VECTRA
SECURITY THAT THINKS

E-BOOK

Ransomware stoppen: Meldungen von vorderster Front

Zusammenfassung

Kein Unternehmen möchte einen Ransomware-Angriff in seiner Umgebung feststellen müssen, doch wenn Sie die Signale schnell erkennen können, haben Sie die besten Chancen, diesen zu stoppen. Wie wird das gemacht? Genau das möchten wir hier erörtern und mit realen Beispielen untermauern. Wir möchten zeigen, wie unsere Top-Kunden mit dem Vectra Sidekick Team zusammenarbeiten, um auf so genannte RansomOps-Angriffe frühzeitig zu reagieren und katastrophale Betriebsunterbrechungen zu verhindern, bevor die Ransomware eingesetzt wird.

In diesem E-Book erfahren Sie, warum es entscheidend ist Aktivitäten von Angreifern und das als RansomOps bezeichnete Auskundschaften zu erkennen, um Ransomware zu stoppen und welche Schritte Sicherheitsexperten unternehmen, um den heutigen Ransomware-Taktiken erfolgreich einen Riegel vorzuschieben. Wir werden darüber berichten, wie Kunden mithilfe des Einsatzes der Vectra Sidekick Services aktive Angriffe quasi sofort erkennen, sowie Ihnen einige der Herausforderungen, Feststellungen und Empfehlungen, die jede Organisation kennen sollte, vorstellen.

Eines ist sicher: Der Unterschied zwischen Erfolg und Misserfolg, wenn es darum geht, Ransomware zu stoppen, liegt in der Responsegeschwindigkeit und im schnellen Handeln – Lassen Sie uns Ransomware in ihre Schranken verweisen!

Vectra Sidekick MDR Service

Vectra Sidekick MDR ist ein Rund-um-die-Uhr-Service an 365 Tagen im Jahr, der proaktiv die von Vectra Detect aufgedeckten bösartige Aktivitäten untersucht.

Sidekick MDR fungiert als Multiplikator für Sicherheitsteams, indem erfahrene Security-Analysten eingesetzt werden, die Ihnen helfen, die KI von Vectra vollumfänglich zu nutzen, um Bedrohungen frühzeitig zu erkennen und Kompromittierung zu verhindern. Mit dem die Vectra-Plattform überspannenden Sidekick MDR erhalten Sie:

- Verstärkung für Ihr Sicherheitsteam durch Zugang zu erfahrenen Sicherheitsanalysten, die dabei helfen, raffinierte Angreifer und Ransomware-Hacker auszuschließen.
- Kompetenz, Kontext und Klarheit in Bezug auf die ersten Anzeichen eines Angriffs, einer Bedrohung oder Ransomware, die von Vectra Detect aufgedeckt werden, damit Analysten proaktiv zu einer schnellen Response beitragen können.
- Proaktive Überwachung rund um die Uhr an 365 Tage im Jahr, damit Sie wissen, wann eine dringliche Bedrohung oder die Erkennung von Ransomware sofortige Maßnahmen und Response erfordert.
- Anpassung des Einsatzes Ihrer Vectra-Anwendung an Ihre spezifischen Umgebung, Geschäftsziele und Branchenrisiken. Einschließlich der Anpassung der Überwachung, Bereitstellung von Expertenempfehlungen, Umgebungstrends und Metriken sowie Beschleunigung der Recherche.

In erster Linie ist Ransomware ein Geschäft

So unangenehm es auch sein mag, Ransomware-Banden und ihre Partner betreiben ein Geschäft, und wie jedes andere Unternehmen auch, sind sie darauf aus, Geld zu verdienen. Sie sind auf Rendite ausgerichtet und schlagen Profit aus der Möglichkeit, auf Systeme zu- und Daten "abzugreifen", die sie am schnellsten stehlen können, während sie dem Bestohlenen für die Rückgabe des eigenen Eigentums eine saftige Summe in Rechnung stellen.

