ENSILO
SILO YOUR DATA FROM THREAT ACTORS

MENU

MAY 16, 2016 BY YOTAM GOTTESMAN

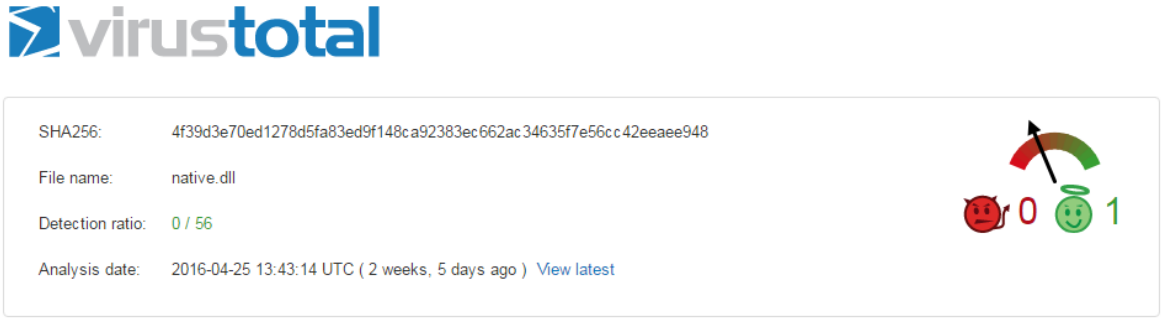
Furtim: The Ultra-Cautious Malware

Furtim is the latest stealthy malware, found in the wild, and its discovery is credited to @hFireF0X.

Clearly, Furtim's developers were more interested in keeping their malware hidden from security's prying eyes than hitting more targets. With stealth a key component, we code-named this downloader Furtim, the Latin translation for "stealthy".

At time of its finding, Furtim showed a 0% detection rate in VirusTotal, signifying that the developers were awarded partial success in their attempt to remain hidden.

In our labs, we purposefully infected a computer to monitor Furtim's activities on the device and its communication with its Command & Control to understand its goals.



/ enSilo's customers are protected from Furtim **/**

What are Furtim's components?

- A driver. The driver tests the target's machine environment – for example, the processes that it runs and the security programs that are installed.
- A downloader. The downloader is the malware component that opens up the backdoor for the following installation of malicious modules of the malware, aka the "payloads". You can consider the downloader as the malware socket, a placeholder that sets everything in place so that when the threat actor decides that the time is ripe, the payload simply plugs into it.
- Three payloads. We found three malicious modules: a power configuration change utility, a stealer and a third file that communicates back to a server. Details on these appear below.

What's so unique about Furtim?

Furtim goes great lengths to ensure that it remains undercover. These measures show that Furtim's developers were very thorough in their activity, anticipating a campaign where they can use Furtim throughout:

- Prior to installation, Furtim checks whether the target machine includes any security product, virtualized or sandboxed environment and foregoes installation if any is found. In fact, Furtim tests the existence of these security parties against a monstrous-size list of more than 400 items, from the obvious well-known products, to those on the verge of the esoteric. While we have seen cases where downloaders and other malwares do not install if other products are present, the list that Furtim tests against is beyond any typical malware.
- Furtim avoids DNS filtering services by scanning the network interfaces on the infected machine. If it finds any of these services, it replaces any known filtering nameserver to public nameservers offered by Google and Level3 Communications.
- Furtim blocks access to nearly 250 security related sites, such as AV update sites, by replacing Windows' hosts file. The blocked sites list also includes technical help sites such as BleepingComputer.com.
- Once installed, the target's device has to be re-booted in order for Furtim to properly latch into the system. At that stage, Furtim ensures that any re-boot policy on a machine, even those defined by an administrator (aka "Group Policy") is overridden so that downloaded payloads will run.
- On first run, Furtim does a few configuration changes on its host system to block the user from accessing the command line and task manager. These measures are taken to prevent the possibility that these tools might reveal, or used to kill, the malicious processes. In addition, Furtim disables Windows notification and pop-up mechanisms.
- Upon initial communication, Furtim collects unique information from the device it is running on, such as the computer name and installation date and sends that information to a specific server. The server stores the received details about the infected machine to ensure that the payload is sent only once. In fact, even if the infected machine sends the

unique information from a different IP, the C&C server will know not to re-send this payload and will return 404 error on any of these subsequent requests. We believe that this is done to prevent security researchers and AV companies trying to collect the samples from the server by repeating previous requests or running the sample multiple times.

