„Angreifer ändern ihre Angriffstaktiken immer häufiger ‚on the fly', da sie auf keinen Fall mit leeren Händen dastehen wollen. Das stellt ganz neue Herausforderungen an die Sicherheitsmaßnamen von Unternehmen." (Sean Gallagher, Senior Threat Researcher, Sophos)

Was nicht verschlüsselt werden kann, wird eingesperrt: Sophos entdeckt neue Ransomware

Memento Ransomware sperrt Dateien in ein passwortgeschütztes Archiv, wenn sie die Daten nicht verschlüsseln kann. Forensische Analyse der SophosLabs gibt detaillierte Einblicke in das neue Vorgehen.

Wiesbaden 18. November 2021. Sophos hat heute Details zu einer neuen Ransomware von einer Gruppe namens Memento veröffentlicht. Die Studie „New Ransomware Actor Uses Password Protected Archives to Bypass Encryption Protection" beschreibt den Angriff, der Dateien in einem kennwortgeschützten Archiv sperrt, wenn die Ransomware Memento die Zieldaten nicht verschlüsseln kann.

„Von Menschen gesteuerte Ransomware-Angriffe sind selten eindeutig und linear", sagt Sean Gallagher, Senior Threat Researcher bei Sophos. „Angreifer nutzen Gelegenheiten spontan, wenn sie sie finden oder manchmal unterlaufen ihnen auch Fehler. Dann ändern sie ihre Taktik 'on-the-fly', denn wenn es ihnen gelingt, in das Netzwerk eines Ziels einzudringen, wollen sie auf keinen Fall mit leeren Händen dastehen. Der Memento-Angriff ist ein gutes Beispiel dafür und erinnert uns daran, dass es wichtig ist, für Sicherheit auf allen Ebenen zu sorgen. Denn in diesem Fall haben die Angreifer nach einer durch ein Sicherheitsprogramm unterbundenen Datenverschlüsselung einen anderen Weg gefunden, ihr Ziel zu erreichen. Die Fähigkeit, Ransomware und Verschlüsselungsversuche zu erkennen und zu unterbinden, ist von entscheidender Bedeutung, aber es ist auch wichtig, über Sicherheitstechnologien zu verfügen, die vor anderen, Aktivitäten, wie zum Beispiel unerwartete Bewegungen und Aktivitäten im Netzwerk warnen können."

Wie wichtig das ist, zeigt das SophosLabs-Protokoll der Memento-Attacke:

+++Mitte April 2021 – Es geht los. Eindringen ins Netzwerk+++
Sophos geht davon aus, dass die Memento-Gruppe Mitte April 2021 in das Netzwerk des Ziels eingedrungen ist. Die Angreifer nutzten eine Schwachstelle in VMware vSphere, einem internetbasierten Cloud-Computing-Virtualisierungstool, um in einen Server einzudringen. Die gefundenen forensischen Beweise deuten darauf hin, dass die Angreifer den Haupteinbruch Anfang Mai 2021 begannen.

Die Täter bewegten sich in den ersten Monaten unbemerkt durch das Netzwerk und stellten Erkundungen an. Sie setzten das Remote Desktop Protocol (RDP), den NMAP-Netzwerkscanner, den Advanced Port Scanner und das Plink Secure Shell (SSH) Tunneling-Tool ein, um eine interaktive Verbindung mit dem angegriffenen Server herzustellen. Die Kriminellen nutzten außerdem Mimikatz, um Zugangsdaten zu sammeln, die sie in späteren Phasen des Angriffs verwenden konnten.

+++20. Oktober 2021 – WinRAR kommt zum Einsatz+++
Laut den Sophos-Forscher:innen setzen die Cyberkriminellen am 20. Oktober 2021 das legitime Tool WinRAR ein, um eine Sammlung von Dateien zu komprimieren und sie über RDP zu exfiltrieren.

++++++23. Oktober 2021 – Roll-out der Ransomware und Plan B ++++++
Die Ransomware selbst kam erstmals am 23. Oktober 2021 ins Spiel. Sophos fand heraus, dass die Angreifenden zunächst versuchten, Dateien direkt zu verschlüsseln, was sich jedoch durch Sicherheitsmaßnahmen verhindern ließ. Die Cyberkriminellen änderten daraufhin ihre Taktik, rüsteten um und setzten die Ransomware erneut ein. Sie kopierten unverschlüsselte Dateien mit einer umbenannten kostenlosen Version von WinRAR in passwortgeschützte Archive, verschlüsselten dann das Passwort und löschten die Originaldateien.

