VARONIS

WHITEPAPER

Wie Varonis dabei helfen kann, **Ransomware zu stoppen**

Einleitung

Ransomware-Banden sind in den letzten Jahren zunehmend raffinierter geworden. Sie sind jetzt schwieriger zu erkennen und gehen durchdacht und gewissenhaft vor. Frühe Ransomware-Angriffe waren relativ ziellos – massenhafte Phishing-Kampagnen brachten Benutzer dazu, den Ransomware-Code auszuführen, und es wurde sehr schnell damit begonnen, viele Dateien zu verändern und umzubenennen.

Überaktives Verhalten des Dateisystems war (und ist) für Varonis leicht zu erkennen, da unsere Plattform die Datenaktivität genau beobachtet und analysiert. Maze, Dopplepaymer, REvil und andere von Menschen betriebene Ransomware-Gruppen verschlüsseln Dateien jedoch nicht sofort – sie übernehmen mehrere Systeme, stehlen Daten und bauen Backdoors ein, bevor sie Lösegeld fordern. Glücklicherweise kann Varonis frühe Anzeichen einer Kompromittierung durch Ransomware-Banden erkennen, so dass Sie einen potenziellen Angriff frühzeitig abwehren können.

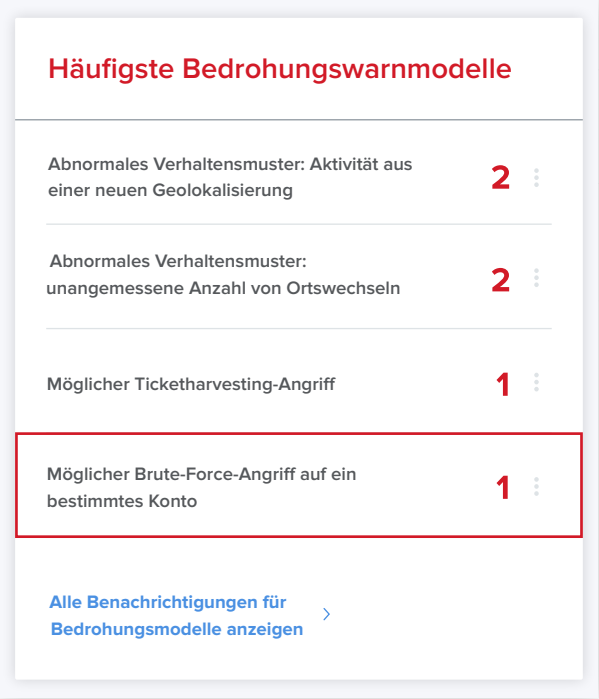
Viele Ransomware-Gruppen nutzen mehrere Techniken, um ein Netzwerk zu infiltrieren, sich dann darin zu bewegen, Zugriff zu erhalten, Daten zu stehlen und diese schließlich zu verschlüsseln. In diesem Whitepaper wird beschrieben, wie Varonis ungewöhnliche Aktivitäten in jeder Phase erkennen kann.

Anfängliche Kompromittierung

Network intrusion Techniken variieren von Opfer zu Opfer. Der erste Einstieg kann über gestohlene Anmeldeinformationen erfolgen, die für die Anmeldung bei Servern mit Internetzugang (z. B. RDP), ausgenutzte Fehlkonfigurationen oder CVEs sowie für Phishing verwendet werden.

Wenn sich ein Angreifer mit legitimen Anmeldedaten bei einem mit dem Internet verbundenen System anmeldet, geschieht dies häufig mit Anmeldedaten, die diese Ressourcen zuvor noch nicht verwendet haben, oder beispielsweise von anderen Orten und zu anderen Uhrzeiten verwendet wurden. Es können auch Brute-Force- oder Password-Spraying-Angriffe verwendet werden, um Kennwörter zu erraten. Durch jede dieser Verhaltensweisen kann ein Varonis-Bedrohungsmodell ausgelöst werden – damit wird auch ein Alarm über einen ungewöhnlichen erfolgreichen bzw. erfolglosen Anmeldeversuch ausgelöst, und mit ihm evtl. Sperrungen. In diesem Fall und im Falle eines korrumpierten Internet-Servers erkennt Varonis ungewöhnliche Verbindungen und Aktivitäten, die vom Angreifer nach der ersten Verbindung vom kompromittierten System generiert wurden.

