SASFIS

trendmicro.com/vinfo/us/threat-encyclopedia/malware/sasfis

Analysis by: Dianne Lagrimas

- Threat Type: Trojan
- Destructiveness: No
- Encrypted:
- In the wild: Yes

OVERVIEW

Infection Channel: Spammed via email, Downloaded from the Internet

Malware belonging to the SASFIS family are known to be downloaded on systems while visiting sites that have been compromised using a particular exploit pack known as "Eleonore". SASFIS variants are also being sent via spammed messages such as the spoofed messages that purported to come from *Facebook* and *iTunes Store*. The said email messages have a .ZIP file attachment that contained TROJ_SASFIS.HN.

It is also known to be associated with FAKEAV variants that are downloaded onto systems when visiting pornographic sites. Though viewed as a simple downloader, SASFIS opens affected systems to botnet attacks, particularly ZeuS and BREDOLAB.

SASFIS have been spotted as early as 2009. Affected systems that may play part in botnet operations, are susceptible to data theft, and are difficult to clean up.

Cybercriminals behind the SASFIS malware use pay-per-install (PPI) and pay-per-access (PPA) business models to earn money.

- PPI business model: Cybercriminals behind other malware families like ZeuS and BREDOLAB pay SASFIS creators for other malware to be downloaded and installed on systems that have been infected with SASFIS.

- PPA business model: SASFIS creators list a number of adult websites in the code of the components downloaded by SASFIS variants. When a SASFIS-infected system accesses any of these websites, it redirects to any of the listed adult websites.

TECHNICAL DETAILS

Installation

This Trojan drops the following files:

%User Profile%\Local Settings\{random file name}.exe

(Note: *%User Profile%* is the current user's profile folder, which is usually C:\Windows\Profiles\{user name} on Windows 98 and ME, C:\WINNT\Profiles\{user name} on Windows NT, and C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003.)

Other System Modifications

This Trojan modifies the following registry entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\Winlogon
Shell = "Explorer.exe rundll32.exe {4 random letters}.{3 random letters} {6 random letters]}"

(Note: The default value data of the said registry entry is *Explorer.exe*.)

It also creates the following registry entry(ies) as part of its installation routine:

HKEY_CURRENT_USER\Software\Microsoft\
Office\11.0\Word\
Security
Level = "4"

HKEY_CURRENT_USER\Software\Microsoft\
Office\11.0\Word\
Security
AccessVBOM = "0"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
SCardSvr = "%User Profile%\Local Settings\{random file name}.exe"

Other Details

This Trojan connects to the following possibly malicious URL:

- http://www.google.com/{BLOCKED}mapandtet
- http://{BLOCKED}.{BLOCKED}.69.202:443/{5 random letters}.php?id={alphanumeric ID}
- http://{BLOCKED}.{BLOCKED}.138.100:80/{5 random letters}.php?id={alphanumeric ID}

Variant Information

This Trojan has the following MD5 hashes:

- 0280c89e03f255141a7d6fc400cfd51e
- 4b0eb6b90c8dbeeaf5a870b7cdf77d00
- ccf8b4c5d8fbcf4f16277f871ecf4197
- eae86cc58b8ef8ad98b7db4dcf01102f