Moderne Ransomware nutzt uralte Version von Adobe ColdFusion

Vergessene, ungepatchte und veraltete Software bietet ein ideales Einstiegstor für Cyberkriminelle. So auch im aktuellen Fall einer Ransomware-Attacke, die eine 11 Jahre alte Software auf einem Server für sich ausnutzte.

Wiesbaden, 21. September 2021. Sophos hat unter dem Titel „Cring Ransomware Exploits Ancient ColdFusion Server“ eine besonders ausgefuchste Attacke aufgedeckt. Betreiber:innen der Cring Ransomware attackierten ihr Opfer, nachdem sie einen Server gehackt hatten, auf dem eine ungepatchte, 11 Jahre alte Version der Adobe ColdFusion Software lief. Das Opfer nutzte den Server, um Arbeitsblätter und Buchhaltungsdaten für die Gehaltsabrechnungen zu sammeln und eine Anzahl von virtuellen Maschinen zu hosten. Die Angreifer drangen innerhalb weniger Minuten in den internetfähigen Server ein und führten die Ransomware 79 Stunden später aus.

Kriminelle nutzten raffinierte Techniken
Die Sophos-Untersuchung ergab, dass die Angreifer:innen als ersten Schritt die Webseite des Opfers mit automatisierten Tools scannten. Sobald sie herausfanden, dass eine ungepatchte ColdFusion-Version auf dem Server lief, konnten sie innerhalb weniger Minuten eindringen. Danach nutzen sie besonders ausgefeilte Techniken zur Vertuschung: Sie initiierten Codiercode in den Speicher und verwischten ihre Spuren mit überschreibenden Dateien mit fehlerhaften Daten oder gelöschten Logs und anderen Artefakten, die Threat Hunter bei ihren Ermittlungen verwenden. Die Hacker:innen waren zudem in der Lage, Security-Produkte zu deaktivieren, da die Manipulationsschutzfunktion ausgeschaltet war. Schließlich veröffentlichten sie eine Notiz, dass sie Daten exfiltriert haben, die sie veröffentlichen, wenn es nicht zu einem „good deal“ käme.

Andrew Brandt, Principal Researcher bei Sophos:
„Geräte, die anfällige und veraltetet Software verwenden, sind genau die Einfallstore, nach denen Cyberkriminelle als einfachstem Weg zu ihrem Opfer suchen. Die Cring Ransomware ist nicht neu, aber selten. In dem untersuchten Fall bestand das Angriffsziel in einem Service-Unternehmen, bei dem lediglich ein internetfähiger Server mit einer veralteten und ungepatchten Software Tür und Tor für die Attacke öffnete. Erstaunlich ist, dass dieser Server im täglichen Gebrauch war. Oft sind die verletzlichsten Geräte die inaktiven, die beim Upgrade oder Patchen entweder vergessen oder übersehen wurden. Aber ganz unabhängig vom Status – aktiv oder inaktiv – ungepatchte, internetfähige Server oder Geräte sind die primären Ziele für Cyberkriminelle, die nach angreifbaren Eintrittspunkten scannen. IT-Administrator:innen sollten deshalb über eine präzise Inventur aller verbundenen Geräte verfügen und alte, kritische Unternehmenssysteme nicht ins öffentliche Netz stellen. Wenn Organisationen derartige Geräte irgendwo in ihrem Netzwerk haben, können sie geradezu sicher sein, dass Cyberkriminelle von ihnen angezogen werden.“

Zum Schutz vor Cring und weiteren Ransomware-Ablegern empfehlen die Sophos-Experten untenstehende Tipps, die sich in der Prävention bewährt haben. Ausführlichere Anleitungen zu diesen Ratschlägen finden sich im Originalartikel „Cring Ransomware Exploits AncientColdFusion Server“ .

Auf der strategischen Ebene:

- Einsatz eines mehrschichtigen Schutzes
- Kombination von menschlicher Expertise und Anti-Ransomware-Technologie

Auf der täglichen/taktischen Ebene:

- Warnmeldungen kontrollieren und reagieren
- Starke Passwörter verwenden und einfordern
- Multi-Faktor-Authentifizierung (MFA) einsetzen
- Zugängliche Dienste sperren (besonders Ports, die gern von VNC, RDP oder Remote Tools genutzt werden)
- Segmentierung und Zero-Trust betreiben
- Offline Backups von Informationen und Anwendungen verwenden
- Inventur von Anlagen und Konten vornehmen
- Auf korrekt konfigurierte Sicherheitsprodukte achten
- Regelmäßig aktive Verzeichnisse prüfen
- Patchen. Alles.

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.

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

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