Neue Ransomware startet PCs im abgesicherten Modus, um Schutzmechanismen auszuhebeln

SophosLabs beschreibt in aktuellem „Snatch"-Report detailliert das Vorgehen der Hacker und liefert interessante Einsichten in die Cybercrime-Szene. Nicht nur das Verschlüsseln von Daten, sondern auch das gezielte Herausfiltern für spätere Erpressungen in Zusammenhang mit der DSGVO scheint immer beliebter zu werden.

Wiesbaden, 10. Dezember 2019 – SophosLabs und Sophos Managed Threat Response haben einen Bericht über eine neue Ransomware veröffentlicht, die eine bisher noch nicht bekannte Angriffsmethode verwendet: Die sogenannte Snatch-Ransomware geht mit variierenden Techniken vor und veranlasst unter anderem einen Neustart übernommener Computer im abgesicherten Modus, um verhaltensorientierte Schutzmaßnahmen, die speziell nach Ransomware-Aktivitäten wie das Verschlüsseln von Dateien Ausschau halten, zu umgehen. Sophos geht davon aus, das Cyberkriminelle damit eine neue Angriffstechnik etabliert haben, um fortschrittliche Schutzmechanismen auszuhebeln.

Neben der neuen Angriffstaktik belegt ein weiterer interessanter Fund, dass sich ein anderer Trend fortzusetzen scheint: Kriminelle filtern immer häufiger Daten heraus, bevor die eigentliche Ransomware-Attacke startet. Die entwendeten Daten könnten zu einem späteren Zeitpunkt für Erpressungen, auch in Zusammenhang mit der DSGVO, verwendet werden. Ähnliches Verhalten konnten die SophosLabs zum Beispiel bei Ransomware-Gruppen wie Bitpaymer feststellen.

„Wir gehen davon aus, dass sich derartige Hybride aus Daten-Diebstahl und Ransomware in Zukunft häufen werden", so Michael Veit, IT-Security-Experte bei Sophos. „Snatch ist ein weiteres Beispiel für eine automatisierte Angriffsmethode, wie sie SophosLabs in seinem Threat Report 2020 beschrieben hat. Sobald Angreifer über Fernzugriffsdienste in ein System eingedrungen sind, nutzen sie das sogenannte Hand-To-Keyboard-Hacking, um möglichst viel Schaden anzurichten." Der Snatch-Report beschreibt, wie Hacker versuchen, Zugang via unsicherer IT-Fernzugriffsdienste zu erlangen, beispielsweise über das Remote Desktop Protocol (RDP). Zudem enthält das Dokument zahlreiche Hintergrundinformationen zur Szene, die unter anderem beschreiben, wie die Snatch-Schöpfer versuchen, Kollaborateure in Dark-Web-Foren zu rekrutieren.

Ebenfalls kein Zufall scheint der Name „Snatch" zu sein. In frühen Versionen der Ransomware findet sich im Erpressungsschreiben die Email-Adresse ImBoristheBlade(at)protonmail.com. Dies könnte eine Referenz an den Film „Snatch" mit Brad Pitt aus dem Jahr 2000 sein, in dem eine KGB-Agentencharakter namens Boris the Blade mit von der Partie ist, der sich durch seine Flinkheit und Zähigkeit auszeichnet. Und auch der von den Hackern im Dark Web genutzte Deckname Bullet Tooth Tony taucht im selben Film auf.

Schutzmaßnahmen gegen Snatch & Co.

- Proaktives Vorgehen beim Threat Hunting: Hier sollte ein professionelles Sicherheitsteam – im Unternehmen oder in Form eines externen Dienstleisters – eingesetzt werden, um mögliche Bedrohungen rund um die Uhr zu überwachen.
- Einsatz von Machine beziehungsweise Deep Learning für das verhaltensbasierte Erkennen von Malware am Endpoint.
- Wo möglich, identifizieren und stoppen von Fernzugriffsdiensten, die aus dem öffentlichen Netz zugänglich sind.

- Ist ein Fernzugriff zwingend für die Arbeitsprozesse nötig, muss dieser unbedingt via VPN mit Multifaktor-Authentifizierung, Passwort-Prüfung und präzisen Zugangs-Kontrollen geschützt sein.
- Jeglicher Server mit Fernzugriff sollte mit aktueller Software ausgestattet sein, hinsichtlich Login-Versuchen und Abweichungen überwacht werden und mit einer Endpoint Sicherheitssoftware geschützt sein.
- Nutzer, die mit Fernzugriffsdiensten eingeloggt sind, sollten für den Rest des Firmennetzwerks nur über begrenzte Rechte verfügen.
- Administratoren sollten für ihre Accounts die Multifaktor-Authentifizierung nutzen.
- Unternehmen können öffentliche Netzwerk-Scan-Dienste verwenden, um nach offenen RDP-Ports in ihrem IP-Bereich zu suchen.

Weitere Informationen zur Snatch-Ransomware mit detaillierten technischen Details finden sich im englischen SophosLabs Snatch Report:
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

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 47.000 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, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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