Sophos entdeckt Code-Ähnlichkeiten in Dridex Botnet und Entropy Ransomware

Analogien im Software-Packer und in den Subroutinen bei forensischen Untersuchungen nach Vorfällen bei einem Medienunternehmen und einer regionalen Behörde aufgespürt.

Wiesbaden, 24. Februar 2022 – Sophos veröffentlicht heute einen neuen Bericht mit dem Titel "Dridex Bots Deliver Entropy in Recent Attacks". Thema ist die Ähnlichkeit in den Codes des Dridex-Botnet und der weniger bekannten Ransomware Entropy. Beide zeigen Analogien in drei Bereichen: im Software-Packer, der zur Verschleierung des Ransomware-Codes verwendet wird, in den Malware-Subroutinen für das Auffinden und zum Verschleiern von Befehlen (API-Aufrufe) sowie in den Subroutinen, die zur Entschlüsselung von kodiertem Text verwendet werden.

Die Security-Experten von Sophos entdeckten die Ähnlichkeiten bei der Untersuchung von zwei Vorfällen, bei denen Angreifer Dridex verwendeten, um Entropy Ransomware zu verbreiten. Die Angriffe richteten sich gegen ein Medienunternehmen und eine regionale Regierungsbehörde. Dabei wurden speziell angepasste Versionen der Entropy Ransomware Dynamic Link Library (DLL) verwendet, die den Namen des Ziels in den Ransomware-Code einbetteten. Bei beiden Angriffen setzten die Angreifer zudem Cobalt Strike auf einigen Ziel-Computern ein und schleusten mit dem Komprimierungstool WinRAR Daten in den Cloud-Speicher ein, bevor sie die Ransomware auf ungeschützten Computern starteten.

„Es ist nicht ungewöhnlich, dass Malware-Kriminelle den Code mit anderen austauschen, diesen ausleihen oder sogar stehlen. Dies geschieht mit dem Ziel, sich die Arbeit zu sparen, einen eigenen Code zu erstellen, die Zuordnung zu verschleiern oder Security-Forscher abzulenken. Diese Vorgehensweise erschwert die Beweisführung, um eine Familie verwandter Malware zu bestätigen oder 'False Flags' zu identifizieren", erklärt Andrew Brandt, Principal Researcher bei Sophos. „Bei dieser Analyse hat sich Sophos auf die Aspekte des Codes konzentriert, die offensichtlich sowohl Dridex als auch Entropy verwendet haben, um eine forensische Analyse zu erschweren. Unsere Forscher stellten fest, dass die Unterprogramme in beiden Schadprogrammen einen grundsätzlich ähnlichen Codefluss und eine ähnliche Logik aufweisen."

Unterschiedliche Angriffsmethoden trotz Ähnlichkeiten im Code

Neben den Ähnlichkeiten im Code hat die Sophos auch einige bemerkenswerte Unterschiede festgestellt. Bei dem Angriff auf das Medienunternehmen nutzten die Angreifer den ProxyShell-Exploit, um einen Exchange-Server anzugreifen und einen Remote-Shell-Befehl zu installieren. Diese nutzten die Angreifer später, um Cobalt Strike Beacons auf andere Computer zu verbreiten. Die Angreifer waren vier Monate lang im Netzwerk, bevor sie Anfang Dezember 2021 Entropy starteten.

Bei dem Angriff auf die Regierungsorganisation wurde das Ziel über einen bösartigen E-Mail-Anhang mit der Malware Dridex infiziert. Die Angreifer nutzten anschließend Dridex, um weitere Malware zu verbreiten und sich seitlich im Netzwerk des Ziels zu bewegen. Die Analyse des Vorfalls zeigt, dass die Angreifer etwa 75 Stunden nach der ersten Erkennung eines verdächtigen Anmeldeversuchs auf einem einzelnen Computer damit begannen, Daten zu stehlen und sie zu einer Reihe von Cloud-Anbietern zu übertragen.

Patchen und aktiv schützen
Die Untersuchung der Sophos Security-Spezialisten ergab, dass es den Angreifern in beiden Fällen gelang, ungepatchte und anfällige Windows-Systeme auszunutzen und legitime Tools zu missbrauchen. Regelmäßige Sicherheits-Patches und die aktive Untersuchung verdächtiger Meldungen durch Threat Hunter und Security Operations Teams machen es Angreifern schwerer, sich Zugang zu einem Ziel zu verschaffen und schädlichen Code zu installieren. Sophos Endpoint-Produkte, wie beispielsweise Intercept X, schützen Unternehmen, indem sie die Aktionen und Verhaltensweisen von Ransomware und anderen Angriffen, wie sie in dieser Sophos Studie beschrieben werden, erkennen.

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 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