Für die Wiederherstellung der Dateien forderten die Cyberkriminellen nun ein Lösegeld in Höhe von einer Million Dollar in Bitcoin. Glücklicherweise konnte das attackierte Unternehmen die Daten ohne die Beteiligung der Cyberkriminellen wiederherstellen.

+++18.Mai, 8. September, 3. Oktober – Neue Eindringline und Kryptominer +++
Während sich die Memento-Gruppe im Netzwerk des Zielunternehmens aufhielt, drangen zwei weitere, verschiedene Cyberkriminelle über denselben verwundbaren Zugangspunkt ein und nutzten dabei ähnliche Sicherheitslücken. Diese Gruppen hatten jeweils Miner für Kryptowährungen auf demselben kompromittierten Server abgelegt. Eine von ihnen installierte am 18. Mai einen XMR-Kryptominer, während die andere am 8. September und erneut am 3. Oktober einen XMRig-Kryptominer einrichtete.

„Wir haben das schon oft erlebt: Wenn Sicherheitslücken im Internet bekannt und nicht gepatcht werden, nutzen Angreifer sie schnell aus und so tummeln sich plötzlich verschiedene Hackergruppen im selben Netzwerk. Je länger die Schwachstellen nicht behoben werden, desto mehr Angreifer werden auf sie aufmerksam", so Gallagher. „Cyberkriminelle durchsuchen das Internet ständig nach verwundbaren Online-Eingangsstellen und zögern nicht, wenn sie eine finden. Wenn mehrere Angreifer in ein System eindringen, bedeutet dies für die Opfer einen größeren Schaden und eine aufwändigere Wiederherstellung. Außerdem wird es für forensische Untersuchungen schwieriger zu klären, wer was getan hat. Genau das aber ist eine wichtige Information für die Bedrohungsbekämpfer, um Unternehmen dabei zu helfen, weitere Angriffe zu verhindern."

Wichtig für die IT-Sicherheit – einige Hinweise
Dieser Vorfall, bei dem mehrere Angreifende einen einzigen ungepatchten, dem Internet ausgesetzten Server ausnutzten, zeigt einmal mehr, wie wichtig es ist, Patches schnell zu installieren und sich bei Drittanbietern, Vertragsentwicklern oder Dienstleistern über die Sicherheit ihrer Software zu informieren.

Sophos empfiehlt die folgenden Best Practices, um sich vor Ransomware und den damit verbundenen Cyberattacken zu schützen:

Auf strategischer Ebene

- **Mehrschichtiger Schutz.** Da immer mehr Ransomware-Angriffe auf Erpressung abzielen, sind Backups nach wie vor notwendig, aber alleine nicht ausreichend. Es ist wichtiger denn je, Cyberkriminelle von vornherein fernzuhalten oder sie schnell zu entdecken, bevor sie Schaden anrichten. Unternehmen sollten einen mehrschichtigen Schutz einsetzen, um Angriffe an möglichst vielen Stellen im Unternehmen zu erkennen und zu blockieren.

- **Kombination aus menschlicher Expertise und Technologie**. Der Schlüssel zum Stoppen von Ransomware ist eine umfassende Verteidigung, die eine spezielle Anti-Ransomware-Technologie und eine von Menschen geführte Bedrohungsjagd

kombiniert. Die Technologie bietet den Umfang und die Automatisierung, die ein Unternehmen benötigt, während menschliche Expert:innen am besten in der Lage sind, die verräterischen Taktiken, Techniken und Verfahren zu erkennen, die darauf hinweisen, dass ein Angreifer versucht, ein Netzwerk zu infiltrieren. Wenn Unternehmen nicht über die entsprechenden Fähigkeiten verfügen, können sie die Unterstützung von externen Cybersicherheitsspezialist:innen in Anspruch nehmen.

Auf tagtäglicher taktischer Ebene

- **Warnungen zuverlässig checken.** Geeignete Tools, Prozesse und Ressourcen (Mitarbeitende) müssen zur Verfügung stehen, um Bedrohungen in der Umgebung zu überwachen, zu untersuchen und darauf zu reagieren. Ransomware-Gruppen planen ihre Angriffe oft außerhalb der Stoßzeiten, an Wochenenden oder in den Ferien, da sie davon ausgehen, dass nur wenige oder gar keine Mitarbeiter:innen aufpassen.

