Telefonsystem 3CX weltweit für DLL-Sideloading-Angriff genutzt

Zurzeit sorgt eine trojanisierte Version der beliebten VOIP/PBX-Software 3CX für Schlagzeilen. Das Geschäftstelefonsystem wird weltweit von Unternehmen in 190 Ländern genutzt. Bei der Attacke scheint es scheint sich um einen Supply-Chain-Angriff gehandelt zu haben, bei dem Angreifer ein Installationsprogramm für die Desktop-Anwendung hinzufügen konnten, das letztendlich eine bösartige, verschlüsselte Nutzlast per DLL seitenweise lädt.

Mat Gangwer, VP Managed Threat Response bei Sophos zur aktuellen Situation: „Den Angreifern ist es gelungen, die Anwendung zu manipulieren, um ein Installationsprogramm hinzuzufügen, das DLL-Sideloading verwendet. Durch diese Hintertür wird schließlich eine schädliche, verschlüsselte Nutzlast abgerufen. Diese Taktik ist nicht neu, sie ähnelt der DLL-Sideloading-Aktivität, die bereits bei anderen Attacken zum Einsatz kam. Wir haben drei der entscheidenden Komponenten dieses DLL-Sideloading-Szenarios identifiziert."

Die betroffene Software 3CX ist ein legitimes, softwarebasiertes PBX-Telefonsystem, das unter Windows, Linux, Android und iOS verfügbar ist. Zurzeit scheinen nur Windows-Systeme von dem Angriff betroffen zu sein. Die Anwendung wurde von den Angreifern missbraucht, um ein Installationsprogramm hinzuzufügen, das mit verschiedenen Command-and-Control-Servern (C2) kommuniziert. Bei der aktuellen Attacke handelt es sich um eine digital signierte Version des Softphone-Desktop-Clients für Windows, die einen bösartigen Payload enthält. Die bisher am häufigsten beobachtete Aktivität nach Ausnutzung der Sicherheitslücke ist das Aktivieren einer interaktiven Befehlszeilenoberfläche (Command Shell).

Sophos MDR identifizierte am 29. März 2023 erstmals böswillige Aktivitäten, die sich gegen seine eigenen Kunden richteten und von 3CXDesktopApp stammten. Darüber hinaus hat Sophos MDR festgestellt, dass bei der Attacke ein öffentlicher Dateispeicher zum Hosten verschlüsselter Malware genutzt wurde. Dieses Repository wird seit dem 8. Dezember 2022 verwendet.

„Der Angriff selbst basiert auf einem DLL-Sideloading-Szenario mit einer bemerkenswerten Anzahl beteiligter Komponenten", so Matt Gangwer. „Dies sollte wahrscheinlich sicherstellen, dass Kunden das 3CX-Desktop-Paket verwenden konnten, ohne etwas Ungewöhnliches zu bemerken."

Bis dato hat Sophos folgende, entscheidende Komponenten des Angriffs identifiziert:

- 3CXDesktopApp.exe, der Clean-Loader
- d3dcompiler_47.dll, eine DLL mit einer angehängten verschlüsselten Nutzlast
- ffmpeg.dll, der trojanisierte bösartige Loader

Die Datei ffmpeg.dll enthält eine eingebettete URL, die einen bösartig kodierten ICO-Payload abruft. In einem normalen DLL-Sideloading-Szenario würde der bösartige Loader (ffmpeg.dll) die legitime Anwendung ersetzen; seine einzige Funktion wäre es, die Nutzlast in eine Warteschlange zu stellen. In diesem Fall ist der Loader jedoch vollständig funktionsfähig, wie es normalerweise im 3CX-Produkt der Fall wäre – als Ersatz wird eine zusätzliche Nutzlast in die DllMain-Funktion eingefügt. Dies erhöht zwar die Paketgröße, hat aber möglicherweise bei Anwendern den Verdacht verringert, dass etwas nicht stimmt, da die 3CX-Anwendung funktioniert wie erwartet – selbst während der Trojaner das C2-Beacon adressiert.

SophosLabs hat die schädlichen Domänen blockiert und die folgende Endpoint-Erkennung veröffentlicht: Troj/Loader-AF. Zusätzlich wurde die Liste bekannter C2-Domains blockiert, die

mit der Bedrohung in Verbindung gebracht werden. Diese wird in der IOC-Datei auf dem Sophos GitHub weiter ergänzt. Last but not least wird die bösartige Datei ffmpeg.dll als von geringer Reputation gekennzeichnet.

Screenshots zur Attacke sind unter: https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/

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