Information Stealer Found Hitting Israeli Hospitals

blog.trendmicro.com/trendlabs-security-intelligence/information-stealer-found-hitting-israeli-hospitals/

June 29, 2017

The abuse of shortcut (LNK) files is steadily gaining traction among cybercriminals. We've seen a plethora of threats that leverage malicious LNK files: from well-known ransomware families, backdoors typically deployed in targeted attacks, and banking Trojans to spam emails, even an exploit to a LNK vulnerability itself. These threats are usually exacerbated by the further abuse of legitimate tools such as PowerShell, or script automation utility AutoIt. It's thus not surprising that we discovered an information stealer employing LNK files, which our sensors detected in Israeli hospitals.

Healthcare is considered a cybercriminal cash cow, as it can be a lucrative source of personally identifiable information that can be monetized in underground marketplaces. Initial findings revealed that any browser-based information, e.g., login credentials, can be stolen, making the use of browser-based management systems and applications important.

We have observed its attempts to gain footholds in the systems and the local networks' shared folders. Another notable aspect we're seeing so far is the combination of worm propagation and stealth capabilities.

Our monitoring and analyses are still ongoing and we will update this post as we find more details about the threat. Here's what we know so far:

Propagation via worm. Initial analysis of the malware indicates it propagates via a worm. It creates copies of itself, including shortcut files, a non-malicious AutoIt executable, and a malicious AutoIt script into the affected system's root directory, i.e., *C:\WinddowsUpdated\ <file copy>.*

Masquerades as a Windows updater. The shortcut files pose as browser and Windows updaters, a web 3D creation tool, and links to the system's Downloads and Games folder.

Execution via AutoIt. AutoIt is a legitimate scripting language software/executable designed to automate tasks (i.e., macros) for several programs in Windows. However, it's known to be abused for wrapping various remote access trojans (RAT). In this case, a legitimate AutoIt executable is used to run a secondary file that contains the malicious commands. We've actually seen a similar threat in the form of the IPPEDO worm (WORM_IPPEDO.B) back in 2014.

It gathers system information. The malware executes a command to retrieve system information via *C:\WINDOWS\system32\cmd.exe /c SystemInfo.*

The LNK files are spawned on the affected machines. The LNK files are embedded with these malicious commands:

cmd.exe /c start ..\WinddowsUpdateCheck\WinddowsUpdater.exe "..\WinddowsUpdateCheck\WinddowsUpdater.zip" & exit

The threat appears to be a highly obfuscated information stealer. The samples we are currently analyzing were highly obfuscated, with payloads hidden under layers of encryption, for instance. The packages we saw each contain malicious 4 LNK files. These LNK files will issue commands leading to AutoIt's execution of .TNT and .EXE files. Based on the behavior we've observed so far, it appears it conducts browser-based information theft and records keystrokes. This actually makes sense given the sensitive nature of the information that goes through healthcare organizations.

As the threat landscape continues to mature and diversify, the IT/system administrators and information security professionals that secure organizations should do the same. Among these countermeasures: patch and keep the system updated, enforce the principle of least privilege, secure the gateways to reduce attack surface, and implement defense in depth by arraying multilayered security mechanisms—from endpoints, networks, and servers.

Indicators of Compromise (IoCs)

- 01e03241c42b12381e5c3ceb11e53f6c5c6bf0fa — WORM_RETADUP.A
- 1186e8d32677f6ac86a35704c9435ccd9ffa8484 — WORM_RETADUP.A
- 479dcd0767653e59f2653b8d3fcddb662a728df4 — LNK_RETADUP.A
- 580ff21d0c9d8aeda2b7192b4caaccee8aba6be4 — LNK_RETADUP.A
- 5f32f648610202c3e994509ca0fb714370d6761d — LNK_RETADUP.A

- 63ac13c121e523faa7a4b871b9c2f63bea05bbff — LNK_RETADUP.A
- 68d90647cf57428aca972d438974ad6f98e0e2b2 — LNK_RETADUP.A
- ce1b01eccf1b71d50e0f5dd6392bf1a4e6963a99 — LNK_RETADUP.A

Update as of June 29, 2017, 2:00 PM (PDT)

Further analysis of the threat reveals that the malware is delivered as an executable file that is bundled with an identically-named file masquerading as another file type. For example, the file named *WinddowsUpdater.exe* comes with a file named *WinddowsUpdater.zip*. While the .EXE file is a legitimate AutoIt file, the alleged .ZIP file is actually an encrypted data file that contains the actual payload. This is the reason why the above mentioned LNK files use a command line to run the executable with only one argument, which is the same the name of the payload file. Looking into its code, the malware contains the following strings, which may indicate that it attempts to gather system information of affected machines:

