Sophos-Forscher entdecken neue Python-Ransomware: Ultra-High-Speed-Angriffe auf ESXi-Server und virtuelle Maschinen

"Dies ist eine der schnellsten Ransomware-Attacken, die Sophos je untersucht hat, und sie scheint genau auf die ESXi-Plattform abzuzielen." - Andrew Brandt, Principal Researcher bei Sophos

Wiesbaden, 5. Oktober 2021 – Sophos gibt Details zu einer neuen, Python-basierten Ransomware bekannt, mit der Cyberkriminelle virtuelle Maschinen auf ESXi-Hypervisoren angreifen und verschlüsseln. Im Report mit dem Titel "Python Ransomware Script Targets ESXi Server for Encryption" beschreiben die Experten der Sophos Labs eine High-Speed-Attacke, die weniger als drei Stunden vom Einbruch bis zur Verschlüsselung benötigte.

"Dies ist eine der schnellsten Ransomware-Attacken, die Sophos je untersucht hat, und sie scheint genau auf die ESXi-Plattform abzuzielen", sagt Andrew Brandt, Principal Researcher bei Sophos. "Python ist eine Programmiersprache, die üblicherweise nicht für Ransomware verwendet wird. Allerdings ist Python auf Linux-basierten Systemen wie ESXi vorinstalliert, so dass Python-basierte Angriffe auf solche Systeme möglich sind. ESXi-Server sind ein attraktives Ziel für Ransomware-Kriminelle, da sie in der Lage sind, mehrere virtuelle Maschinen mit möglicherweise geschäftskritischen Anwendungen oder Diensten gleichzeitig anzugreifen. Angriffe auf Hypervisoren können sowohl schnell als auch äußerst desaströs sein. Ransomware-Gruppen wie DarkSide und REvil haben es bei ihren Angriffen auf ESXi-Server abgesehen."

Ablauf des untersuchten Angriffs
Die Untersuchung ergab, dass der Angriff um 0:30 Uhr an einem Sonntag begann, als ein TeamViewer-Konto gekapert wurde, das auf einem Computer lief, auf dem auch Zugangsdaten für den Domain-Administrator vorhanden waren.
Nur 10 Minuten später nutzen die Angreifenden das Tool Advanced IP Scanner, um nach Zielen im Netzwerk zu suchen. Die SophosLabs gehen davon aus, dass der ESXi-Server im Netzwerk verwundbar war, weil er über ein Active Shell verfügte, eine Programmierschnittstelle, die IT-Teams für Befehle und Updates verwenden. Dadurch konnten die Cyberkriminellen ein sicheres Netzwerkkommunikationstool namens Bitvise auf dem Rechner des Domänenadministrators installieren, das ihnen Fernzugriff auf das ESXi-System einschließlich des Speichers ermöglichte, der von den virtuellen Maschinen verwendet wurde. Gegen 3:40 Uhr morgens wurde die Ransomware aktiviert und verschlüsselte Festplatten der ESXi-Server.

Hinweis für mehr Sicherheit
„Administrator:innen, die ESXi oder andere Hypervisoren in ihren Netzwerken betreiben, sollten bewährte Sicherheitspraktiken befolgen. Dazu gehört die Verwendung von sicheren Passwörtern und der Einsatz einer Multi-Faktor-Authentifizierung, wo immer dies möglich ist", so Brandt. "Die ESXi-Shell kann und sollte immer dann deaktiviert werden, wenn sie von den Mitarbeiter:innen nicht für routinemäßige Wartungsarbeiten verwendet wird, zum Beispiel während der Installation von Patches. Das IT-Team kann dies entweder über die Steuerelemente der Server-Konsole oder über die vom Hersteller bereitgestellten Software-Management-Tools steuern."