What are the payloads that Furtim accepts?

We have witnessed the following three payloads though it is possible that Furtim was developed to accept more than just these three.

1. Power saving configuration tool. The tool disables sleep mode and hibernation to ensure that the system is always up and running unless manually shut down by a user. This way, open communications with the C&C server is maintained.
2. A stealer, named Pony Stealer. Pony Stealer is a commercial credential stealer, considered one of the more powerful stealers in the market today. As its name implies, this malicious program steals saved credentials from various installed programs and sends them back to a server where they are conveniently organized in a searchable web platform for easy access. In practice, stealers are used to aid in lateral movement inside the organization.
3. A third unknown payload. This payload communicates back a list of certain discovered processes to a Russian server. These processes of interest include virtualization environments and security products. On the face of it, Furtim would not have installed were these processes in place, however, this double check is done as a second precautionary step. This third payload may very well include also the main malicious functionality and persistence capabilities. Given its complexity, it will take a while to completely understand that extent of its functionality. We will update its section, once more details are revealed.

Who's behind this attack?

Given the defense measures that Furtim takes, we can imagine that Furtim is more than a downloader used by common fraudsters. The threat actors behind Furtim were dedicated, knowing that it's worth to remain stealthy, even on the expense of hitting more targets, than being revealed.

We do know that the C&C server is hosted at a Russian domain, which resolves to several Ukrainian IP addresses.

Additionally, communications are configured to accept Russian.

With this in mind, it is easy to point a finger at Russia. However, we cannot jump to those conclusions as threat actors typically hide their identity by masquerading as coming from a certain location.

Who is Furtim targeting?

This is one more question we don't have the answer for. Nor do we know how the victim becomes infected. We do know that this is an active malware as the server is live and kicking, communicating with its instances.

How can you protect yourself against Furtim and other such malware?

All evidence points that the threat actors behind Furtim are dedicated and will take the necessary measures to slowly infect and remain stealthy. The dedicated threat actor has the will and time to infiltrate. With this in mind, we need to recognize that infiltration is inevitable, and address threat actors under the assumption that they already inside. This approach requires cutting out in real-time the malicious communications so that once inside, they cannot communicate outbound and in return, the consequences of the attack are prevented.

POST TAGS RESEARCH

Subscribe to enSilo's Blog and Stay on Top of the Latest Security Research and Industry News

Email*

SUBSCRIBE

Recent Posts

- Cyber-Security in 120 Secs: Congress Calling Out on HIPAA
- Cyber-Security in 120 Secs: Symantec Critical Vulnerability
- Cyber-Security in 120 Secs: Breach at the Clinton Foundation
- Cyber-Security in 120 Secs: Nation State Cyber-Espionage
- Cyber-Security in 120 Secs: Cryptxxx Nearing Extinction
- Revenge of the Nerds: enSilo Featured as Gartner's Cool Vendor
- Furtim: The Ultra-Cautious Malware
- Cyber-Security in 120 Secs: Vulnerability in SAP
- Cyber-Security in 120 Secs: The Feds Issue Cyber Espionage Alerts
- Cyber-Security in 120 Secs: Breach at Bay Area's Children's Association

Posts by Topic

- Weekly Security News (41)
- Research (10)
- Industry (7)
- Business (6)
- Windows (5)

Archive by Month

- May 2016 (9)
- October 2015 (7)
- February 2016 (7)
- December 2015 (6)
- January 2016 (6)
- November 2015 (5)
- March 2016 (4)
- April 2016 (4)

- September 2015 (3)
- March 2015 (2)
- April 2015 (2)
- June 2015 (2)

see all