Carbon Black’s TrueBot Detection

By Fae Carlisle

Published: 2023-06-01 · Archived: 2026-04-05 23:44:17 UTC

VMware’s Carbon Black Managed Detection and Response (MDR) team began seeing a surge of TrueBot activity in May 2023. TrueBot, otherwise known as Silence.Downloader has been seen since at least 2017. TrueBot is under active development by Silence, with recent versions using a Netwrix vulnerability for delivery. In this article, we will break down what we have seen in customers’ environments and how Carbon Black MDR detects and responds to the threat.

History

Just as its name suggests, TrueBot is a downloader trojan botnet that uses command and control servers to collect information on compromised systems and uses that compromised system as a launching point for further attacks, as seen recently with Clop Ransomware.

TrueBot was known for using malicious emails to drop their malware but was recently seen using a Netwrix vulnerability as their delivery method. VMware’s MDR team has seen this vulnerability used firsthand in customer environments, as explored below. TrueBot is also using Raspberry Robin (a worm) as a delivery vector.

While Silence Group is known for targeting banks and financial institutions, TrueBot has also been seen targeting the education sector. In the Carbon Black Detection & Notable Attacks section, we break down the sectors that we have seen targeted from our platform.

Attribution

Though a threat actor group called Silence Group is attributed to this malware, Group-IB has linked the group with Russia’s EvilCorp (Indrik Spider) due to the downloaders they use being similar. The MDR team has explored this link and has not found substantial evidence to back this claim.

Researchers thought EvilCorp to be linked to TrueBot due to TrueBot dropping FlawedGrace. FlawedGrace is malware that is attributed to EvilCorp. Though TrueBot drops this payload, the malware operators could purchase access to this tool directly from EvilCorp. Another link explored was TrueBot dropping Clop Ransomware, which was previously used by EvilCorp. However, Clop is ransomware-as-a-service, so anyone can purchase access to this tool. Lastly, Silence is a Russian-speaking cybercriminal group that uses Russian web hosting services. Though EvilCorp is also Russian, this is not strong evidence to link the two, as there are dozens of Russian APTs.

Due to these findings, we cannot say for sure whether EvilCorp and TrueBot are connected.

Carbon Black is very effective at detecting TrueBot and its associated activity. This section will focus on what Carbon Black detected and the visibility into the attack process.

Figure 1.1 Process Chain

The infection appeared to have started with a drive-by-download from Chrome for the executable ‘update.exe’.

The file **c:[redacted]downloads\unconfirmed 875646.crdownload** was first detected on a local disk. The device was on the corporate network using the public address [redacted] The file is not signed. The file was created by the application **c:\program files\google\chrome\application\chrome.exe**.

Figure 1.2 Update.exe being downloaded

A user had to click on this in order to execute the malware. Upon execution, the malware immediately begins to look for EDR and antivirus software.

The application **c:[redacted]ownloads\update.exe** attempted to open the process "c:\program files\cisco\amp\7.5.1.20833\sfc.exe", by calling the function "OpenProcess". The operation was successful.

Figure 1.3 Looking for EDR/AV

Once executed, it connected to 94[.]142.138.61IP, which is a Russian IP address that is known to be attributed to TrueBot. At the address, the executable ‘3ujwy2rz7v.exe’ was downloaded and then launched by cmd.exe.

The file **c:[redacted]ppdata\local\3ujwy3rz7v\3ujwy3rz7v.exe** was first detected on a local disk. The device was on the corporate network using the public address [redacted] United States). The file is not signed. The file was created by the application **c:[redacted]ownloads\update.exe** after it established a TCP/80 connection to 94.142.138.61:80 (located in MOS, Russia) from [redacted]

Figure 1.4 3ujwy2rz7v.exe activity

The executable then connected to the C2 domain name ‘dremmfyttrred[.]com’.

The activity thereafter included dumps of LSASS, exfiltration of data, and system and process enumerations.

Managed Detection and Response stops this activity through first the detection of the activity and then the implementation of system quarantines, hash banning, policy reviews, and policy modifications. Customers are informed of the observed activity and actions taken by the team every step of the way.

Indicators of Compromise

- 45.182.189[.]103
- Dremmfyttrred.com
- 94.142.138[.]61
- Locations: Russia, Panama
- Update.exe
- Document_26_apr_2443807.exe
- fe746402c74ac329231ae1b5dffa8229b509f4c15a0f5085617f14f0c1579040
- 172.64.155[.]188
- 104.18.32[.]68
- 3ujwy2rz7v.exe

Summary

TrueBot can be a particularly nasty infection for any network. When an organization is infected with this malware, it can quickly escalate to become a bigger infection, similar to how ransomware spreads throughout a network. Carbon Black is able to quickly detect TrueBot and its associated activity and, with the help of MDR, be able to detect and contain it early in the attack chain before the threat escalates.
