X_Trader Supply Chain Attack Affects Critical Infrastructure Organizations in U.S. and Europe

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

Threat Hunter TeamSymantec

The X_Trader software supply chain attack affected more organizations than 3CX. Initial investigation by Symantec's Threat Hunter Team has, to date, found that among the victims are two critical infrastructure organizations in the energy sector, one in the U.S. and the other in Europe. In addition to this, two other organizations involved in financial trading were also breached.

As reported yesterday by Mandiant, Trojanized X_Trader software was the cause of the 3CX breach, which was uncovered last month. As a result of this breach, 3CX's software was compromised, with many customers inadvertently downloading malicious versions of the company's voice and video calling software DesktopApp. In addition to wider victims, Symantec has also discovered additional indicators of compromise, listed below.

It appears likely that the X_Trader supply chain attack is financially motivated, since Trading Technologies, the developer of X_Trader, facilitates futures trading, including energy futures. Nevertheless, the compromise of critical infrastructure targets is a source of concern. North Korean-sponsored actors are known to engage in both espionage and financially motivated attacks and it cannot be ruled out that strategically important organizations breached during a financial campaign are targeted for further exploitation.

Malicious Installer

The infection chain starts with the Trojanized installer named X_TRADER_r7.17.90p608.exe (SHA256: 900b63ff9b06e0890bf642bdfcbfcc6ab7887c7a3c057c8e3fd6fba5ffc8e5d6), which is digitally signed by "Trading Technologies International, Inc." and contains a malicious executable named Setup.exe. Our analysis of one version of this executable (SHA256: aa318070ad1bf90ed459ac34dc5254acc178baff3202d2ea7f49aaf5a055dd43) found that when executed, it examined the file named X_TRADER-ja.mst (also contained in the installer) for the following marker bytes at hardcoded offset 0x167000:

5E DA F3 76

If the marker bytes are present, it creates a folder named:

C:\Programdata\TPM

It then copies the file C:\Windows\Sysnative\immersivetpmvscmgrsvr.exe as C:\Programdata\TPM\TpmVscMgrSvr.exe to the new folder.

Next, it will drop two malicious DLLs:

- C:\Programdata\TPM\winscard.dll (SHA256: cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2)
- C:\Programdata\TPM\msvcr100.dll (SHA256: d937e19ccb3fd1dddeea3eaaf72645e8cd64083228a0df69c60820289b1aa3c0)

The content of the dropped files is generated by decrypting chunks of the file X_TRADER-ja.mst mentioned earlier using the XOR algorithm with the following key:

74 F2 39 DA E5 CF

To achieve persistence on the victim's system, the malware invokes a CLSID_TaskScheduler COM object, possibly to create a scheduled task to run periodically the following file:

C:\Programdata\TPM\TpmVscMgrSvr.exe

Setup.exe then drops a file named X_TRADER.exe, also contained within the installer. The content of the dropped file is generated by decrypting chunks from one of its own portable executable resources starting at hardcoded offset 0x1CB40 using the XOR algorithm with the following key:

74 F2 39 DA E5 CF

Setup will then execute X_Trader.exe before deleting itself.

Backdoor Installation

Once installed, the legitimate X_Trader executable side-loads the two malicious DLLs dropped by the installer. The first, winscard.dll, acts as a loader and contains code that will load and execute a payload from the second (msvcr100.dll). The msvcr100.dll file contains an encrypted blob appended to the file. The blob starts with the hex value FEEDFACE, which the loader uses to find the blob.

The process for payload installation is almost identical as that seen with the Trojanized 3CX app, where two side-loaded DLLs are used to extract a payload from an encrypted blob.

In this attack, the payload extracted is a modular backdoor called Veiledsignal (SHA256: e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345). Veiledsignal contains another DLL (SHA256: 19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae), which is a process-injection module. This can be injected into the Chrome, Firefox, or Edge web browsers. The module contains a second DLL (SHA256: f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce), which is a command-and-control (C&C) module. It connects to the following C&C URL:

https://www.tradingtechnologies.com/trading/order-management

Hydra-like Campaign

The discovery that 3CX was breached by another, earlier supply chain attack made it highly likely that further organizations would be impacted by this campaign, which now transpires to be far more wide-ranging than originally believed. The attackers behind these breaches clearly have a successful template for software supply chain attacks and further, similar attacks cannot be ruled out.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

900b63ff9b06e0890bf642bdfcbfcc6ab7887c7a3c057c8e3fd6fba5ffc8e5d6 - Trojanized installer (X_TRADER_r7.17.90p608.exe)

6e989462acf2321ff671eaf91b4e3933b77dab6ab51cd1403a7fe056bf4763ba – Possible Trojanized installer

aa318070ad1bf90ed459ac34dc5254acc178baff3202d2ea7f49aaf5a055dd43 - Malicious component of Trojanized installer (setup.exe)

6e11c02485ddd5a3798bf0f77206f2be37487ba04d3119e2d5ce12501178b378 - Malicious component of Trojanized installer (setup.exe)

47a8e3b20405a23f7634fa296f148cab39a7f5f84248c6afcfabf5201374d1d1 - Benign Windows executable used for side-loading (tpmvscmgrsvr.exe) cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2 – Veiledsignal loader (winscard.dll)

277119738f4bdafa1cde9790ec82ce1e46e04cebf6c43c0e100246f681ba184e – Veiledsignal loader (devobj.dll)

cb374af8990c5f47b627596c74e2308fbf39ba33d08d862a2bea46631409539f – Malicious DLL (msvcr100.dll)

d937e19ccb3fd1dddeea3eaaf72645e8cd64083228a0df69c60820289b1aa3c0 – Malicious DLL (msvcr100.dll)

e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345 - Veiledsignal main component

19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae - Veiledsignal process-injection module

f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce - Veiledsignal communications module

https://www.tradingtechnologies[.]com/trading/order-management - Veiledsignal C&C server

\\.\pipe\gecko.nativeMessaging.in.foo8bc16e6288f2a -Veiledsignal named pipe

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 Edg/95.0.1020.40 - Veiledsignal user agent

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.