Indicators of Compromise

For SentinelOne customers, no action is needed. We've provided technical indicators to benefit all potential victims in hunting for the SmoothOperator trojan.

Recommendations

SentinelOne Protects Against SmoothOperator

Interestingly, Apple's security team investigated and found that the SmoothOperator trojan is delivered via a maliciously crafted version of the 3CX Desktop App.

Further incident response work at 3CX by Mandiant initially led to the identification of a backdoor dubbed SIMPLESEA in the 3CX environment. An investigation revealed that this backdoor was used to attack 3CX PBX installations.

The second stage UpdateAgent, which self-deletes after execution, collects account information about the victim's 3CX installation, specifically the following:

- The hostname and domain name
- The version of the 3CX software
- The username of the victim account
- The operating system

The UpdateAgent then sends these details to a command-and-control (C2) server. The C2 server sends back a payload, which is executed by the UpdateAgent.

The malicious dylib's main purpose is to gather environmental information, send this to a C2 server, and to retrieve a 2nd stage payload, written out to a file.

The cross-platform malware's macOS version was initially triaged by independent security researcher Patrick Wardle, who concluded that the SmoothOperator trojan is designed to steal data from victims.

The macOS Trojans contains a hardcoded URL rather than relying on retrieving the C2 from the icons located on Github. The dylib and UpdateAgent are designed to gather information about the victim's environment and send it to a C2 server.

The 3CX Desktop macOS Trojan contains a shellcode that can maliciously download additional payloads, including a 2020 Chrome update.

The 3CX Desktop App is available for Windows, macOS, and Linux; there are also mobile versions for Android and iOS, as well as a Chrome extension.

Software to Deploy Additional Payloads, Including a 2020 Chrome Update

Patrick Wardle has observed that the SmoothOperator trojan can download additional payloads, including a 2020 Chrome update.

The 3CX PBX client is available for Windows, macOS, and Linux; there are also mobile versions for Android and iOS, as well as a Chrome extension.

The trojanized 3CXDesktopApp is the first stage in a multi-stage attack chain that pulls icon files appended with base64 data from Github and uses a PowerShell script to download and execute payloads.

By Juan Andres Guerrero-Saade, Asaf Gilboa, David Acs, James Haughom, Phil Stokes & SentinelLabs

March 30th, 2023: We have updated our IOCs with contributions from the research community. The compromise includes a code signing certificate used to sign the trojanized binaries.