildung 2: Prävention/Erkennung von dateiloser Malware

Die Abwehr dieser TTPs ist auch deshalb wesentlich schwieriger, weil ein System nicht daran gehindert werden kann, seine eigenen Binärdateien auszuführen. Stattdessen müssen wir auf In-Memory- oder Verhaltensanalysen zurückgreifen, um festzustellen, ob eine Runtime-Umgebung normal oder unregelmäßig (und damit potenziell bösartig) läuft. Abbildung 2 zeigt eine häufige Situation, in der es um die Verhinderung oder Erkennung von dateiloser Malware geht.

Neue und aufkommende Technologien

Wir müssen uns auch mit der Zukunft von Abwehrmechanismen in der Informationssicherheit befassen, um zu verstehen, wie neue Technologien dabei helfen können, Ransomware-Angriffe zu verhindern und zu entschärfen. Zu den wichtigsten Lösungen, die Sie kennen sollten, gehören die folgenden:

- **Encrypted Traffic Analysis (ETA):** Angreifer verschlüsseln möglicherweise ihren Netzwerkdatenverkehr, um Erkennungsmechanismen zu umgehen. Ein verschlüsselter Datenverkehr führt jedoch nicht zu unzugänglichen Metadaten. Vielmehr können wir nach wichtigen Metadaten-Signaturen und -Mustern suchen, die Aufschluss über die Absicht des verschlüsselten Datenverkehrs geben können.
- **Moving Target Defense (MTD):** Dieser Präventionsmechanismus beruht auf Morphing oder der dynamischen Änderung des Codes, um Angriffsversuchen auszuweichen. Angreifer verwenden zum Ausnutzen von Sicherheitsrisiken hauptsächlich statischen Code oder Binärdateien. MTD verhindert die Ausnutzung, indem es die Möglichkeit zur Ausnutzung beseitigt.
- **Ereignisaggregation, -korrelation und -Eindringschutz mittels KI:** Technisch weit vorausschauend können KI-Erkennungs- und -Präventionsmechanismen eingesetzt werden, um zu einem Eindringen führende Ereignisse zu korrelieren und zu erkennen und sie letztlich zu stoppen, bevor ein Angreifer die Chance hat, in einem Unternehmen Fuß zu fassen.

Abschließende Überlegungen

Leider haben die Jahre 2020 und 2021 den Grundstein dafür gelegt, dass Ransomware-Akteure sich einen Namen machen und aus dem digitalen Leid anderer ein großes Geschäft machen können. Obwohl Ransomware keine neue Bedrohung ist, werden die Angreifer ihre TTPs weiterhin ständig ändern, um ihre Erfolgschancen zu maximieren und der Entdeckung zu entgehen. Dies stellt für Sicherheitsteams sowohl eine Herausforderung als auch eine Chance dar, auch wenn sich dadurch die Prioritäten für ihre Erkennungs- und Präventionsmaßnahmen verschieben können.

In diesem Whitepaper wurde erläutert, wo Unternehmen Prioritäten setzen müssen, indem einige der aktuellen Ransomware-Trends untersucht und Aspekte identifiziert wurden, auf die Unternehmen im Jahr 2022 achten müssen. Ganz gleich, ob es sich um eine Änderung der Taktik und der Erkennungsmethoden, die Verwendung einer bewährten Technik oder einfach um eine Verhaltensänderung hinsichtlich der Forderungen und Erpressungen handelt – Ransomware-Akteure wird es sicherlich noch sehr lange geben (solange sie damit Geld machen können), und wir können davon ausgehen, dass diese Art der Bedrohung immer wieder auftauchen wird.

Auch wenn es in diesem Whitepaper hauptsächlich um Ransomware ging, müssen Sicherheitsteams bedenken, dass Angreifer unabhängig von ihrem endgültigen Ziel oft gemeinsame TTPs verwenden. Häufige Angriffsschritte wie das Abgreifen von Anmeldeinformationen und laterale Bewegung sind nicht nur bei Ransomware zu beobachten. Indem Ransomware als Katalysator für die Verbesserung der Präventions-, Erkennungs- und Reaktionsfähigkeiten genutzt wird, kann sich ein Unternehmen gegen verschiedene Arten von Angriffen und Angreifern wappnen.

Dieses Whitepaper befasste sich auch mit Angriffs- und Verteidigungstrends zu einem bestimmten Zeitpunkt. Wir sind jedoch die Ersten, die sagen, dass das, was Ihre Umgebung benötigt, das ist, was anderen Umgebungen fehlt. Umgekehrt kann eine Haltung und Strategie, die an der einen Stelle funktioniert, an anderer Stelle überhaupt nicht funktionieren. Die einzige Konstante hierbei ist, dass dies den Angreifern egal ist. Sie haben nur ein einziges Ziel vor Augen, und das können wir zu unserem Vorteil nutzen. Wir ermutigen jedes Sicherheitsteam, die komplexen und einzigartigen Anforderungen seiner eigenen Umgebung zu berücksichtigen und Ransomware-Abwehr- und Gegenmaßnahmen entsprechend einzusetzen.

Sponsoren

SANS möchte sich bei den Sponsoren dieses Whitepapers bedanken: