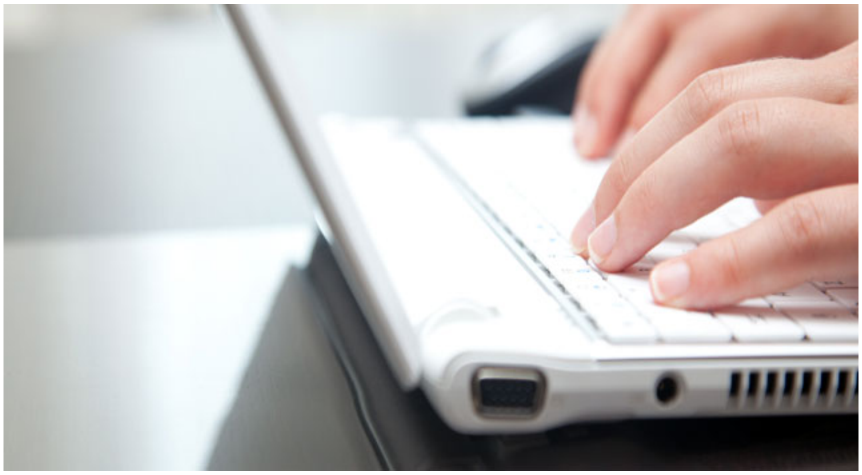
Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers

blog.trendmicro.com/trendlabs-security-intelligence/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers/

May 21, 2020



Cybercriminals are taking advantage of “the new normal” — involving employees’ remote working conditions and the popularity of user-friendly online tools — by abusing and spoofing popular legitimate applications to infect systems with malicious routines. We found two malware files that pose as Zoom installers but when decoded, contains the malware code. These malicious fake installers do not come from Zoom’s official installation distribution channels. One of the samples installs a backdoor that allows malicious actors to run malicious routines remotely, while the other sample involves the installation of the Devil Shadow botnet in devices.

Figure 1. The malicious installers are significantly larger in file size compared to the legitimate Zoom installer.

It is possible that cybercriminals will also take advantage of other video conferencing apps to bundle malware. Because of this, we are closely monitoring other platforms, routines, and samples for signs of tampering and bundling as well. To avoid infection from these malicious fake installers, only download Zoom or any application from trusted sources, including the Google Play store, the Apple App store and https://zoom.us/download.

Fake installer bundles backdoor with remote access capabilities

We found a sample of a fake Zoom installer bundled with backdoor capabilities. Comparing the malicious installer and the dropped legitimate copy with the legitimate installer from the official Zoom site, the dropped file’s properties are closer to the official version. The malicious installer is an executable that contains a number of encrypted files, and will decrypt the malicious version to write into a file (*%User Temp%\Zoom Meetings\5.0.1\setup.exe*) for execution.

Analysis of the malicious sample showed that it kills all running remote utilities upon installation and opens port 5650 and the transmission control protocol (TCP) to gain remote access to the infected system. Simultaneously, it also adds four registries that appear to be configuration settings for the malicious routine.

Figure 2. Opening port 5650

Figure 3. Adding four configurations on installation

Looking into the disassembled functions of added *notification* registry, it showed that the strings contained configurations and values used to notify the command and control (C&C) server that the email has been set up, credentials of the user have been stolen, and flag the infected machine as ready for access.

Figure 4. Disassembling the *notification* registry

After investigating the suspicious behaviors, it will run the legitimate version of Zoom installer to avoid suspicion. Once installed, malicious actors can use the opening to remotely execute commands at any given point.

Devil Shadow botnet

This malicious installer consisted of a file named pyclient.cmd, which contains malicious commands. The cmd_shell.exe file is a self-extracting archive (SFX) containing *new_script.txt*, which contains the C&C server, *madleets.ddns.net* and *shell.bat* to gain persistence, and a copy of the *zoom.exe* installer in the v5.0.1 version. The botnet_start.vbs file runs pyclient.cmd, while the dropped component boot-startup.vbs runs to gain persistence.

The repurposed installer will drop the tampered app installer, the malicious archive and codes, and the commands for persistence and communication.

Figure 5. Malicious files dropped

Figure 6. Malware ensuring persistence

Analysis found that the cybercriminals used the legitimate application *node.exe* to run the file *new_script.txt*, which contains the C&C server.

Figure 7. Communicating with the C&C

A look into the commands in *pyclient.cmd* shows that it connects to the host URL https[:]//hosting303[.]000wenhostapp[.]com, and downloads the binaries related to the app's malicious features and functions.

Figure 8. Downloading the app's binaries

Figure 9. The downloaded binaries perform the commands listed.

