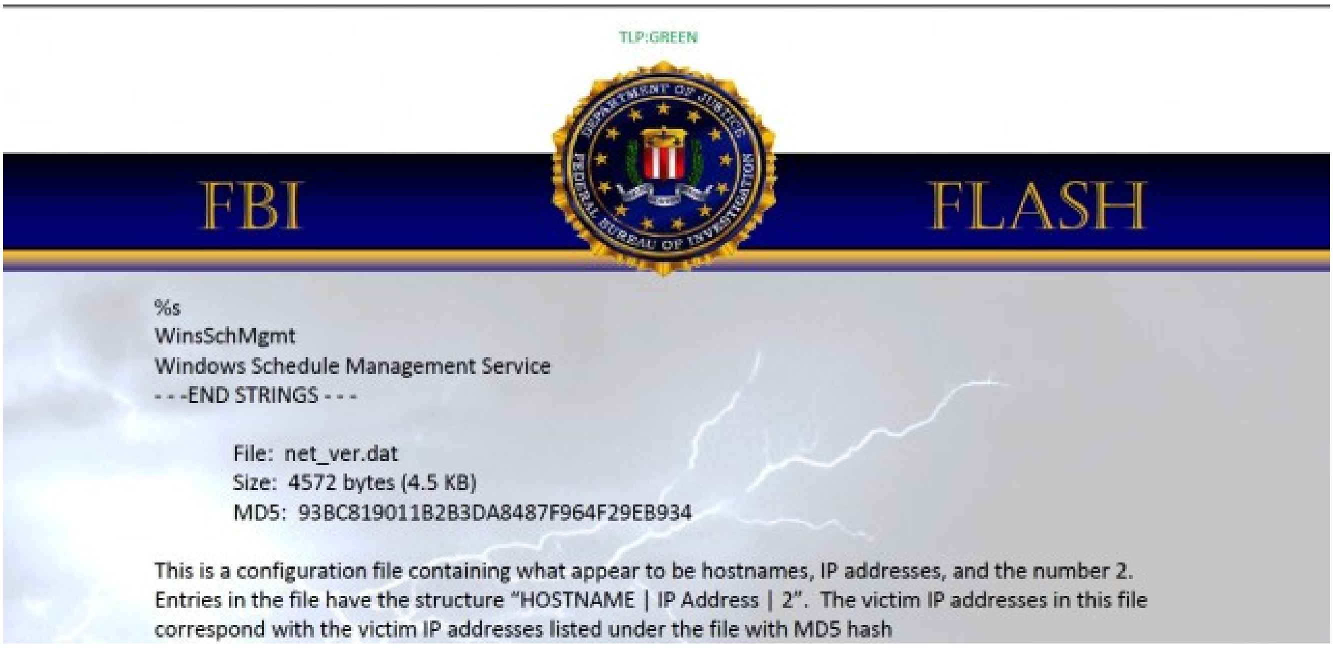
BIZ & IT —

Inside the “wiper” malware that brought Sony Pictures to its knees [Update]

Analysis of code shows it used knowledge of Sony's Windows network to spread and wreak havoc.

SEAN GALLAGHER - 12/4/2014, 9:30 AM



TLP:GREEN

FBI FLASH

%s
WinsSchMgmt
Windows Schedule Management Service
- - -END STRINGS - - -

File: net_ver.dat
Size: 4572 bytes (4.5 KB)
MD5: 93BC819011B2B3DA8487F964F29EB934

This is a configuration file containing what appear to be hostnames, IP addresses, and the number 2. Entries in the file have the structure “HOSTNAME | IP Address | 2”. The victim IP addresses in this file correspond with the victim IP addresses listed under the file with MD5 hash

Part of an FBI memo detailing destructive malware believed to have been used in the Sony Pictures cyber attack.

Details of malware that may have been associated with the attack on Sony Pictures were disseminated in an FBI “Flash” earlier this week. A copy of the memorandum obtained by Ars Technica details “a destructive malware used by unknown computer network exploitation (CNE) operators” that can destroy all the data on Windows computers it infects and spread itself over network file shares to attack Windows servers.

Meanwhile, Re/code reports that Sony is ready to announce that the company has attributed the attack on its network to North Korea, according to sources at the company. Given the details of the malware and its similarity to an attack on South Korean companies last year, a tie to North Korea seems possible, though the people taking credit for the attack claim it was motivated by Sony Pictures’ alleged discrimination in the layoffs and firings of employees during a corporate reorganization started earlier this year.

The malware used in the attack, which has been described by a Sony spokesperson as “very sophisticated,” is almost certainly the same as that identified in the FBI memo. That malware uses Microsoft Windows’ own management and network file sharing features to propagate, shut down network services, and reboot computers—and files named for key Windows components to do most of the dirty work of communicating with its masters and wreaking havoc on the systems it infects.

