Eine alte Bekannte, die nicht müde wird: ClickFix ist bei Cyberkriminellen nach wie vor beliebt

Im Rahmen der kontinuierlichen Untersuchung der im Umlauf befindlichen Malware, haben die Spezialisten von Sophos X-Ops erneut ClickFix als eine zwar alte aber nach wie vor sehr aktive Bedrohung ausgemacht. Die Sicherheitsexperten identifizierten ein breites Spektrum von Organisationen, die in letzter Zeit von dieser Angriffsmethode betroffen waren. Darunter befanden sich insbesondere Unternehmen, die Customer-Relationship- und Kalenderdienste nutzen – Autohäuser, Kliniken und kleine Arztpraxen machten etwa ein Viertel der Organisationen aus, die im März von ClickFix und dem Trojaner SecTopRat betroffen waren.

Ein kriminelles Erfolgsmodell

Die Angriffstaktik ClickFix wird von zahlreichen böswilligen Akteuren verwendet, in einigen Fällen auch von staatlich gelenkten Cyberkriminellen. Ihr Einsatz hat hauptsächlich den Diebstahl von Zugangsdaten zum Ziel.

Dafür nutzen die Bedrohungsakteure kompromittierte Webressourcen - insbesondere JavaScript-Ressourcen, die von kompromittierten WordPress-Websites oder Website-Plugins von Drittanbietern bereitgestellt werden. Bei der Attacke wird ein JavaScript-Code von einer angegriffenen Website geladen, der den Anwender zu einer bestimmten Tastenkombination in einer vermeintlichen Sicherheitsprüfung verleiten soll. Die Tastaturkombination öffnet in Wirklichkeit jedoch das Windows-Befehlsfeld „Ausführen“, fügt einen maliziösen Code ein und führt diesen dann aus. In vielen Fällen wird dabei der Trojaner SecTopRat installiert, der zum Diebstahl von Benutzernamen, Kennwörter und andere Informationen, die den Zugriff auf SaaS-Webseiten, Bankdaten oder Unternehmensnetzwerke erlauben, genutzt wird.

Schutz vor ClickFix & Co.

Die ClickFix-Technik ist zwar schon einige Jahre alt, jedoch gehen die Spezialisten von Sophos X-Ops nicht davon aus, dass diese Angriffsmethode in absehbarer Zeit verschwinden wird. Kompromittierte Anmeldedaten repräsentieren das größte Einfallstor für Netzwerkeinbrüche und daher existiert ein großer, lukrativer Markt für gestohlene Systemzugangsdaten. ClickFix und ähnliche Angriffstechniken mit Benutzerinteraktion und „Social Engineering“, versprechen den Kriminellen eine hohe Erfolgsquote.

Daher sollten Unternehmen regelmäßig auf die Mitarbeiterinformation und Schulung setzen. Wer gut informiert ist, wird vermeintliche Sicherheitsüberprüfungen wie durch ClickFix nicht ausführen. Gleichzeitig sind die technische und menschliche Überwachung von Verhaltensweisen in der Infrastruktur entscheidend, um verdächtige Aktionen, wie die Verwendung der Windows-Verknüpfung „Ausführen“, verdächtige PowerShell-Befehle oder Windows-Installationsprogramme, zu identifizieren. Network Detection and Response (NDR) oder Managed Detection and Response (MDR)-Services helfen Unternehmen, den Angreifern einen entscheidenden Schritt voraus zu sein.

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/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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