Typhoon-like data wiper is latest computer virus headache

August 19 2012, by Nancy Owano

```
00021160  00421160
000211A0  004211A0
000211E0  004211E0
00021220  00421220
00021260  00421260
000212A0  004212A0
000212E0  004212E0
00021320  00421320
00021360  00421360
000213A0  004213A0
000213E0  004213E0
00021420  00421420
00021460  00421460
000214A0  004214A0
000214E0  004214E0
00021520  00421520
00021560  00421560
000215A0  004215A0
```

Source: Kaspersky Lab

(Phys.org) -- A new computer virus is leaving security experts asking what could be the motive and where is the source—but one suspicion is that it is targeting infrastructure in the energy industry. The culprit, called Shamoon, wipes out files and then makes the affected computer unusable.

Guesses that it is going after the energy sector are based on a recent incident where the network for the national oil company in Saudi Arabia was taken offline following a malware intrusion. In a Saudi Aramco statement acknowledging the attack, but not naming any specific virus, the explanation was disruptions were "suspected to be the result of a virus that had infected personal workstations without affecting the primary components of the network." It affirmed the continued integrity of its networks.

Security experts set about trying to explore details of the virus and issued their statements. According to Symantec, “W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable.”

Kaspersky Lab noted that this new virus has a file named Wiper. “The “wiper” reference immediately reminds us of the Iranian computer-wiping incidents from April 2012 that led to the discovery of Flame,” said a Kaspersky source.

That led them to ask if this was another Wiper incident similar to the attack in Iran. They answered their own question, No.

“Based on researching several systems attacked by the original Wiper, is that it is not. The original “Wiper” was using certain service names (“RAHD...”) together with specific filenames for its drivers (“%temp%~dxxx.tmp”) which do not appear to be present in this malware. Additionally, the original Wiper was using a certain pattern to wipe disks which again is not used by this malware.” Kaspersky Lab called Shamoon “the work of script kiddies.”

Nonetheless, the attack is considered a grown-up headache in that it makes computers unusable. The person’s PC is unbootable. The machine’s data is wiped. A list of the wiped files is passed to the attacker’s center, in turn replacing the files with JPEG images. This move successfully thwarts rescue attempts to get the deleted files back.

What puzzled security sleuths examining Shamoon is that its motive, unlike other worms, was not to steal information, but just to wipe it off. Seculert, security specialists, said the code had unusual characteristics compared with that seen in other attacks."The interesting part of this malware is that instead of staying under the radar and collect information, the malware was designed to overwrite and wipe the files," the company said.

While the malware does not try to steal sensitive information, it does appear to be concerned with names of the files that it deleted and how many files and the IP address of the infected computers.

One Symantec researcher said that, since the malware was an executable, it might arrive at the victim’s workstation as an e-mail attachment.

Generally, security firms examining Shamoon agreed that the malware was not widespread and was launched in very focused attacks.

By Friday, reports coming in from the UK said that, in a post on the website Pastebin.com, the Arab Youth Group claimed responsibility for the attack. The group called the attack a message to Saudi officials.

More information: www.securelist.com/en/blog?pri … 1&weblogid=208193786

Citation: Typhoon-like data wiper is latest computer virus headache (2012, August 19) retrieved 27 April 2024 from https://phys.org/news/2012-08-typhoon-like-wiper-latest-virus-headache.html