- @ComputerName
- @UserName
- @LogonDomain
- DriveGetSerial("C:")
- @IPAddress1
- EnvGet("OS") and other os related strings
- @OSLang
- @OSVersion
- @OSBuild

It also connects to the following domain via HTTP:

hxxp://palestineop[.]com/myblog/user

By digging further, we found out that this domain appears to have been registered in November 2016, and that there is evidence that a phishing page has been hosted in the root folder of the domain just a few days after it was registered. The said phishing page, which entices users to click on a link that will supposedly lead them to Yahoo! Mail service, will instead point to the following URL:

newsofpalestine[.]com/newss/gsan

This second URL was already down when we tried to access the page. However, we managed to find evidence that that the domain used to host some news content in the past while also storing some malware. Thus, we strongly believe that the page hosted at *newsofpalestine[.]com/newss/gsan* must have also been a phishing page designed to retrieve email credentials.

We will continue to update this post as we uncover more details about this threat.

Update as of June 30, 2017, 4:05 AM (PDT)

Additional analyses indicate the main malware to be a backdoor (WORM_RETADUP.A) in the form of a worm. It's quite unique in that most remote access Trojans/backdoors deployed in these kinds of attacks often require the help of other malicious components in order to propagate.

RETADUP's backdoor routines include:

- Downloading files
- Connecting to URLs/command and control (C&C) servers
- Opening command-line (cmd) to execute commands
- Installing a keylogger
- Taking screenshots
- Extracting passwords from web browsers Mozilla Firefox, Opera, and Google Chrome
- Starting, terminating, and restarting processes
- Issuing *sleep* command within a specified time
- Shutting down, restarting, and logging off the machine
- Displaying a message in a dialogue box
- Updating a copy of itself from a specific Uniform Resource Identifier (URI) location via C&C communications
- Re-executing a copy of itself

RETADUP is also notable for its stealth. It has a checklist of antivirus (AV) products, script file names, analysis, forensics, and debugging tools as well as sandboxes and virtual machines. It self-destructs if any of these are detected by the malware. Its propagation routine entails dropping copies of itself in all drives, including all existing folders in removable media.

Interestingly, it also checks for the presence of certain LNK files related to online payment and money remittance, indicating the malware may also be stealing information from those sites:

- C:\WinddowsUpdateCheck\ebay.lnk
- C:\WinddowsUpdateCheck\hamazon.lnk
- C:\WinddowsUpdateCheck\hebay.lnk
- C:\WinddowsUpdateCheck\hmoneygram.lnk
- C:\WinddowsUpdateCheck\hpaypal.lnk
- C:\WinddowsUpdateCheck\hpayza.lnk
- C:\WinddowsUpdateCheck\hskrill.lnk
- C:\WinddowsUpdateCheck\hukash.lnk
- C:\WinddowsUpdateCheck\hwestern union.lnk
- C:\WinddowsUpdateCheck\moneygram.lnk
- C:\WinddowsUpdateCheck\paypal.lnk

- C:\WinddowsUpdateCheck\skrill.lnk
- C:\WinddowsUpdateCheck\ukash.lnk
- C:\WinddowsUpdateCheck\western union.lnk

Update as of July 4, 2017, 9:50 PM PDT

RETADUP's original codes resemble another malware, ROWMANTI (WORM_ROWMANTI.B), which emerged in 2015 sporting similar capabilities as RETADUP's. ROWMANTI, in turn, appears to be derived from the IPPEDO worm that surfaced a year earlier.

Underground conversations and code exchanges also know it as "rad worm", released as a "final pack" in 2014 and was using a Visual Basic Script-based RAT (DUNIHI) controller that was modified to support "rad-worm" (IPPEDO). We've seen later versions but found that they were simply re-uploads of this "final pack" with predefined C&C servers rather than the default "Your Domain Here" string.

Snapshot of the controller; it only works with IPPEDO because the initial communication protocol has been changed for ROWMANTI and RETADUP.

The network protocols of the three malware look alike. ROWMANTI and RETADUP's protocols are similar, for instance, but IPPEDO—their predecessor—uses a different separator and keyword at the start of the protocol. Another notable difference is that IPPEDO's communication is in plain text, while ROWMANTI and RETADUP's are encoded in Base64. They also differ in their use of separators and starting string for their initial phone-home communications.

The C&C servers used by ROWMANTI in 2015 also contain the string "rad", which is the original name of the malware used by their developers. We also saw an underground forum post from 2015 showing a code snippet of the Domain Generating Algorithm (DGA) section of the worm (by a different malware author), but this DGA code is present only in RETADUP. This indicates that while the codes of RETADUP originated from the "rad-worm", it also integrated codes from other malware authors.