While the FBI memo provided a means to detect the “beacon” message used by the malware to communicate back to the command and control (C&C) servers used by the attackers who planted it, that information by itself may not protect targeted organizations. That’s because the malware only begins to broadcast back to the C&C servers once it’s been launched—and deletion of data on the targeted network has already begun.

However, other details on the malware provided by the FBI could help find the malware on infected systems before it’s triggered—if attackers don’t significantly alter its code before using it again. And others have already begun security analysis of the malware, unearthing more details about its command and control network and functionality.

Sony Pictures Hacks

Sony Pictures settles employee class action lawsuit over *The Interview* hack

North Korean defector to airdrop DVD, USB copies of *The Interview*

Feds: Sony hackers’ next target will be an unnamed news organization

The unusual suspects: Ex-employees, Lizard Squad may have aided Sony hack

Sony Pictures’ *The Interview* will get a Christmas release after all [Updated]

> View more stories

Special delivery

The delivery mechanism for the malware hasn’t yet been revealed, other than that it arrives like most PC malware—wrapped in an executable “dropper” that installs it and supporting files. In this case, the “dropper” installs itself as a Windows service when executed.

In addition to installing the malware, the service appears to create a network file share using the “%SystemRoot%” Windows environmental variable—which points to the location of Windows system files in the PC’s file directory structure (usually \WINDOWS). It then gives unrestricted access to that share, allowing any other computer on the local network to access it. It also uses the command line of the Windows Management Interface (WMI) in what looks like an attempt to communicate with other computers on the network to launch code on them from that network share to spread itself further—to other desktops as well as to servers. According to analysis of the dropper posted on the community security analysis site Malwr, the dropper communicates with a set of IP addresses in Japan, possibly connected to Sony's corporate network. Then it shuts itself down.

The dropper also installs a file with the same name as Microsoft’s Internet Information Server (IIS), iissrv.exe. Like Internet Information Server, it listens on TCP/IP port 80—the same port used by most web traffic. **Update:** The file actually is a web server—an internal one used to display the scrolling text and JPEG message that victims saw as their computer files were deleted.

At some point—either based on a hard-coded time within the malware package or after some other communication with the attackers—the nasty part of the malware package gets launched—a Windows executable called “igfxtrayex.exe”. It does a few interesting things before it goes on its rampage of destruction—it makes a total of four copies of itself and launches each of them with different command-line arguments, apparently to trigger different parts of the code. It also issues commands to shut down the Microsoft Exchange Information Store service, dismounting Exchange’s databases and making e-mail inaccessible.

The malware then attempts to connect to the C&C network of the attackers; according to the FBI analysis, this is through one of three IP addresses hard-coded into the malware: one in Italy that recently belonged to a HideMyAss VPN exit point, one belonging to a Polish import-export business, and one at a university in Thailand. Additional IP addresses were discovered by other security researchers.

At the same time, the malware starts accessing the hard drive and deleting its contents sector by sector. Once it’s complete, it issues a command to Windows to suspend for two hours, then reboots the computer when it wakes. At that point, the drive is completely wiped.

The malware is able to make physical changes to the hard drive thanks to a commercial disk driver from EldoS, which is installed as part of the malware disguised as a USB 3.0 device driver. The driver gives the malware the ability to overwrite data on the hard drive while running in user mode—not requiring administrative privileges.

Early detection

While the FBI provided a Snort profile for the “beacon” signal sent out by the malware to its C&C servers, detecting that signal doesn’t do much good—it means that the deletion of data has already begun. The FBI, however, did provide a description of the malware that can be used with YARA, an open-source malware research tool, to identify it among malware samples, including the hard-coded IP addresses in the wiper:

```
rule unknown_wiper_error_strings{

meta: unique custom error debug strings discovered in the wiper malware

strings:

$IP1 = "203.131.222.102" fullword nocase

$IP2 = "217.96.33.164" fullword nocase

$IP3 = "88.53.215.64" fullword nocase

$MZ = "MZ"

condition:

$MZ at 0 and all of them

}
```

Given the nastiness of this malware, early detection of the dropper and its installed files would be essential to prevent significant data losses. Companies reliant on Windows and Microsoft server products—especially older versions of Windows—would be particularly vulnerable to the attack.

There’s no explanation from the FBI of how data might have been exfiltrated over the network in the volume claimed by the attackers, who identify themselves as the “Guardians of Peace.” Based on the amount of data stolen, and the nature of the malware itself, it’s likely the attackers had physical access to the network and that the attack may have been ongoing for months—though the wiper malware itself appears to have been compiled just a week before Sony Pictures’ networks were brought down.