Angreifer verwenden oft Phishing, um das erste Opfer zu kompromittieren. Sobald sie sich im System etabliert haben, lässt sich oft beobachten, wie mit dem BEACON-Agenten von CobalStrike vom korrumpierten Gerät aus mit dem C&C-Server kommuniziert wird. Sobald der Angreifer die Kontrolle hat, beginnt er, die Umgebung auszuspähen und auf andere Systeme überzugehen, indem er Beacons und „Web Shells“ verwendet. Diese kann Varonis durch die Analyse von Web-Aktivitäten und DNS-Anfragen erkennen, wie im nächsten Abschnitt beschrieben.



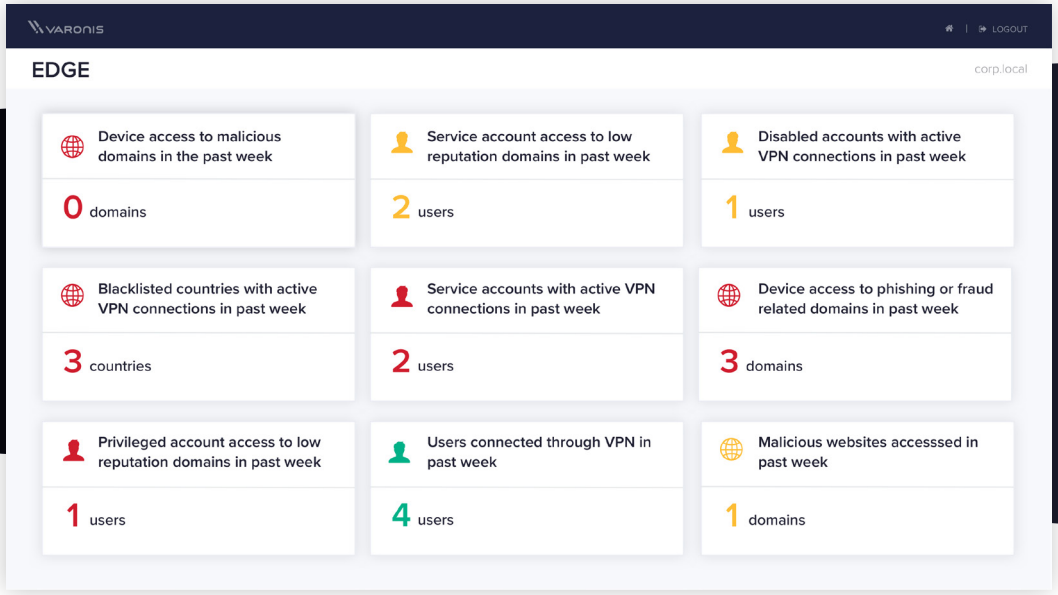
Spionage und Etablierung

Ransomware-Gruppen suchen nach weiteren Systemen, die sie übernehmen können, indem sie DNS-Server und Dateifreigaben mit Tools wie nslookup und smbtools abfragen und dann Malware auf weitere Systeme verteilen.

Varonis erkennt durch die Analyse von DNS und AD ungewöhnliche DNS-Anfragen, wie z. B. eine ungewöhnliche Anzahl von Reverse-IP-Lookups und Benutzeraufzählungsaktivitäten. Sobald Systeme gefunden wurden, verbindet sich Maze mit ihnen (z.B. über RDP) und installiert Malware.

Varonis überwacht die Verbindungen zwischen Benutzern und den Geräten und Ressourcen, auf die sie zugreifen. Daher erkennen die Bedrohungsmodelle eine ungewöhnliche Anzahl von Verbindungen, die von einem Konto hergestellt werden, Verbindungen zu Systemen, auf die normalerweise nicht zugegriffen wird, sowie Brute-Force-Angriffe wie Password Spraying und Credential Stuffing.