Endpoint-Produkte, wie beispielsweise Sophos Intercept X, schützen Systeme, indem sie die Aktionen und Verhaltensweisen von Ransomware und anderen Angriffen erkennen. Der

Versuch, Dateien zu verschlüsseln, wird entsprechend blockiert. Spezielle Sicherheitshinweise für ESXi-Hypervisoren sind hier online verfügbar. Sophos empfiehlt außerdem die folgenden Standard-Best-Practices zum Schutz vor Ransomware und damit verbundenen Cyberattacken:

Sicherheit auf strategischer Ebene

- Einsatz eines mehrschichtigen Schutzes. Es ist wichtiger denn je, Angriffe von vornherein fernzuhalten oder sie so frühzeitig zu entdecken, dass sie keinen Schaden anrichten können. Ein mehrschichtiger Schutz hilft, Attacken an möglichst vielen Stellen im Unternehmen zu erkennen und zu blockieren.
- Kombination von menschlichen Experten und Anti-Ransomware-Technologie. Der Schlüssel ist eine umfassende Verteidigung, die eine spezielle Anti-Ransomware-Technologie und eine von Menschen geführte Bedrohungsjagd kombiniert. Die Technologie inkludiert den Umfang und die Automatisierung, die ein Unternehmen heute zum Schutz benötigt und kombiniert dies mit menschlichen Expert:innen, die in der Lage sind, die verräterischen Taktiken, Techniken und Verfahren der Angriffe zu erkennen. Unternehmen, deren eigenes IT- oder Sicherheitsteam nicht über diese speziellen Fähigkeiten verfügt, können auf die Unterstützung von externen Cybersicherheitsspezialist:innen zählen.

Sicherheit auf taktischer Ebene

- Überwachung und Reaktion auf Warnungen. Unternehmen sollten sicherstellen, dass Tools, Prozesse, Ressourcen und Expert:innen 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.
- Sichere Passwörter im gesamten Unternehmen. Passwörter sollten einmalig oder komplex sein und nie mehrfach verwendet werden. Die Organisation von Passwörtern lässt sich mit einem Passwort-Manager leichter bewerkstelligen.
- Einsatz der 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.
- Dienste für Zugänge sperren. Mit Netzwerk-Scans lassen sich Ports, die häufig von VNC, RDP oder anderen Fernzugriffstools verwendet werden identifizieren und anschließend sperren. Wenn ein Rechner über ein Remote-Management-Tool erreichbar sein muss, sollte dieses Tool mit einem VPN oder einer Netzwerkzugangslösung, die MFA als Teil der Anmeldung verwendet, eingerichtet werden.
- Segmentierung und Zero-Trust. Kritische Server sollten voneinander und von Workstations getrennt sein, indem separate VLANs eingebunden werden und konsequent auf das Zero-Trust-Netzwerkmodell hingearbeitet wird.
- Erstellen von Offline-Backups von Informationen und Anwendungen. Es gilt, Backups auf dem neuesten Stand zu halten und die Wiederherstellbarkeit sicherzustellen. Zudem sollte eine Kopie offline aufbewahrt werden.
- 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 Bestandsaufnahme aller angeschlossenen Recheninstanzen ist unerlässlich. Nützlich dafür sind Netzwerk-Scans, IaaS-Tools und physische Überprüfungen, um alle Komponenten zu lokalisieren, zu katalogisieren und um einen Endpoint-Schutz auf allen Rechnern, die nicht geschützt sind, einzurichten.
- Korrekte Konfiguration der Sicherheitslösungen. Unzureichend geschützte Systeme und Geräte sind anfällig. Es ist wichtig sicherzustellen, dass die Sicherheitslösungen ordnungsgemäß konfiguriert sind und die Sicherheitsrichtlinien regelmäßig überprüft,

validiert und aktualisiert werden. Neue Sicherheitsfunktionen werden nicht immer automatisch aktiviert. Der Manipulationsschutz sollte nie deaktiviert werden und es sollten keine umfassenden Erkennungsausschlüsse konfiguriert werden, die einem Angreifer die Arbeit erleichtern.
- Prüfen des Active Directory. Wichtig ist eine regelmäßige Prüfung aller Konten im Active Directory sowie sicherzustellen, dass keine Konten über mehr Zugriffsberechtigungen verfügen, als für den jeweiligen Zweck erforderlich. Konten von ausscheidenden Mitarbeiter:innen sollten deaktiviert werden, sobald diese das Unternehmen verlassen.
- Patchen. Windows und andere Betriebssysteme und Software sollten immer auf dem neuesten Stand sein. Zudem ist es wichtig, dass Patches sowohl korrekt installiert wurden als auch für kritische Systeme wie Rechner mit Internetanschluss oder Domänencontroller überhaupt vorhanden sind.

Weitere Informationen über Python Ransomware gibt es auf 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