Doppelte Attacke:
Malware Dropper und Finanzbetrug über denselben anfälligen Exchange Server

SophosLabs untersucht Einsatz der Malware-„Verteilstation“ Squirrelwaffle in Kombination mit Social Engineering.
Sophos veröffentlicht zudem einen Incident Guide für Security Teams von Unternehmen, die von Squirrelwaffle betroffen sind.

In einem aktuellen Artikel beschreibt das Sophos Rapid Response Team einen Fall, bei dem Squirrelwaffle-Malware einen anfälligen Exchange-Server ausnutzte, um über gekaperte E-Mail-Threads bösartigen Spam zu verbreiten. Gleichzeitig wurde von den Angreifern ein E-Mail-Thread entwendet, um arglose Nutzer zu einer Geldüberweisung zu verleiten.

Die hierbei verwendete Kombination aus Squirrelwaffle, ProxyLogon und ProxyShell wurde vom Sophos Rapid Response Team in den letzten Monaten mehrfach beobachtet. In diesem Fall zeigt es sich jedoch zum ersten Mal, dass Angreifer Typo-Squatting einsetzen, um die Fähigkeit zum Versenden von Spam aufrechtzuerhalten, auch wenn der Exchange-Server gepatcht wurde. Dabei führen die Cyberkriminellen Nutzer, die beim Eintippen eines Webseitenamens einen Schreibfehler machen, auf eine von ihnen gesteuerte, bösartige Seite.

Squirrelwaffle-Malware und Social Engineering in Zweifach-Angriff
Die aktuelle Attacke konnte dazu genutzt werden, um Squirrelwaffle massenhaft an interne und externe Empfänger zu verteilen, indem manipulierte Antworten in bestehende E-Mail-Threads von Beschäftigten des Unternehmens eingefügt wurden. Die Sophos-Forscher:innen entdeckten, dass während der Durchführung der bösartigen Spam-Kampagne derselbe anfällige Server obendrein für einen Finanzbetrug missbraucht wurde. Mithilfe des Wissens, das die Kriminellen aus einem gestohlenen E-Mail-Thread zogen, versuchten sie per Typo-Squatting Angestellte des betroffenen Unternehmens davon zu überzeugen, eine eigentlich für einen Kunden bestimmte Geldtransaktion an die Angreifer umzuleiten. Und der perfide Betrug wäre beinahe geglückt: Die Überweisung an die Cyberkriminellen wurde bereits genehmigt, aber zum Glück schöpfte eine Bank Verdacht und stoppte die Transaktion im letzten Moment.

Patchen allein reicht nicht
Matthew Everts, Analyst bei Sophos Rapid Response und einer der Autoren der Studie, sagt: „Bei einem typischen Squirrelwaffle-Angriff über einen anfälligen Exchange-Server endet der Angriff, wenn die Verteidiger die Sicherheitslücke entdecken und beheben, indem sie die Schwachstellen patchen und dem Angreifer die Möglichkeit nehmen, E-Mails über den Server zu versenden. In dem von uns untersuchten Vorfall hätte eine solche Maßnahme den Finanzbetrug jedoch nicht verhindern können, da die Angreifer einen E-Mail-Thread über Kundenzahlungen vom Exchange-Server des Opfers exportiert hatten. Dies ist eine gute Erinnerung daran, dass Patches allein nicht immer ausreichen, um Schutz zu bieten. Bei anfälligen Exchange-Servern muss beispielsweise auch sichergestellt werden, dass die Angreifer keine Web-Shell hinterlassen haben, um den Zugang aufrechtzuerhalten. Und wenn es um ausgeklügelte Social-Engineering-Angriffe geht, wie sie beim Hijacking von E-Mail-Threads eingesetzt werden, ist es für die Erkennung entscheidend, die Mitarbeiter darüber zu informieren, worauf sie achten müssen und wie sie es melden können.“

Hilfe für betroffene Unternehmen: der Squirrelwaffle Incident Guide
Begleitend zum aktuellen Artikel hat Sophos auch einen Squirrelwaffle Incident Guide veröffentlicht, der eine Schritt-für-Schritt-Anleitung zur Untersuchung, Analyse und Reaktion auf Vorfälle mit diesem immer beliebter werdenden Malware-Loader enthält.
Er wird als schädliches Office-Dokument in Spam-Kampagnen verbreitet und erlaubt Cyberkriminellen einen ersten Fuß in die Umgebung eines Opfers zu bekommen sowie einen Kanal zur Verbreitung und Infizierung von Systemen mit anderer Malware aufzubauen.

Der Leitfaden ist Teil einer Reihe von Incident Guides, die vom Sophos Rapid Response Team erstellt werden, um Incident Responder und Security Operations Teams dabei zu unterstützen, weit verbreitete Bedrohungs-Tools, -Techniken und -Verhaltensweisen zu identifizieren und zu beseitigen.

Den Bericht zum beschriebenen Vorfall gibt es unter diesem Link:
https://news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/

Den ausführlichen Leitfaden für Squirrelwaffle-Malware-Vorfälle finden Sie hier:
https://news.sophos.com/en-us/2022/02/15/rapid-response-the-squirrelwaffle-incident-guide/

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

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