Ungewöhnliche Verbindungen, zurück zu den C&C-Servern können auf verschiedene Weise erkannt werden. Erstens: Wenn eine Verbindung zu einer bekannten schädlichen Domäne besteht, alarmiert Varonis über diese Verbindung und markiert sie. Zweitens erkennt Varonis, wenn Angreifer ihren Traffic in vielen Verbindungen verstecken (sog. „White Smoke“), indem ein Algorithmus zur Generierung von Domänen (Domain Generation Algorithm, DGA) verwendet wird. Drittens erkennen die Verhaltensmodelle von Varonis auch, wenn Angreifer DNS als verdeckten Kanal verwenden, um ihre Befehle oder Datentransfers als Abfragen zu tarnen. Schließlich warnt Varonis auch bei ungewöhnlichen Web-Aktivitäten, wie z. B. bei der Verwendung neuer oder ungewöhnlicher User-Agents1, bei ungewöhnlichem oder erstmaligen Zugriff auf das Internet durch ein Konto oder bei ungewöhnlichen Upload-Aktivitäten.



1 Ein Benutzer-Agent ist eine Zeichenfolge, die vom Web-Client an den Web-Server gesendet wird und den Browser sowie die Betriebssystemversion angibt.

Berechtigungseskalation

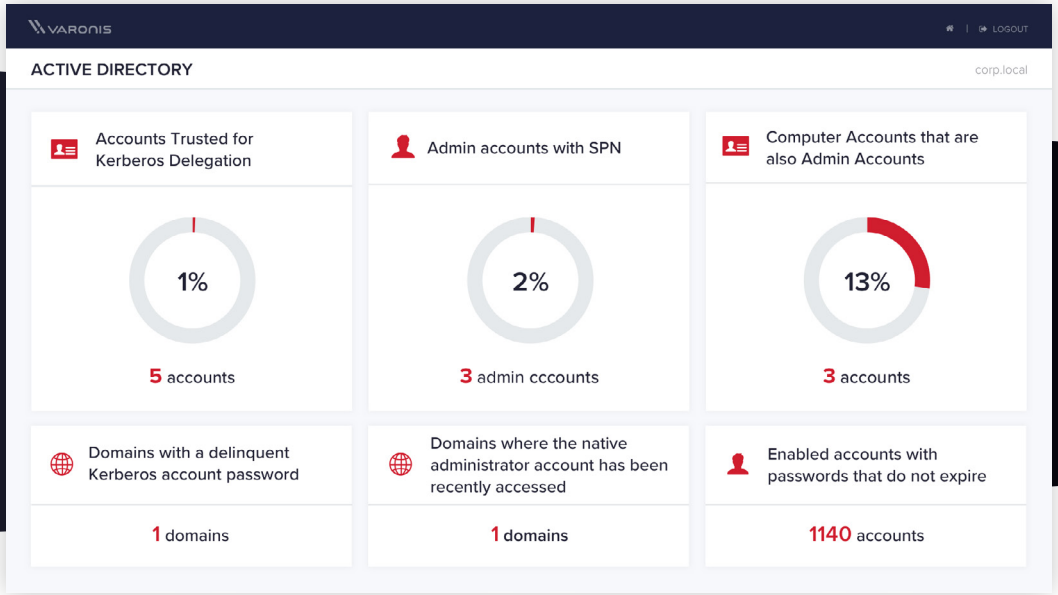
Angreifer erhalten Anmeldedaten für privilegierte Konten, indem sie bekannte Open-Source-Tools verwenden, nach als Plain Text gespeicherten Passwörtern suchen und Anmeldedaten aus Active Directory harvesten. Sobald der Angreifer die administrativen Zugangsdaten erhalten hat, kann er einen oder mehrere Benutzer zu einer Domänen Administratorgruppe hinzufügen und die Zugangsdaten in Cloud-Speicherdienste hochladen.

Durch Beobachten der Dateisystemaktivitäten erkennt Varonis es schnell, wenn bekannte Penetrationstools auf der Festplatte gespeichert werden oder wenn ein Benutzer Dateifreigaben nach Dateien mit Kennwörtern oder anderen sensiblen Daten durchsucht. Jedes Benutzerkonto hat in der Regel Zugriff auf weitaus mehr Daten, als es sollte. Solche Suchen sind daher oft erfolgreich – mehr Informationen zum Beheben dieser Situation finden Sie weiter unten.

Viele Gruppen verwenden auch Tools wie Mimikatz, um Anmeldeinformationen zu sammeln, indem sie beispielsweise nach Administratorkonten suchen, bei denen es keine starken Verschlüsselungsanforderungen gibt.