The executable named *screenshot.exe* takes screenshots of the user's desktop and active windows. *Webcam.exe* scans the system for any connected webcams.

Figure 10. Screenshot.exe

Figure 11. Webcam.exe

The legitimate Zoom executable will be installed so users do not suspect any malicious activity, but the malware will continue to run on the system even after it is done installing. A look at the task scheduler shows that the malware sends all the gathered information to its C&C every 30 seconds every time the computer is turned on.

Figure 12. Send stolen information every 30 seconds

Conclusion

These installers are hosted on suspicious websites and not from official marketplaces such as the Play Store, App Store, or Zoom's own download center, which could be taken as a telltale sign of their maliciousness. Another observable sign is that the malicious installers drop and run the "legitimate Zoom installer" slower than the one official Zoom installation. The malicious versions take more time to run since they extract the malicious components before running Zoom.

The cybercriminals behind this malware may also be in the process of research and development; they're using multiple components with a legitimate application to evade security programs. Considering that cybercriminals have started tampering with the app, cybercriminals may also be exploring the monetization possibilities of bundling malware into video conferencing apps.

Zoom became more popular during the coronavirus pandemic for its ease of use, and Zoom continues to update the platform in response to issues being disclosed. As with most malicious routines, cybercriminals are riding on its popularity to infect as many systems as possible with forecasts for business continuity citing the increasing necessity of online tools. As such, both pieces of malware can be used to infiltrate systems of high-value targets in enterprises or non-business industries to steal proprietary and confidential information. Unknown to the user, cybercriminals can use these to infiltrate meetings, log keystrokes, use cameras, install other malware, or record audio and video. And given the availability of these apps on a variety of platforms and operating systems, an expansion to other devices may be in the works as well.

Users with remote and work-from-home set ups can apply these best practices for business continuity and productivity:

- Only download apps and software from official marketplaces and platforms.
- Secure your video conferencing apps and operating systems. This can be done by updating device software to the latest version, using passwords for meetings, and configuring host controls.

Trend Micro solutions

Users can supplement these safety measures with a multilayered protection system installed to block and detect known and unknown threats. Trend Micro Apex One™ offers advanced automated threat detection and response against an ever-growing variety of threats. Trend Micro XDR applies artificial intelligence and analytics to the deep data sets collected from Trend Micro solutions across the enterprise, leading to early and better detection.

Indicators of Compromise (IOCs)

Backdoor

SHA256	Description	Detection
4070e977823d74478aec248862302063918fda16b57f2c3b561018605bfbf4fe	svchîst.exe1	Backdoor.Win32.RADMIN.CMU
57bf83837c18a75d2e7327cdf5bfdcc906ccf78d82237ec961a4f1bee85473cf	install.exe1	Trojan.Win32.ZAPIZ.A
9b6b1807f886bb9eccdc170988d6e419e4301c96817f362aca3d01df17c352fd	reg.exe1	Trojan.Win32.ZAPIZ.THA
90728a5b2f22460e1b28e3dc350a95b993a185a6170b4aa5e45b57834b90bcee	Zoom 5.0.1 RUS, ENG.exe	

Devil Shadow botnet

SHA256	Description	Detection
a26f3981ed3784bb86f5223bf14fb0047ff3fd86b8fc94753ce5a3f1702ebb56	Zoom installer.exe	Backdoor.Win32.DEVILSHADOW.THEAABO
93bf084daddb10b3760f4e4424b1bc4d5d5590c30064045d01c8658a6fe50d3a	pyclient.cmd1	Trojan.BAT.DEVILSHADOW.THEAABO
f01da52509792a52c6def452b3ee9b0b78acaca399341926fbe4f3212c42a55e	boot-startup.vbs1	
5b7804919d437688c8811e85c54cb36efba72652bac8093833ca04b811ea87b7	cmd_shell.exe1	Trojan.Win32.DEVILSHADOW.THEAABO
628928fe61e86d3b246a7822b1d1505d3694becc4a73e373f73653851d22f1a5	new_script.txt1	Trojan.JS.DEVILSHADOW.THEAABO
65f725f380c9b90d409539b74bfbd8a57f0fa48843ee79838fa57ad28240feb5	shell.bat1	Trojan.BAT.DEVILSHADOW.THEAABO

URLs

hosting303[.]000webhostapp[.]com/devil_shadow	Malware accomplice
madleets[.]ddns[.]net	C&C server

Malware

We found two malware files that pose as Zoom app installers. One of the samples installs a backdoor that allows malicious actors to run routines remotely, while the other sample involves the installation of the Devil Shadow botnet in devices.

By: Raphael Centeno, Bren Matthew Ebriega, Llalum Victoria May 21, 2020 Read time: (words)

Content added to Folio