Diese Denkweise ist die Grundlage für viele der in diesem E-Book besprochenen Feststellungen, und das Verständnis für die Motivation von Angreifern ist ein Schlüsselelement für jede Sicherheitsstrategie. In dem Moment, in dem Sie wissen was Angreifer antreibt, und die Systeme und Daten in einer Umgebung eindeutig bestimmen können, die im Falle eines Angriffs zu Unterbrechungen führen würden, ist Ihre Organisation gut aufgestellt, um die Durchführung eines Angriffs deutlich zu erschweren.

Wir werden sehen, warum Tischrechner zur Verdeutlichung beitragen können und wie Red Teams eine objektive Bewertung der aktuellen Bereitschaft vornehmen können.

Mit den Grundlagen beginnen

Am besten ist es natürlich, wenn Sie verhindern, dass Ransomware-Banden jemals Zugang zu Ihrer Umgebung erhalten. Und obwohl Prävention nie narrensicher ist, kann diese renditegesteuerte Mentalität für Sie von Vorteil sein. Tatsächlich können Sie Ihr Risiko drastisch reduzieren, wenn Sie die Grundlagen von Authentifizierung und Patching richtig beherrschen.

Dies liegt daran, dass der Erstzugriff von Angreifern in den meisten Fällen über eine ungepatchte und in der DMZ (Demilitarized Zone = entmilitarisierte Zone) aufgedeckten Schwachstelle, ein Konto ohne mehrstufige Authentifizierung oder ähnliche Lösungen, die schnell und einfach umgesetzt werden können, erfolgt. Wenn also Unternehmen einige der grundlegenden Präventionsmethoden außer Acht lassen, müssen Angreifer keine ausgeklügelten und zeitaufwendigen Taktiken anwenden, um sich Zugang zu verschaffen.

> Das optimale Ergebnis ist natürlich, wenn verhindert wird, dass Ransomware-Banden jemals Zugang zu Ihrer Umgebung erhalten.

Die gute Nachricht ist, dass Sie durch die Aktivierung von MFA (Multi-Faktor-Authentifizierung) auf Ihrem VPN, IDP und anderen Zugangspunkten Angreifern das Leben schwer machen, die sich dann vielleicht dazu entschließen, stattdessen die Tür eines anderen einzurennen. Das gilt gleichermaßen für die Patch-Verwaltung: Wenn Sie sicherstellen, dass die Patch-Praxis Ihre DMZ einschließt, können Sie Angriffe abwehren. Auch wenn keine Präventionsstrategie hundertprozentig sicher ist, können sinnvolle Investitionen in die Prävention den Angreifern dennoch das Eindringen erschweren.

Bereit sein, schnell zu reagieren … zu jeder Zeit

Beherrscht man die Grundlagen, kann man das Risiko zwar verringern, aber nicht ausschalten. Dafür gibt es viele Gründe. Wahr ist, dass es lediglich eines Fehlers bei der Kontoeinrichtung, eines nicht eingespielten Patches, eines Benutzers, der auf einen Link klickt, den er nicht anklicken sollte … oder einen neuen 0-Day im VPN Ihrer Wahl (finanziert durch die Unmengen an Geld, die in das Ransomware-Ökosystem fließen) bedarf, um sich Zugang zu verschaffen. Wir haben schon alles erlebt.

Und wenn ein Ransomware-Hacker in Ihre Umgebung eindringt, müssen Sie damit rechnen, dass er SCHNELL agiert. Allerdings haben wir auch schon auf Angriffe reagiert, die sich über mehrere Tage hinzogen – aber – es ist nicht ungewöhnlich, dass der Großteil eines Angriffs an einem einzigen Abend, nach Feierabend, stattfindet. Man sollte nicht vergessen, dass Zeit für renditeorientierte Angreifer eben Geld ist. Ob aus Responsezeitmangel seitens der Verteidiger oder aus reiner Berechnung, im Allgemeinen sehen wir nur wenige Anzeichen dafür, dass Angreifer versuchen, unter dem Radar zu bleiben. Tatsächlich ist die allgemeine Verweildauer in Bezug auf Ransomware-Angriffe in den letzten Jahren deutlich gesunken.

Die gute Nachricht für Verteidiger ist, dass Geschwindigkeit mit der richtigen Erkennungstechnologie den Angriff offensichtlich macht. Wie im Fall von Vectra haben wir kritische Hosts innerhalb von zwei Minuten nach dem ersten Zugriff erkannt. Aufgrund der Geschwindigkeit des Angriffsverlaufs ist es jedoch auch entscheidend, schnell und entschlossen zu reagieren, um der Bedrohung Einhalt zu gebieten, bevor die Ransomware eingesetzt wird.

Leider ist Fähigkeit, schnell zu reagieren, nicht nur auf die Geschäftszeiten beschränkt. Wir haben beobachtet, dass Auskundschaften und Lateral Movement in der Anfangsphase zu jeder Zeit stattfinden, scheinbar immer dann, wenn der Ransomware-Hacker ein wenig Zeit hat. Das kann während des Tages, nachts, am Wochenende oder sogar an einem Feiertag sein. Wir haben festgestellt, dass es jedoch wahrscheinlicher ist, dass es schließlich mitten in der Nacht, am Wochenende oder einem Feiertag zur Exfiltration und Verschlüsselung kommt – also dann, wenn die Responsemöglichkeiten auf Vorfälle am geringsten sind.

In der Praxis bedeutet dies, dass die rund-um-die Uhr- Überwachung ein absolutes Muss ist.

Entwickeln Sie Ihre Responsestrategie

Der erste Schritt bei der Response auf eine Ransomware-Bedrohung ist die Erkennung des Angreifers in Ihrer Umgebung. Ebenso wichtig ist es, zu wissen, was in verschiedenen Szenarien zu tun ist, um den Angriff zu stoppen. Wie weit gehen Sie dabei? Bei einem unserer Einsätze schaffte es der Angreifer bis zum Domain-Administrator auf dem Domain-Controller durchzukommen, wo das Sicherheitsteam in Sekundenbruchteilen die Entscheidung treffen musste, die Systeme vollständig vom Netz zu nehmen, um Zeit für eine Response zu gewinnen. Glücklicherweise hat das in diesem Fall funktioniert.

Auch wenn dieses Team an einem Ransomware-Angriff gerade noch vorbeigeschrammt ist, ist dieses Szenario gar nicht so unüblich. Es könnte sich die Frage lohnen: Was würden Sie tun, wenn Ihre Organisation in der gleichen Situation wäre? Wäre dieser Grad der Unterbrechung für das Unternehmen akzeptabel? Wären Sie in der Lage, ohne Konnektivität Ihres externen Sicherheitspersonals effektiv zu reagieren? Gibt es weitere Responsemöglichkeiten, die Sie einkaufen müssten?

Wir haben gesehen, dass unter Stress schnelles, entschlossenes Handeln ein Schlüsselelement für eine erfolgreiche Response ist. Wenn Sie Ihren Schlachtplan kennen und trainieren, bevor Sie ihn benötigen, kann das über Erfolg und Misserfolg entscheiden.

Um Ransomware zu stoppen, nicht nach der Ransomware suchen

Bei modernen Ransomware-Angriffen (eigentlich RansomOps) wird die Ransomware-Binärdatei erst ganz am Ende des Angriffs eingesetzt. Das heißt, wenn Sie die Ransomware selbst erkennen, ist es höchstwahrscheinlich zu spät.

Dieser weitverbreitete Irrglaube ist ein Problem, denn um diese Angriffe zu stoppen, müssen Sie die Schritte, die VOR der Ransomware eingesetzt werden, erkennen und darauf reagieren. In der Realität sieht es aber wohl so aus, dass Sie mit ziemlicher Sicherheit agieren werden, ohne den Gegner bzw. sein Ziel zu kennen. In vielen Fällen sehen Sie einen schnell voranschreitenden Angriff und möglicherweise einige verräterische Anzeichen in den Werkzeugen oder der C2-Infrastruktur, die es Ihnen erlauben, eine begründete Vermutung darüber anzustellen, was passiert.

In diesem Fall müssen sich Ihre Responsepläne auf einen allgemeineren Verlauf des Eingriffs und Angriffs konzentrieren, wobei das Endergebnis lediglich eine Wahrscheinlichkeit und keine Gewissheit darstellt.

