Fünf Tage auf Tuchfühlung mit der Conti-Ransomware

Sophos beschreibt in drei Reports detailliert das Vorgehen einer realen Conti-Ransomware-Attacke und wie sie gestoppt wurde. Mit dabei: Angriffsverhalten, technische Hintergründe und praktische Tipps für IT-Administratoren.

Wiesbaden, 16. Februar 2021 – Conti-Ransomware-Attacken, die vermehrt seit Mitte letzten Jahres ihr Unwesen treiben, sind ein eindrückliches Beispiel dafür, wie Cyberkriminelle mit moderner und ausgebuffter Technologie gezielt ihren Angriff planen und damit ihre Erfolgschancen stark verbessern, erfolgreich in Unternehmensnetzwerke einzudringen. In drei detaillierten Reports beschreibt das Sophos-Rapid-Response-Team eine reale Attacke und den Verlauf über fünf Tage hinweg: „Dies war ein sehr schneller und potenziell verheerender Angriff", sagt Peter Mackenzie, Manager von Sophos Rapid Response. „Bei unserer forensischen Aufarbeitung haben wir gesehen, dass die Angreifer Lücken in der Firewall ausnutzten, um in nur 16 Minuten das Netzwerk zu kompromittieren und Zugriff auf die Domain-Administrationsdaten zu erhalten. Danach setzten die Angreifer Cobalt Strike Agents auf den Servern ein, die das Rückgrat des Ransomware-Angriffs bilden sollten."

Das Besondere an diesem Angriff war, dass die Cyberkriminellen ihn eigenhändig steuerten und nicht alles einer automatisierten Routine überließen. Bei diesen von Menschenhand gesteuerten Attacken können sich die Angreifer anpassen und in Echtzeit auf veränderte Situationen reagieren. Dank solcher Flexibilität haben diese Attacken höhere Erfolgschancen und Opfer können sich nicht in Sicherheit wiegen, nur weil ein erster Angriffsversuch entdeckt und vereitelt wurde. Denn dann passiert, was im folgenden Tagebuch einer realen Conti-Ransomware-Attacke beschreiben wird – zum Glück in diesem Fall mit Happy End:

Tag 1: Die Angreifer durchdringen die Firewall und benötigen nur 16 Minuten, um auf zwei Servern des Opfers den Admin-Account zu kapern. Im Anschluss setzen sie einen Cobalt Strike Agent auf dem ersten Server ein, bis dieser Angriff vom Opfer entdeckt und gestoppt wird. Nur 15 Minuten später wiederholen die Angreifer ihre Aktion auf dem zweiten Server, und diese Attacke wird nicht bemerkt. Einmal den Fuß in der Tür, begeben sich die Angreifer auf „Schleichfahrt" durch das Firmennetzwerk des Opfers und infizierten einen dritten Server.

Tag 2: Es werden keine Angriffsaktivitäten vom Opfer bemerkt.

Tag 3: Die Angreifer sehen sich rund zehn Stunden lang nach Dateiordnern mit potenziell interessanten Informationen um und ziehen diese mit Hilfe des legitimen Open-Source-Management-Tools RClone, das unbemerkt auf dem dritten gekaperten Server installiert wurde, ab. Unter anderem sind Daten aus der Finanz-, HR- und IT-Abteilung betroffen.

Tag 4: Die Angreifer nutzen ihr aus Tag 1 gesammeltes Wissen über die Endpoint- und Serverstruktur und installieren zunächst einen Cobalt Strike Agent auf einem vierten Server, um die Ransomware zu testen. Nach der Erfolgsmeldung installieren sie Cobalt Strike auf nahezu 300 Geräten und starten nach weiteren 40 Minuten die Conti-Ransomware. Dabei laden die kompromittierten Endpoints den Code von verschiedenen Command&Control-Adressen und führen diesen aus. Das perfide dabei: Es werden keine Daten auf die Festplatten geschrieben, sondern die Ransomware direkt im Arbeitsspeicher ausgeführt, um einer Entdeckung zu entgehen. In der Folge versucht die Ransomware drei Stunden lang Daten zu verschlüsseln, wird auf den mit Sophos Intercept X geschützten Rechnern allerdings trotz der Verschleierungstaktik geblockt. Das angegriffene Unternehmen kappt nun die Internetverbindung mit Ausnahme der Sophos-Anwendung, fährt die kritische

Infrastruktur herunter und stoppt die Arbeitsprozesse. Das Sophos Rapid-Response-Team wird hinzugezogen, identifiziert die infizierten Endpoints und Server, stoppt die verschiedenen Angriffsprozesse und beginnt, kompromittierte Bereiche wieder herzustellen.

Tag 5: Die Rapid-Response-Eingreiftruppe identifiziert bei ihren abschließenden Recherchearbeiten eine zweite, potenzielle Datenexfiltrierung, einen zweiten kompromittierten Account sowie verdächtigen RDP-Traffic (Remote Desktop Protocol) durch die anfällige Firewall. Gleichzeitig stellt das Opfer die ungesicherten Endpoints wieder her und fährt die kritische Infrastruktur hoch.

Die Moral von der Geschicht…
Oft sind es die IT-Administratoren, die bei einem Ransomware-Angriff in der direkten Schusslinie stehen. Sie sind diejenigen, die morgens zur Arbeit kommen und alles verschlüsselt samt einer Lösegeldforderung vorfinden. Basierend auf den Erfahrungen seines Rapid-Response-Teams hat Sophos eine Aktionsliste entwickelt, um die herausfordernden ersten Stunden und die folgenden Tage eines Ransomware-Angriffs bestmöglich zu meistern.

- Abschalten des Remote-Desktop-Protokolls (RDP) zum Internet, um Cyberkriminellen den Zugriff auf Netzwerke zu verwehren.
- Wenn der Zugriff auf RDP unbedingt nötigt ist, sollte dieser über eine VPN-Verbindung abgesichert sein.
- Mehrschichtige Sicherheitsmaßnahmen – einschließlich EDR-Funktionen (Endpoint Detection and Response) und Managed-Response-Teams für die 24/7-Überwachung der Netzwerke – verhindern Angriffe und tragen maßgeblich zum Schutz und zur Erkennung von Cyberangriffen bei.
- Ständiges Monitoring bekannter Frühindikatoren, die Ransomware-Angriffen oftmals vorausgehen.
- Anlegen eines Incident-Response-Plans, der kontinuierlich mit den Veränderungen der IT-Infrastruktur und des Unternehmens aktualisiert werden sollte. Externe Experten können hierbei mit viel Erfahrung exzellente Hilfeleistung bieten.

Drei Conti-Ransomware-Reports von Sophos
In den drei Reports von Sophos wird die Conti-Ransomware-Attacke aus unterschiedlichen Blickwinkeln beschrieben und es werden konkrete Handlungsanweisungen für den Fall eines Angriffs gegeben. Die englischsprachigen Berichte stehen unter den folgenden Links zum Download bereit:

Zeitliche Ablauf einer Conti-Ransomware-Attacke:
A Conti Ransomware Attack Day-by-Day

Technische Beschreibung der SophosLabs zur evasiven Natur der Conti-Ransomware:
Conti Ransomware: Evasive by Nature

Anleitung inklusive einer 12-Punkte-Checkliste für IT-Administratoren, um eine Attacke zu bewältigen:
What to Expect When You've Been Hit with Conti Ransomware

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. 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