Varonis analysiert die Active-Directory-Aktivitäten, um Credential Harvesting (z. B. Kerberoasting) und andere Angriffe zu erkennen. Um die Erfolgschancen solcher Angriffe zu verringern, weist Varonis auf einem Dashboard auf potenzielle Ziele hin (z. B. Administratorkonten, die mit einem Service Principal Name (SPN) verknüpft sind). Dadurch wird die Angriffsfläche in AD und auf Dateisystemen verkleinert und den Ransomware-Gruppen wird das Handwerk gelegt. Varonis alarmiert auch, wenn ein Konto zu einer administrativen Gruppe hinzugefügt wird.

Sollte eines dieser Konten zum ersten Mal eine Verbindung zum Internet herstellen, eine Verbindung zu böswilligen Domains aufbauen oder ungewöhnliche Upload-Aktivitäten aufweisen, wird Varonis, wie bereits beschrieben, einen Alarm zu diesen Signalen auslösen.

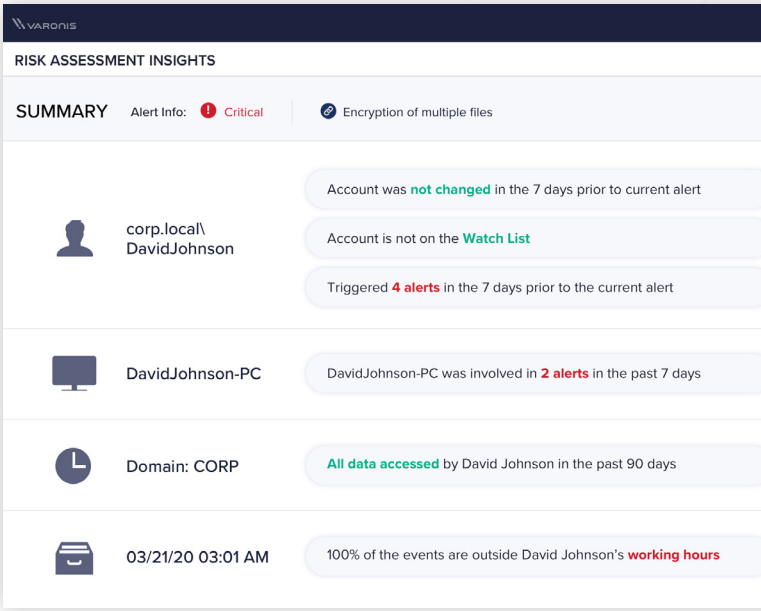


Endphase

Wenn die ersten Anzeichen einer Kompromittierung, einer Seitwärtsbewegung und einer Berechtigungseskalation übersehen werden, bietet Varonis eine weitere kritische Schutzschicht. Diese schützt Ihre größten Datenspeicher, Windows- und UNIX-Server, NAS-Geräte, SharePoint und Exchange (sowohl lokal als auch in 365).

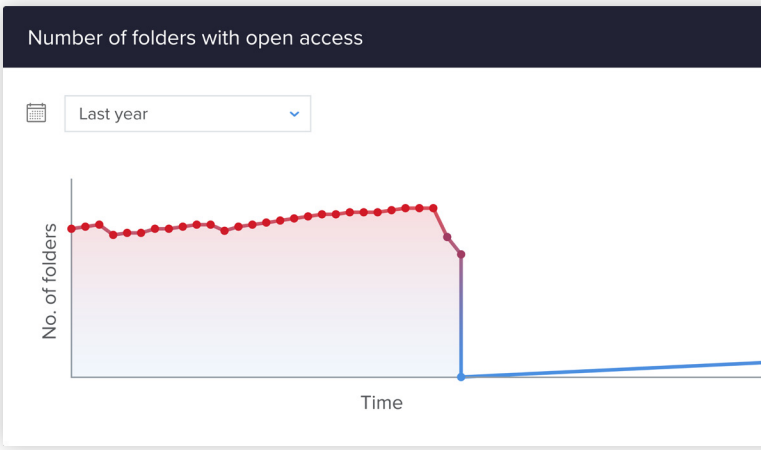
Mit Varonis lassen sich mehr Informationen darüber erfassen, wie Benutzer mit Daten interagieren, als mit jeder anderen Technologie – es analysiert die Dateisystemaktivität auf Plattformen, die über ihre APIs angemessene Möglichkeiten für Audits bieten, wie Microsoft 365 und NAS-Geräte von NetApp und EMC. Dort, wo native Audits nicht ausreichend sind, wie bei Windows, UNIX, Exchange und SharePoint, verwendet Varonis im Einsatz erprobte Dateisystemfilter zur Erfassung von Dateioperationen.