Der Schlüssel: Konten und Verwaltungstools

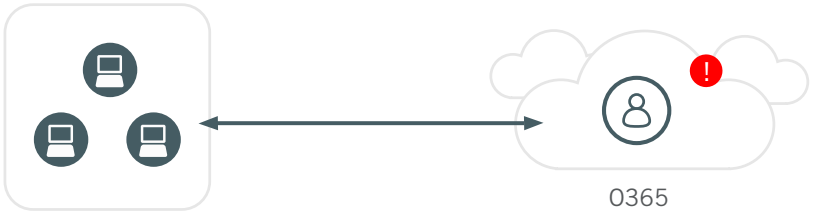
Wir haben beobachtet, dass Exploits, Sicherheitsprobleme von Software, genutzt werden, um einen ersten Zugriff zu erhalten, und gelegentlich auch, um Lateral Movement vorzunehmen. Doch wie bei den meisten modernen Angriffen liegt der Schwerpunkt auf den Anmeldedaten: Administrations- und Dienstkonten. In Verbindung mit Verwaltungsprotokollen stellen diese die bevorzugten Taktiken für praktisch jeden der Ransomware-Hacker dar.

Wie bei vielen Angriffen besteht die Absicht darin, den Domain-Administrator auf dem Domain-Controller zu erreichen, um die letzte Phase des Angriffs einzuleiten. Von diesem Standpunkt aus ist es einfach, Zugang zu den wertvollsten aller Daten zu erhalten. Es ist auch möglich, Ransomware blitzschnell zu verteilen, indem man Admin-Tools wie GPO (Group Policy) verwendet.

Da der Schwerpunkt auf Anmeldedaten liegt, ist es extrem wichtig, die Verwendung aller privilegierten Konten sorgfältig zu überwachen. Unserer Erfahrung nach ist dies sicher eines der wertvollsten Signale zur Erkennung von Angriffen.

Gemeinsame Themen

Die Analysten von Vectra haben Herausforderungen im Bereich Nutzer, Prozess und Sicherheit, die bei verschiedenen Kundenprojekten auftraten, zusammengetragen.



Initialzugriff

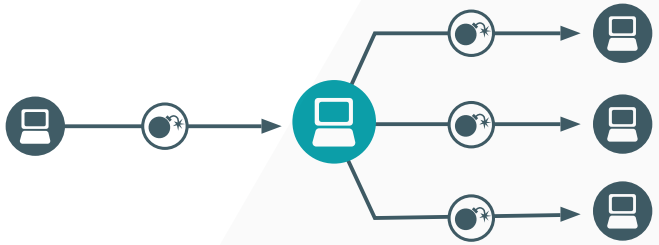
- Angreifer suchen weiterhin nach Schwachstellen in öffentlich zugänglichen, mit dem Internet verbundenen Diensten und Systemen.
- Server, auf denen RDP, FTP oder VPN laufen, sind beliebte Ziele, die ersten Zugriff auf Unternehmen und Cloud bieten.
- Das Fehlen einer mehrstufigen Authentifizierung ist eine häufig genutzte Lücke.
- In einigen Fällen dauerte es nur wenige Stunden, bis die Angriffe fortschritten, in anderen Fällen Tage oder sogar Wochen. Die Sicherheitsteams haben genug Zeit, für eine frühzeitig Erkennung und Response, aber müssen rund um die Uhr wachsam sein.

C2

- Cobalt Strike scheint das derzeit beliebteste Werkzeug zu sein.
- Gängige Tools für den Fernzugriffs, unabhängig davon, ob sie genehmigt oder nicht genehmigt waren, wurden ebenfalls zur Kontrolle von Systemen eingesetzt. In einem Fall haben wir die Software „Cisco AnyConnect“, die von einer Person außerhalb des Unternehmens genutzt wurde, um Rechner im Unternehmen zu kontrollieren, entdeckt.

