# Get 3CX - Absolutely Free!

Agathocles Prodromou April 20, 2023

## Mandiant identifies the source of internal network compromise

While Mandiant's investigation is still ongoing, we now have a clear overall understanding of the attack. Following our previous update, we would like to share some additional technical details to support our customers and the community. We have also published additional indicators of compromise that organizations can leverage for their network defenses.

## Initial Intrusion Vector

Mandiant identified the source of our internal network compromise began in 2022 when an employee installed the Trading Technologies X_TRADER software on the employee's personal computer. Although the X_TRADER installation software was downloaded from the Trading Technologies website, it contained VEILEDSIGNAL malware, which enabled the threat actor (identified as UNC4736) to initially compromise and maintain persistence on the employee's personal computer.

The X_TRADER installer (X_TRADER_r7.17.90p608.exe) was digitally signed by a valid code signing certificate with the subject of "Trading Technologies International, Inc". It was hosted on hxxps://download.tradingtechnologies[.]com. While the X_TRADER software was reportedly retired in 2020 by Trading Technologies, the software was still available for download on the Trading Technologies website in 2022. The code signing certificate used to digitally sign the malicious software was set to expire in October 2022.

For more technical detail on the X_TRADER software supply chain attack, including YARA Rules for hunting, please read Mandiant's blog at https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise.

## Lateral Movement

Following the initial compromise of the employee’s personal computer using VEILEDSIGNAL malware, Mandiant assesses the threat actor stole the employee's 3CX corporate credentials from his system. VEILEDSIGNAL is a fully-featured malware that provided the threat actor with administrator-level access and persistence to the compromised system. The earliest evidence of compromise uncovered within the 3CX corporate environment occurred through the VPN using the employee's corporate credentials two days after the employee's personal computer was compromised.

Additionally, Mandiant identified the use of the Fast Reverse Proxy tool (https://github.com/fatedier/frp) which the threat actor used to move laterally within the 3CX environment. The tool was named MsMpEng.exe and located in the C:\Windows\System32 directory.

## CI/CD Build Environment Compromise

Mandiant’s investigation was able to reconstruct the threat actor’s steps through our environment as they harvested credentials and moved laterally. Eventually, the threat actor was able to compromise both the Windows and macOS build environments. On the Windows build environment, the attacker deployed the TAXHAUL launcher and COLDCAT downloader which persisted by performing DLL hijacking for the IKEEXT service and ran with LocalSystem privileges. The macOS build server was compromised using a POOLRAT backdoor using LaunchDaemons as a persistence mechanism.

## Attribution

Based on the Mandiant investigation into the 3CX intrusion and supply chain attack thus far, they attribute the activity to a threat actor cluster named UNC4736. Mandiant assesses with high confidence that UNC4736 has a North Korean nexus.

## Indicators of Compromise

X_TRADER_r7.17.90p608.exe
SHA256: fbc50755913de619fb830fb95882e9703dbfda67dbd0f75bc17eadc9eda61370
SHA1: ced671856bbaef2f1878a2469fb44e9be8c20055
MD5: ef4ab22e565684424b4142b1294f1f4d

Setup.exe
SHA256: 6e11c02485ddd5a3798bf0f77206f2be37487ba04d3119e2d5ce12501178b378
SHA1: 3bda9ca504146ad5558939de9fece0700f57c1c0
MD5: 00a43d64f9b5187a1e1f922b99b09b77

Code signing certificate serial #
9599605970805149948

MsMpEng.exe
SHA256: 24d5dd3006c63d0f46fb33cbc1f576325d4e7e03e3201ff4a3c1ffa604f1b74a
SHA1: d7ba13662fbfb254acaad7ae10ad51e0bd631933
MD5: 19dbffec4e359a198daf4ffca1ab9165

## Command and Control

Mandiant identified that malware within the 3CX environment made use of the following additional command and control infrastructure.
www.tradingtechnologies[.]com/trading/order-management

## Going Forward

Our priority throughout this incident has been transparency around what we know as well as the actions we’ve taken.

As we wind down our incident investigation, 3CX has taken this opportunity to continue to strengthen our policies, practices, and technology to further protect against future attacks. With that, we’re announcing a **7 Step Security Action Plan**. In this plan, we’re committing to actionable steps to harden our defenses. You can read in more detail here.