Wenn ein Benutzer beginnt, auf eine im Vergleich zu seinem normalen Verhalten ungewöhnliche Datenmenge zuzugreifen, erkennt Varonis dies mit einem oder mehreren Verhaltensmodellen (wie oben erwähnt werden auch ungewöhnliche Uploads erkannt.) Wenn ein Benutzer beginnt, Dateien zu verschlüsseln, wird auch dies erkannt – viele Kunden automatisieren Reaktionen auf diese Art von Verhalten, wodurch das das Konto deaktiviert und seine aktiven Verbindungen abgebrochen werden.



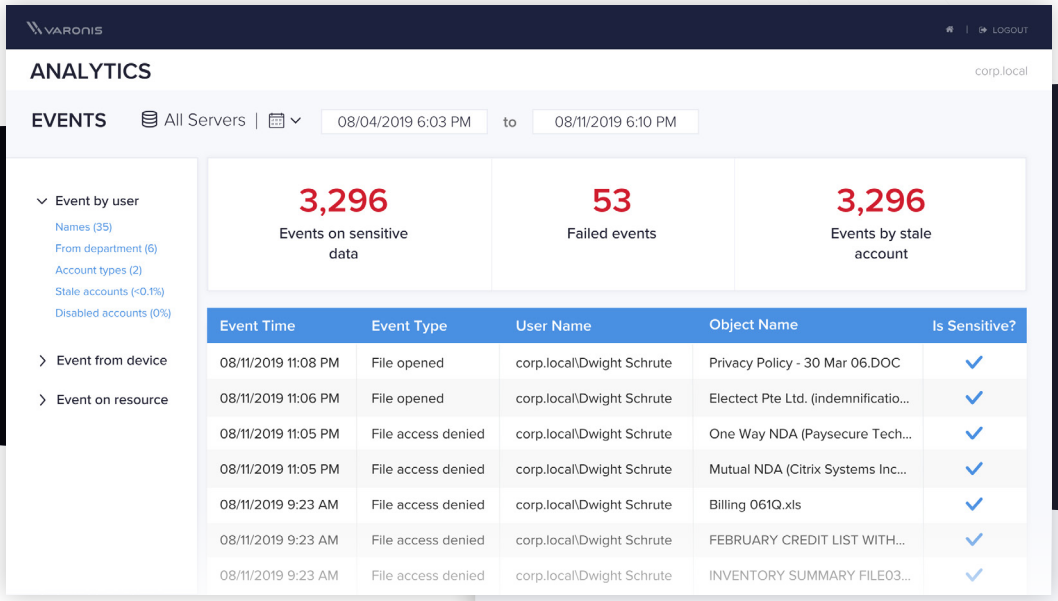
Varonis kann automatisierte Dateisystemaktivitäten leicht von menschlichen Aktivitäten unterscheiden.

Varonis zeigt auch auf, wo Daten zu leicht zugänglich sind und wo Benutzer bzw. Gruppen Zugriff haben, den sie nicht benötigen. Die Prozesse, um solche Zugriffe zu sperren, werden ebenfalls automatisiert. Die Beschränkung des Zugriffs auf wichtige Daten reduziert die Gesamtangriffsfläche und erschwert Bedrohungsakteuren ihre Arbeit.



Die Abschaffung von Gruppen mit globalem Zugriff verringert sofort das Risiko.

Mit einem detaillierten, durchsuchbaren Protokoll aller Zugriffe auf das Dateisystem lassen sich Schäden viel schneller bewerten und beheben. Anstatt Verzeichnisse nach Lösegeldforderungen zu durchsuchen, können Sie eine Abfrage aller Änderungen ausführen, die in einem bestimmten Zeitraum von Benutzern durchgeführt wurden, um die betroffenen Dateien aufzuspüren und danach die richtige Version jeder Datei wiederherzustellen.