Aufklärung und Lateral Movement

- In den meisten Fällen wurde, unter anderem Netzwerkzuordnung, rDNS-Abfragen und Aufzählung von Freigaben, aggressiv gescannt. Durch das schnelle Scannen wurden die Angriffe im Allgemeinen innerhalb von Minuten nach dem Initialzugrifff offensichtlich.
- Die Auskundschaftung von Anmeldedaten, auch von LDAP-Abfragen und RPC-Aufrufe zur Zuordnung von Standorten zu Anmeldedaten, war ebenfalls üblich.
- In der Anfangsphase schloss Lateral Movement allgemeine Exploits ein. Spätere Phasen griffen hauptsächlich auf Anmeldedaten und Verwaltungsprotokollen zurück.



Exfiltration

- Kostenlose Filesharing-Seiten wurden häufig genutzt, um Aufklärungsdaten zur Analyse hochzuladen. Dazu gehörten auch Mega Upload (mega.com) und temp.sh.

Empfehlungen

Unsere Teams arbeiten täglich eng mit Sicherheitsteams zusammen und reagieren auf kritische Warnmeldungen, die von der Vectra KI-gesteuerten Lösung zur Erkennung und Response von Bedrohungen generiert werden. Wenn wir mit Kunden erstmals in Kontakt treten, ist es nicht offensichtlich, ob es sich bei einer Bedrohung um Ransomware handelt. Mit zunehmendem Schweregrad der Warnungen gewinnen wir mehr Klarheit und Kontext in Bezug auf den Angriff und können feststellen, ob es sich tatsächlich um Ransomware handelt. Wir haben eine Reihe von Sicherheitstools und Sicherheitspraktiken ausfindig gemacht, die es Angreifern erschweren, erfolgreiche Kampagnen mit Ransomware zu fahren und können diese schlussendlich stoppen. Dazu gehören:

Prävention

- Bewerten Sie Ihre externe Sicherheitslage regelmäßig und setzen Sie vorrangige Maßnahmen zur Fehlerbehebung um. Konzentrieren Sie sich besonders auf die Infrastruktur für den Fernzugriff und allgemein anfällige Dienste wie RDP und FTP, die sich als beliebte Ziele erwiesen haben.
- Aktivieren Sie mehrstufige Authentifizierung, wo immer dies möglich ist, bei allen Identitätsanbietern oder Infrastrukturen für Fernzugriff.
- Im Allgemeinen erschweren strenge präventive Kontrollen, Regeln und Richtlinien die Ausweitung von Privilegien selbst nach einem Zugriff, wodurch mehr Responsezeit zur Verfügung steht.
- Besonderes Augenmerk gilt den privilegierten Konten. Trotz der operativen Herausforderung gilt, dass je mehr getan werden kann, um die Nutzung von "Jump-Servern" und Systemen zur Verwaltung privilegierter Konten zu forcieren, desto schwieriger wird der Eskalationsweg.

Erkennung

- Es bleibt Zeit, den Angriff zu stoppen, nachdem der Ransomware-Hacker sich Zugang verschafft hat und bevor Daten exfiltriert werden oder Ransomware eingesetzt wird.
- Investieren Sie in die Erkennung von und Response auf Bedrohungen in Ihrem Netzwerk, Ihrer Identitätsinfrastruktur, Ihrer Cloud und Ihren Endgeräten, um die Chancen auf eine frühzeitige Erkennung zu maximieren.

Recherche und Response

- Ransomware-Angriffe können schnell voranschreiten, zu jeder Tages- und Nachtzeit. Es ist von entscheidender Bedeutung, dass Sie kritische Warnmeldungen rund um die Uhr und an 365 Tage im Jahr überwachen, sei es durch die Aufstockung interner Teams oder durch die Nutzung von Managed Detection and Response (MDR) oder MSSP-Angeboten.
- Die Integration der Telemetrie aus Netzwerk-, Endpunkt- und Cloud-Protokollen bieten besten Kontext, Klarheit für die und eine Bereicherung der Recherche von Bedrohungen und der Suche nach einer grundlegenden Ursache.
- Ein Rückblick auf verstärkte Scan-Aktivitäten in der DMZ vor dem ersten Zugriff kann, in Kombination mit OSINT, eine frühzeitige Einschätzung des wahrscheinlichen Hackers liefern und für mehr Klarheit bei der Response sorgen.

Näheres erfahren Sie unter info@vectra.ai.

E-Mail: info@vectra.ai vectra.ai/de