Zugangsdaten stehlen und MFA austricksen mit Evilginx

Eine böswillige Mutation des weit verbreiteten nginx-Webservers erleichtert bösartige Adversary-in-the-Middle-Attacken. Sophos X-Ops haben in einem Versuchsaufbau das kriminelle Potential von Evilginx analysiert und geben Tipps für den Schutz.

Evilginx ist eine Malware, die auf dem legitimen und weit verbreiteten Open-Source-Webserver nginx basiert. Sie kann dazu verwendet werden, Benutzernamen, Passwörter und Sitzungs-Token zu stehlen und sie bietet Angreifenden eine Chance, die Multi-Faktor-Authentifizierung (MFA) zu umgehen.

So arbeitet Evilginx

Evilginx nutzt im Kern den legitimen und beliebten Webserver nginx, um den Webverkehr über bösartige Webseiten zu leiten. Diese werden von den Bedrohungsakteuren erstellt, um echte Dienste wie Microsoft 365 zu imitieren – in der Fachsprache wird das als Adversary-in-the-Middle (AitM)-Angriff bezeichnet. Zur Demonstration dieser Angriffstaktik hat Sophos X-Ops eine bösartige Domain und ein Microsoft-Phishlet mit einer eigenen Subdomain eingerichtet. Das Phishlet enthält einen Köder, den der anvisierte Benutzende sieht, wenn die Cyberkriminellen versuchen, Benutzernamen und Passwörter abzufangen.

Die Formulare und Bilder, die der Anwendende sieht, stammen tatsächlich von Microsoft und werden über den Evilginx-Server an den Nutzenden weitergeleitet. Im Backend bietet Evilginx jedoch die Möglichkeit zur Konfiguration der Benutzererfahrung. In den Tests hat Sophos X-Ops ein MFA-geschütztes Benutzerkonto nachgeahmt und konnte diese Hürde sofort umgehen. Der Benutzende erlebt einen „normalen“ Login. Erst wenn ein besonders aufmerksamer Benutzender auf eine der Anwendungen auf der linken Seite des Bildschirms klickt, könnte er bemerken, dass etwas seltsam ist, da er erneut zur Anmeldung aufgefordert wird.

Abfangen von Passwörtern, Sitzungs-Tokens und Cookies

Zusätzlich zum Abfangen von Benutzernamen und Passwörtern werden auch Sitzungs-Token erfasst. Dies ist möglich, indem der Angreifende die Funktion „Angemeldet bleiben“ wählt, sobald die Microsoft-Eingabeaufforderung erscheint. Evilginx speichert diese Daten in einer Datenbank mit Informationen über jede Sitzung – einschließlich der öffentlichen IP-Adresse für den Zugriff auf den Server, den verwendeten Benutzeragenten und – ganz wichtig – das Cookie. Damit braucht der Angreifende nur ein Fenster auf der legitimen Anmeldeseite zu öffnen und das Cookie zu importieren, um sich als legitimer Benutzender anzumelden. Von hier aus haben Cyberkriminelle vollen Zugriff auf das Mailbox-Konto des Benutzeraccounts. Sobald der Zugriff auf das Konto möglich ist, können Cyberkriminelle die MFA-Geräte zurücksetzen, Passwörter ändern und eine Reihe anderer Aktionen durchführen, um sich einen erweiterten Kontenzugriff zu verschaffen.

So kann man sich schützen

Um der Gefahr eines Angriffs mit Evilginx zu begegnen, eignen sich zwei präventive beziehungsweise reaktive Maßnahmen.

Im Rahmen einer reaktiven Gegenmaßnahme sollte der erste Schritt darin bestehen, dem Bedrohungsakteur den Zugriff zu entziehen und die Türe vollständig zu schließen. Zunächst werden dafür alle Sitzungen und Tokens über Entra ID und Microsoft 365 widerrufen, um den erlangten Zugriff zu entfernen. Diese Aktionen können im Benutzerkonto sowohl in Entra ID als auch in Microsoft 365 über die Schaltflächen „Sitzungen widerrufen“ und „Von allen Sitzungen abmelden“ durchgeführt werden.

Als Nächstes gilt es die Passwörter und MFA-Geräte des Benutzers zurückzusetzen. Abhängig von der Art des hinzugefügten MFA-Geräts kann dies einen passwortlosen Zugriff auf das Konto ermöglichen, wodurch das Ändern von Passwörtern und das Entfernen von Sitzungen wirkungslos werden.

Gefahr erkannt, jedoch nicht gänzlich gebannt
Evilginx repräsentiert eine beeindruckende kriminelle Methode zur Umgehung der MFA und zur Kompromittierung von Anmeldeinformationen. Der Existenz von Evilginx sorgt zudem dafür, dass eine komplexe Angriffstechnik vergleichsweise leicht einsetzbar ist, was zu einer weiten Verbreitung führen kann. Allerdings haben die Nutzenden mit den beschriebenen Abhilfemaßnahmen gute Möglichkeiten, den Erfolg eines Angriffs stark einzuschränken.

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