- **Immer wichtig: Sichere Passwörter.** Starke Passwörter sind eine der ersten Verteidigungslinien. Passwörter sollten einmalig oder komplex sein. Dies lässt sich mit einem Passwort-Manager, der die Anmeldedaten der Mitarbeitenden speichern kann, leichter bewerkstelligen.

- **Multifaktor-Authentifizierung (MFA).** Selbst starke Passwörter können kompromittiert werden. Jede Form der Multifaktor-Authentifizierung ist besser als gar keine, um den Zugang zu wichtigen Ressourcen wie E-Mail, Remote-Management-Tools und Netzwerkressourcen zu sichern.

- **Sperrung zugänglicher Dienste.** IT-Teams sollten Netzwerk-Scans von außen durchführen sowie Ports, die häufig von VNC, RDP oder anderen Fernzugriffstools verwendet werden, identifizieren und sperren. Wenn ein Rechner über ein Remote-Management-Tool erreichbar sein muss, sollte dieses Tool hinter ein VPN oder eine vertrauenswürdige Netzwerkzugangslösung gesetzt werden, die MFA als Teil der Anmeldung verwendet.

- **Auf Segmentierung und Zero-Trust setzen.** Kritische Server sollten voneinander und von Workstations getrennt werden, indem sie in separate VLANs eingebunden werden. Gleichzeitig sollte auf ein Zero-Trust-Netzwerkmodell hingearbeitet werden.

- **Offline-Backups von Informationen und Anwendungen.** Backups sollten auf dem neuesten Stand sein und ihre Wiederherstellbarkeit muss sichergestellt sein. Ebenso nützt eine Kopie des Backups offline.

- **Inventarisierung von Vermögenswerten und Konten.** Unbekannte, ungeschützte und nicht gepatchte Geräte im Netzwerk erhöhen das Risiko und schaffen eine Situation, in der bösartige Aktivitäten unbemerkt bleiben könnten. Eine aktuelle Bestandsaufnahme aller angeschlossenen Recheninstanzen ist unerlässlich. Es sollten Netzwerk-Scans, IaaS-Tools und physische Überprüfungen gemacht werden, um sie zu lokalisieren und zu katalogisieren. Zudem muss Endpunktschutz-Software auf alle Rechner, die nicht geschützt sind.

- **Korrekte Konfiguration der Sicherheitsprodukte**. Auch ungeschützte Systeme und Geräte sind anfällig. Es ist wichtig, dass die Sicherheitslösungen ordnungsgemäß konfiguriert sind, und die Sicherheitsrichtlinien regelmäßig überprüft und, falls erforderlich, validiert und aktualisiert werden. Neue Sicherheitsfunktionen werden nicht immer automatisch aktiviert. Der Manipulationsschutz sollte aktiv sein.

- **Überprüfung von Active Directory (AD).** Unternehmen sollten regelmäßig alle Konten in der AD überprüfen, damit nicht mehr Konten Zugriff haben, als für ihren

Zweck erforderlich ist. Sobald Mitarbeitende aus dem Unternehmen ausscheiden, gilt es ihre Konten umgehend zu deaktivieren.

- **Alles patchen**. Windows und andere Betriebssysteme und Software müssen auf dem neuesten Stand sein. Patches bitte korrekt installieren und für kritische Systeme wie Computer mit Internetanschluss oder Domänencontroller bereitstellen.

Sophos Endpoint-Produkte, wie etwa Intercept X, schützen Anwender, indem sie die Aktionen und das Verhalten von Ransomware und anderen Angriffen erkennen. Die CryptoGuard-Funktion blockiert den Versuch, Dateien zu verschlüsseln. Integrierte Endpoint-Erkennung und -Reaktion, einschließlich Sophos Extended Detection and Response (XDR), können dabei helfen, skrupellose Aktivitäten zu erfassen, wenn zum Beispiel Angreifer kennwortgeschützte Archive erstellen, wie sie bei der Memento Ransomware-Attacke verwendet wurden.

Weitere Informationen finden Sie in dem Report über Memento Ransomware in den SophosLabs Uncut.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de