Security Update Tuesday 11 April 2023 - Interim Assessment Concluded

By Pierre Jourdan

Published: 2023-04-11 · Archived: 2026-04-05 14:20:42 UTC

Initial Results from Mandiant Incident Response

Following the appointment of Mandiant as our security incident response team, forensic analysis on our network and product is in progress. In a nutshell, the interim assessment concluded:

Attribution

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

Windows-based Malware

Mandiant determined that the attacker infected targeted 3CX systems with **TAXHAUL** (AKA “TxRLoader”) malware. When executed on Windows systems, **TAXHAUL** decrypts and executes shellcode located in a file named <machine hardware profile GUID>.TxR.0.regtrans-ms located in the directory C:\Windows\System32\config\TxR\. The attacker likely chose this file name and location to attempt to blend into standard Windows installations. The malware uses the Windows CryptUnprotectData API to decrypt the shellcode with a cryptographic key that is unique to each compromised host, which means the data can only be decrypted on the infected system. The attacker likely made this design decision to increase the cost and effort of successful analysis by security researchers and incident responders.

In this case, after decrypting and loading the shellcode contained within the file <machine hardware profile GUID>.TxR.0.regtrans-ms was a complex downloader which Mandiant named **COLDCAT**. It is worth noting, however, this malware differs from **GOPURAM** referenced in Kaspersky’s report.

The following YARA rule can be used to hunt for **TAXHAUL** (TxRLoader):

```
 rule TAXHAUL
{
meta:
author = "Mandiant"
created = "04/03/2023"
modified = "04/03/2023"
version = "1.0"
strings:
```

```
$p00_0 = {410f45fe4c8d3d[4]eb??4533f64c8d3d[4]eb??4533f64c8d3d[4]eb}
$p00_1 = {4d3926488b01400f94c6ff90[4]41b9[4]eb??8bde4885c074}
condition:
uint16(0) == 0x5A4D and any of them
}
```

Please note that in a similar way to any YARA rule, this should be properly assessed within a test environment first before usage in production. This also comes with no guarantees regarding false positive rates, as well as coverage for this entire malware family and eventual variants.

MacOS-based Malware

Mandiant also identified a MacOS backdoor, currently named **SIMPLESEA**, located at /Library/Graphics/Quartz (MD5: d9d19abffc2c7dac11a16745f4aea44f). Mandiant is still analysing **SIMPLESEA** to determine if it overlaps with another known malware family.*****

The backdoor written in C communicates via HTTP. Supported backdoor commands include shell command execution, file transfer, file execution, file management, and configuration updating. It can also be tasked to test the connectivity of a provided IP and port number.

The backdoor checks for the existence of its configuration file at /private/etc/apdl.cf. If it does not exist, it creates it with hard-coded values. The config file is single-byte XOR encoded with the key 0x5e. C2 comms are sent over HTTP requests. A bot id is generated randomly seeded with the PID of the malware upon initial execution. The id is sent with C2 communications. A brief host survey report is included in beacon requests. Message contents are encrypted with the A5 stream cipher according to the function names in the binary.

***** Previous reporting mentioned the macOS build server was compromised with SIMPLESEA. Mandiant Intelligence analyzed the sample and determined it to have a high degree of code overlap with POOLRAT, deprecating SIMPLESEA in favor of POOLRAT.

Persistence

On Windows, the attacker used DLL side-loading to achieve persistence for **TAXHAUL** malware. DLL side-loading triggered infected systems to execute the attacker's malware within the context of legitimate Microsoft Windows binaries, reducing the likelihood of malware detection. The persistence mechanism also ensures the attacker malware is loaded at system start-up, enabling the attacker to retain remote access to the infected system over the internet.

The malware was named C:\Windows\system32\wlbsctrl.dll to mimic the legitimate Windows binary of the same name. The DLL was loaded by the legitimate Windows service IKEEXT through the legitimate Windows binary svchost.exe.

Command and Control

Mandiant identified that malware within the 3CX environment made use of the following command and control infrastructure:

- azureonlinecloud[.]com
- akamaicontainer[.]com
- journalide[.]org
- msboxonline[.]com

Discuss this article
