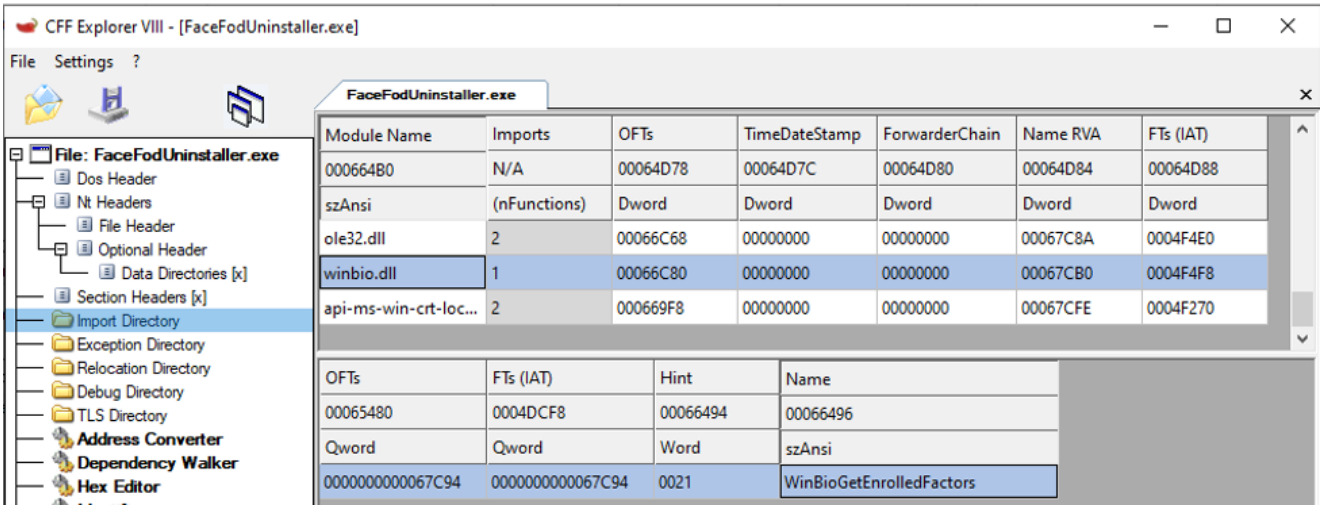
Introducing BIOLOAD: FIN7 BOOSTWRITE's Lost Twin

fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html

December 26, 2019



A couple of months ago, enSilo's endpoint protection platform blocked malicious payloads running in legitimate Microsoft Windows processes. A deeper look uncovered that the attacker abused the DLL search order to load their own malicious DLL. Some of the samples in the environment matched ones described in a recent publication by FireEye about FIN7's new tools and techniques, specifically BOOSTWRITE. Comparing the rest of the samples to BOOSTWRITE revealed they have a common codebase and carry the Carbanak backdoor.

The Abused Target

Windows OS uses a common method to look for required DLLs to load into a program. Adversaries may use this behavior to cause the program to load a malicious DLL, a technique known as DLL search order hijacking (or binary planting).

The abused application in this case is *FaceFodUninstaller.exe*. It exists on a clean OS installation starting from Windows 10 RS4 (1803) at the "*%WINDR%\System32\WinBioPlugIns*" folder. The executable is dependent on winbio.dll, which is usually found in the parent directory ("*%WINDR%\System32*").

Figure 1: FaceFodUninstaller.exe import table

What makes this executable even more attractive in the eyes of an attacker is the fact that it is started from a built-in scheduled task named *FODCleanupTask*, thereby minimizing the footprint on the machine and reducing the chances of detection even further. This demonstrates the group's ongoing technological research efforts.

Figure 2: The built-in task view in Windows Task Scheduler

BIOLOAD

The loader file name is *WinBio.dll* (note the uppercase characters) and is placed by the attacker alongside the executable in the same folder ("*WinBioPlugIns*"), thus leveraging the default DLL search order. Because the file path is under *%WINDIR%*, it means that in order to plant it the attacker needed to have elevated privileges on the victim's machine such as administrator or a SYSTEM account.

Figure 3: WinBioPlugIns folder of an infected machine

Like BOOSTWRITE, this loader was also developed in C++. It exports only a single function which is the one *FaceFodUninstaller.exe* imports.