Varonis entlarvt globale Cyber-Kampagnen

Mit Edge konnten unsere Sicherheitsforscher wichtige Klassen von Malware-APTs erkennen, die anderen Sicherheitslösungen entgangen waren.

Next-Gen-Malware für Banking-Anwendungen (Qbot)

- Neue Qbot-Variante zum Stehlen von Banking-Informationen
- Edge hat eine schadhafte VBS-Datei, C2-Kommunikation über DNS sowie Brute-Force-Versuche gegen Domänenbenutzer erkannt

RESEARCH-BERICHT LESEN >

Ein getarnter Cryptominer (Norman)

- XMRig-basierter Cryptominer — ein Hochleistungs-Miner für die Kryptowährung Monero
- Edge hat Alarm geschlagen, aufgrund abnormaler Web-Aktivität und zugehöriger abnormaler Dateiaktivitäten

RESEARCH-BERICHT LESEN >

VARONIS

FAZIT

Ransomware-Gruppen werden zunehmend raffinierter. Sie können länger unerkannt bleiben, Ihre Daten auf andere Weise monetarisieren und schließlich Lösegeld für Ihre Daten verlangen. Leider funktioniert diese Vorgehensweise gut – solange Unternehmen weiterhin zahlen und Kryptowährungen eine sichere, anonyme Möglichkeit bieten, diese Aktivitäten zu monetarisieren, gibt es keinen Grund zur Annahme, dass Ransomware-Gruppen verschwinden.

Fortschrittliche Erkennung kann Ihrem Unternehmen einen Vorteil verschaffen – ebenso wie die Reduzierung der Gesamtangriffsfläche. Varonis' datenzentrierte Technologie verläuft von innen nach außen und baut eine Ringstruktur aus Erkennungsmechanismen auf, von Daten über Active Directory und DNS bis hin zu VPNs und Proxies. Varonis macht Sie auch auf gefährdete Konten und Daten aufmerksam, so dass Sie diese sperren können, bevor Angreifer sie ausnutzen. Diese Kontrollmechanismen tragen dazu bei, Ihr Unternehmen vor allen Bedrohungsakteuren zu schützen – vom gewöhnlichen Insider bis hin zu den fortschrittlichen persistenten Bedrohungen, mit denen wir es heutzutage allzu häufig zu tun haben.

Zusätzliche Vorfalls-Reaktionsdienste

Wenn Sie angegriffen werden oder einfach Hilfe benötigen, um zu verstehen, was Sie beobachten, können Sie das Fachwissen unseres Vorfallsreaktionsteams in Anspruch nehmen. Es wird Ihnen helfen, jegliche Vorfälle zu untersuchen und zu lösen, ganz gleich, ob Sie Varonis-Kunde oder Testnutzer sind.

VARONIS

Varonis kostenlos ausprobieren

Richten Sie Varonis in Ihrer eigenen Umgebung ein. Schnell und mühelos

info.varonis.com/demo

ÜBER VARONIS

Varonis ist ein Pionier im Bereich Datensicherheit und Analytik, und kämpft an anderer Front als die herkömmlichen Cybersicherheitsanbieter. Varonis ist spezialisiert auf den Schutz von Unternehmensdaten in lokalen Systemen und in der Cloud: sensible Dateien und E-Mails, vertrauliche Kunden-, Patienten- und Mitarbeiterdaten, Finanzdaten, strategische Pläne und Produktpläne sowie sonstiges geistiges Eigentum.

Die Datensicherheitsplattform von Varonis erkennt Insider-Risiken und Cyberangriffe durch Analysieren von Daten, Kontoaktivitäten und des Benutzerverhaltens, beugt durch Sperren und Einschränken sensibler und veralteter Daten Katastrophen vor und sorgt durch Automatisierung für einen sicheren Zustand. Varonis eignet sich für zahlreiche Zielsetzungen mit Schwerpunkt auf Datensicherheit, einschließlich Governance, Compliance, Klassifizierung und Bedrohungsanalyse. Varonis hat seine Geschäftstätigkeit im Jahr 2005 aufgenommen und hat Tausende Kunden weltweit – darunter Branchenführer aus den Bereichen Technologie, Konsumgüter, Handel, Finanzdienstleistungen, Gesundheitswesen, Manufacturing, Energie, Medien und Bildung.