Ransomware-Bande BlackCat nutzt Pentesting-Tool Brute Ratel als neues Angriffswerkzeug

Sophos X-Ops stellt aktuelle Threat-Intelligence-Ergebnisse vor: Angriffsserie zeigt, wie Cyberkriminelle Computer weltweit über ungepatchte Firewalls und VPN-Dienste infizieren

Wiesbaden, 26. Juli 2022 – Sophos X-Ops enthüllt in dem neuen Bericht „BlackCat Ransomware Attacks Not Merely a Byproduct of Bad Luck“, dass die Ransomware-Bande ihr Arsenal an Angriffswerkzeugen um das Pentesting-Tool Brute Ratel erweitert hat. Der Artikel beschreibt eine Reihe von Ransomware-Angriffen, bei denen BlackCat ungepatchte oder veraltete Firewalls und VPN-Dienste nutzte, um weltweit in anfällige Netzwerke und Systeme in verschiedenen Branchen einzudringen.

Die BlackCat Ransomware tauchte erstmals im November 2021 als selbsterklärter „Marktführer“ im Ransomware-as-a-Service-Bereich auf und erregte schnell Aufmerksamkeit durch seine ungewöhnliche Programmiersprache Rust. Bereits im Dezember 2021 wendeten sich die betroffenen Unternehmen an Sophos Rapid Response, um mindestens fünf Angriffe mit BlackCat untersuchen zu lassen. Bei vier dieser Vorfälle erfolgte die Erstinfektion durch die Ausnutzung von Schwachstellen in Produkten verschiedener Firewall-Anbieter. Eine dieser Schwachstellen stammt aus dem Jahr 2018, eine andere wurde im vergangenen Jahr entdeckt. Sobald die Cyberkriminellen in das Netzwerk eingedrungen waren, konnten sie sich die auf diesen Firewalls gespeicherten VPN-Zugangsdaten beschaffen. Dies ermöglichte es ihnen, sich als autorisierte Benutzer anzumelden und dann mithilfe des Remote-Desktop-Protokolls (RDP) auf Schleichfahrt durch die Systeme zu gehen.

Wie schon bei früheren BlackCat-Vorfällen nutzten die Angreifenden auch Open-Source- und kommerziell erhältliche Tools, um zusätzliche Backdoors und alternative Wege für den Fernzugriff auf die Zielsysteme zu schaffen. Dazu gehörten TeamViewer, nGrok, Cobalt Strike und Brute Ratel.

„Bei BlackCat und anderen Angriffen konnten wir in letzter Zeit beobachten, dass die Bedrohungsakteure sehr effizient und effektiv arbeiten. Sie nutzen bewährte Methoden wie Angriffe auf verwundbare Firewalls und VPNs. Sie waren aber auch bei der Umgehung von Sicherheitsmaßnahmen sehr innovativ und wechselten bei ihren Angriffen zum neueren Post-Exploitation C2-Framework Brute Ratel“, erläutert Christopher Budd, Senior Manager, Threat Research bei Sophos.

Angriffe ohne klares Muster, einzige Gemeinsamkeit: Schwachstellen als leichte Beute
Bei den Angriffen konnte aber kein klares Muster beobachtet werden. Sie erfolgten in den USA, Europa und Asien bei großen Unternehmen, die in verschiedenen Industriesegmenten tätig sind. Die angegriffenen Unternehmen wiesen jedoch bestimmte Schwachstellen in ihrer Umgebung auf, die den Angreifern die Arbeit erleichterten. Dazu gehörten veraltete Systeme, die nicht mehr mit den neuesten Sicherheits-Patches aktualisiert werden konnten, das Fehlen einer mehrstufigen Authentifizierung für VPNs und flache Netzwerke (Netzwerk von gleichberechtigten Knoten)

„Der gemeinsame Nenner all dieser Angriffe ist, dass sie leicht durchzuführen waren”, so Budd. „In einem Fall installierten dieselben BlackCat-Angreifer Kryptominer einen Monat vor dem Start der Ransomware. Unsere jüngsten Untersuchungen machen deutlich, wie wichtig es ist,

bewährte Sicherheitsverfahren zu befolgen. Sie können immer noch Angriffe verhindern und vereiteln, auch Mehrfachangriffe auf ein einzelnes Netzwerk."

Weiter Informationen über die Serie von BlackCat-Angriffen:
BlackCat Ransomware Attacks Not Merely a Byproduct of Bad Luck
Sophos hat außerdem einen nGrok Incident Response Guide zusammengestellt, der Sicherheitsteams dabei hilft, Angreifer daran zu hindern, das nGrok Tool zu missbrauchen.

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 Anwendern 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 http://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