SECURELIST

Shamoon the Wiper - Copycats at Work

0.7

GReAT
Kaspersky Lab Expert
Posted August 16, 16:05 GMT
Tags: Targeted Attacks, Wiper, Microsoft

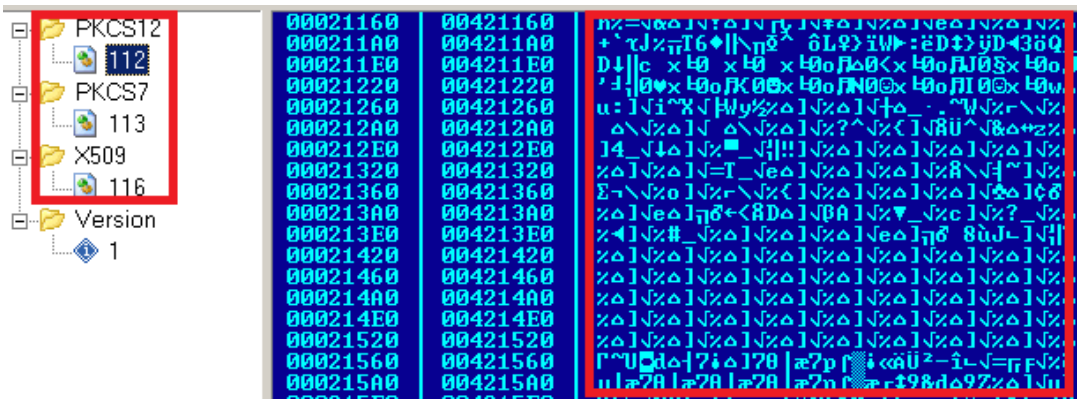
Earlier today, we received an interesting collection of samples from colleagues at another anti-malware company.

The samples are especially interesting because they contain a module with the following string:

```
C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb
```

Of course, the ?wiper reference immediately reminds us of the Iranian computer-wiping incidents from April 2012 that led to the discovery of Flame.

The malware is a 900KB PE file that contains a number of encrypted resources:



The resources 112, 113 and 116 are encrypted using a 4 byte XOR operation. They keys for decryption, including another resource from one of the binaries are:

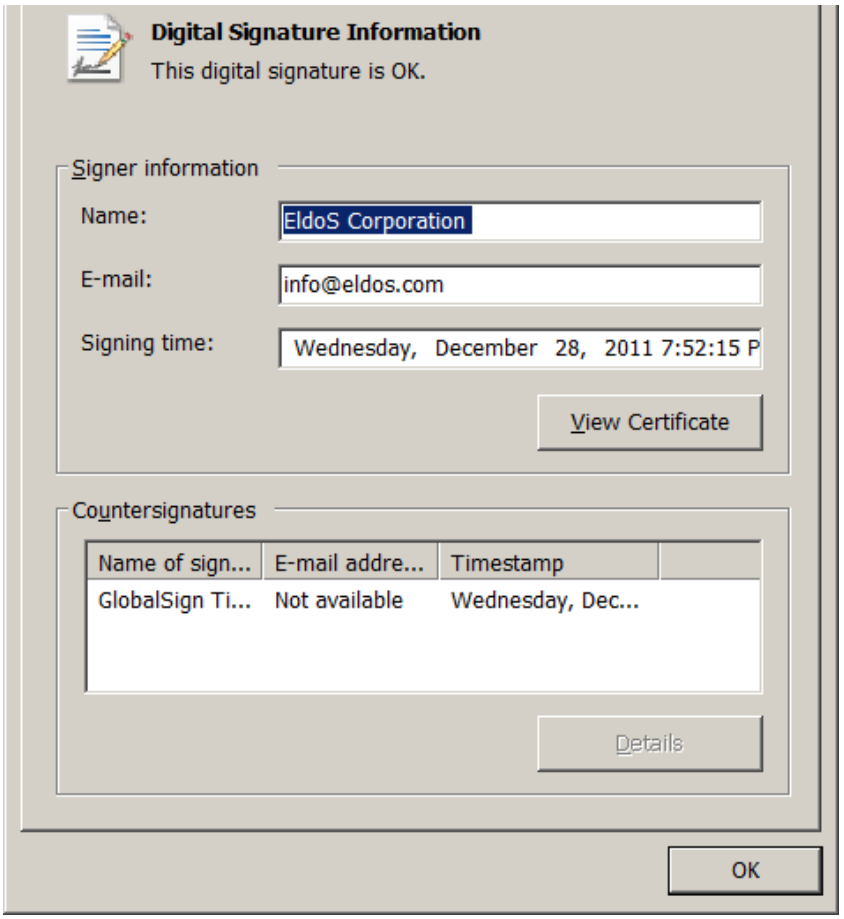
```
{0x25, 0x7f, 0x5d, 0xfb}
{0x17, 0xd4, 0xba, 0x00}
{0x5c, 0xc2, 0x1a, 0xbb}
{0x15, 0xaf, 0x52, 0xf0}
```

The malware appears to be collecting information about ?interesting files on the infected system:

```
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i download 2>nul >f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i download 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i document 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i picture 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i video 2>nul >>f1.inf
dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i music 2>nul >>f1.inf
dir "C:\Documents and Settings\" /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >f2.inf

dir C:\Users\ /s /b /a:-D 2>nul  | findstr -i desktop 2>nul >>f2.inf
dir C:\Windows\System32\Drivers /s /b /a:-D 2>nul >>f2.inf
dir C:\Windows\System32\Config /s /b /a:-D 2>nul | findstr -v -i systemprofile 2>nul >>f2.in
dir f1.inf /s /b 2>nul >>f1.inf
dir f2.inf /s /b 2>nul >>f1.inf
```

Inside resource 112, another resource (101) exists which contains a signed disk driver:



The disk driver itself does not appear to be malicious. However, it is used for raw disk access by the malware components to wipe the MBR of infected systems.

Interestingly, the driver is signed by EldoS Corporation, a company that has a mission to *?Help people feel confident about integrity and security of valuable information,* according to their website.

Also:

EldoS Corporation is an international company specializing in development of security-related software components for corporate market and individual software developers.

Of course, one big question emerges: ?Is this the malware known as Wiper, that attacked Iran in April 2012?

Our opinion, 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.

It is more likely that this is a copycat, the work of a script kiddies inspired by the story. Nowadays, destructive malware is rare; the main focus of cybercriminals is financial profit. Cases like the one here do not appear very often.

We detect the 32 bit components of the malware as Trojan.Win32.EraseMBR.a. The 64 bit component is detected as Trojan.Win64.EraseMBR.a. We proactively detected the main dropper by heuristics as "HEUR:Trojan.Win32.Generic"

PS: We are not yet sure of the meaning of ?Shamoon. It could be a reference to the Shamoon College of Engineering http://www.sce.ac.il/eng/. Or, it could simply be the name of one of the malware authors. Shamoon is the equivalent of Simon in Arabic.

Update(17 Aug 2012): Our friends from Seculert have posted their own analysis of the Shamoon attack. They suggest it is a two stage attack, with lateral movement.

Update(17 Aug 2012): During the past 24 hours, we have collected telemetry from our users on Trojan.Win32.EraseMBR.a sightings. So far, there are only two reports, both from China, which appear to be security researchers. So we can conclude that the malware is not widespread and it was probably only used in very focused targeted attacks.