The samples target a 64-bit OS and were compiled in March and July of 2019. BOOSTWRITE targets 32-bit machines and was compiled (and signed) in May 2019. According to previous reports on the group, they do not falsify compilation timestamps of the binaries.

When the DLL is started it checks the number of command line arguments of the process to decide how to act. When the executable is started by the task scheduler it doesn't have command line arguments and the malware works as follows:

1. Creates a log file at *%TEMP%\~bio<epoch_time>*. Logs are textual and aren't encrypted.
2. Starts itself again as a child process with one command line argument comprised of 32 random upper-case letters.
3. Establishes persistency by using COM objects to access the task scheduler. The malware makes sure the task is enabled, adds a trigger to start it 30 seconds after Windows boots and does not wait for idle state.

When *WinBioGetEnrolledFactors* is called, the malware loads the original *winbio.dll* and invokes the original function.

The worker process loads and executes the payload DLL in-memory. It starts by creating a log file at *%TEMP%\~wrk<epoch_time>*. It then makes sure only a single instance is currently running by creating a named mutex based on environments variables in this fashion:

BIOLOAD also has the encrypted payload DLL embedded in it. In contrast to BOOSTWRITE, it does not support multiple payloads. Furthermore, to decrypt the payload it uses a simple XOR decryption rather than a ChaCha cipher, nor does it access a remote server to fetch the key. Instead, BIOLOAD is tailor-made for every machine it infects as it relies on the machine name to properly derive the decryption key.

The length of the key is 16 bytes and is also embedded in the loader. A portion of the key is overwritten with the result of MurmurHash3 on the key using a CRC32 checksum of the computer name as the seed. This hinders detection by sandboxes and obstruct researchers from analyzing the payload when the relevant context is missing.

Figure 4: Start of the MurmurHash3 function disassembly

The PE loader implementation is the same as the one in BOOSTWRITE. The format of the log file name is similar as well.

The Carbanak Backdoor

As mentioned, the payload this loader carries is the Carbanak backdoor. The samples we extracted from BIOLOAD are newer builds of the backdoor, dated January and April of 2019, according to their timestamps.

One notable addition is that it checks to see if another Anti-Virus (AV) is running on the machine, besides Kaspersky, AVG and TrendMicro. The result, however, has no effect on the operations of the backdoor, unlike with previously detected AVs.

Final Thoughts

This is the first public case of FaceFodUninstaller.exe being abused as host process by a threat actor.

The shared codebase with recent tools attributed to FIN7, together with the same techniques and backdoor, allows to attribute this new loader to the cybercrime group. The timestamps, together with simpler functionality, suggest BIOLOAD is a preceding iteration of BOOSTWRITE.

Since the loader is specifically built for each targeted machine and requires administrative permissions to deploy, it suggests the group gathers information about its targets' networks.

Solutions

This malware uses a common, yet stealthy and effective, method to execute its payload in the context of legitimate processes.

Countermeasures should be in place to detect this malicious behavior. The recently acquired FortiEDR – an Endpoint Detection and Response solution integrated into FortiGate firewalls, FortiSIEM and FortiSandbox - detects and blocks such behavior post-infection to help incident responders quickly mitigate and respond to such threats.

FortiClient detects and blocks the IOCs listed below as **W64/Inject.B!tr.spy** and **W64/Carbanak.A2EB!tr**.

In addition, as part of our membership in the Cyber Threat Alliance, details of this threat were shared in real time with other Alliance members to help create better protections for customers.

IOCs

WinBio.dll (scrubbed key and payload) SHA256

7bdae0dfc37cb5561a89a0b337b180ac6a139250bd5247292f470830bd96dda7
c1c68454e82d79e75fefad33e5acbb496bbc3f5056dfa26aaf1f142cee1af372

Carbanak SHA256

77a6fbd4799a8468004f49f5929352336f131ad83c92484b052a2eb120ebaf9a
42d3cf75497a724e9a9323855e0051971816915fc7eb9f0426b5a23115a3bdcb

Learn more about FortiGuard Labs and the FortiGuard Security Services portfolio. Sign up for our weekly FortiGuard Threat Brief.

Read about the FortiGuard Security Rating Service, which provides security audits and best practices.