Endpoint Protection

symantec.com/connect/blogs/sykipot-attacks

Dec 08, 2011 02:16 PM

Migration User

Thanks to Stephen Doherty, Andrea Lelli, Nicolas Falliere, Paul Mangan, Asuka Yamamoto, and Sean Kiernan for their technical contributions.

Recently, we posted two blogs about attacks leveraging the latest Adobe vulnerability. These attacks are part of a long-running series of attacks using the Sykipot family of malware. Sykipot has been used in targeted attacks for at least the past couple of years, and unconfirmed traces date back to as early as 2006. The latest wave spiked on December 1, 2011 with a huge uptick of targeted entities being sent a PDF containing a zero-day exploit against Adobe Reader and Acrobat (CVE-2011-2462).

Symantec classifies the set of Trojans used by these attackers as ‘Sykipot’ and includes detection names such as JS.Sykipot and Backdoor.Sykipot.

The goal of the attackers is to collect intellectual property and send it to a remote server of their choosing. Depending on the targeted organization the data could be design, financial, manufacturing, or strategic planning information. The attackers involved in Sykipot have a history of attacking various industries, a majority of which belong to the defense industry.

This isn’t the first time the attackers have used a zero-day exploit either. In March 2010 the Sykipot attackers leveraged a flaw in Internet Explorer—the Microsoft Internet Explorer 'iepeers.dll' Remote Code Execution Vulnerability (BID 38615).

These attacks have been long running, persistent, and targeted, leading us to believe that the attackers are well-funded and motivated to acquire specific, high-value information.

The companies attacked by this latest wave of Sykipot include, but aren’t limited to, organizations in the following market sectors, primarily based in the US or UK:

- Defense contractors
- Telecommunications
- Computer Hardware
- Chemical

- Energy
- Government Departments

The attackers consistently use targeted emails containing either a link or malicious attachment. In both cases, the attackers either exploit unpatched application flaws (zero-day exploits) or simply leverage known exploit code in the hopes that the targeted computer is running vulnerable software. One can see an example of such an email from earlier this month below.

The attackers spent a substantial amount of time researching information on the people they intended to target. Intended recipients of malicious emails exploiting the Adobe Acrobat and Reader vulnerability were mostly high-ranking executives, including C-Level, Vice-Presidents, and Directors within the organizations. These employees may have access to sensitive information and computers containing intellectual property of interest to the attackers. Furthermore, these employee's computers, and the information gathered from them, may be used to mount attacks on lower-level employees and the computers that hold the desired information.

The attackers always used enticing file names for the Trojan, such as '[REMOVED]-weapons.scr', '[REMOVED]_af_navy.scr', and 'occupy-wall-street-[NUMBER].scr'.

Once a computer was compromised, we have observed the attackers initially issue reconnaissance commands to gather system and network information to determine if the computer was a host of interest to them. If so, the attackers would issue custom commands specific to the compromised environment in order to locate and exfiltrate desired information.

Threat Details

In the recent attack, when the malicious PDF is opened, Sykipot is executed and the user is shown a copy of a clean PDF file before Skyipot is injected into the following processes:

- iexplore.exe
- outlook.exe
- firefox.exe

The Trojan is also copied to a local folder as a file named 'pretty.exe' with a compile date of November 22, 2011.

The Trojan DLL has a few supporting files which are copied into the local settings folder. The file names and their functions are as follows:

File name	Function

Gtpretty.tmp	Orders from the C&C
Gdtpretty.tmp	Decrypted version of orders from the C&C
Pdtpretty.tmp	Logfile
Ptpretty.tmp	Encrypted version of logfile

This particular variant contacts the command and control server, www [dot] prettylikeher [dot] com, via HTTPS. In addition, another underlying encryption scheme is used that uses the key 19990817 (this appears to be the date August 17, 1999).

The command and control server is configured to automatically send commands to instruct Sykipot to send system and network information before attackers can issue custom commands in order to locate and exfiltrate sensitive information.

Previous attacks performed similar actions, as can be seen here.

Sykipot will continually ping the command and control server using the following GET requests:

```
https://[C&C DOMAIN]/asp/kys_allow_get.asp?name=getkys.kys&hostname=
[COMPUTER NAME]-[IP ADDRESS]-pretty20111122
```

It also uses a hardcoded referer of 'www.yahoo.com' when making these HTTP requests.

Sykipot supports the following commands:

Command	Function
cmd	Execute command using CreateProcess and log results in configured log file
door	This command supports five subcommands explained below
time	Configure delay timer for C&C querying
getfile	Download a file
putfile	Upload a file

The 'door' command allows five subcommands, such as the following:

Sub-Commands for 'door'	Function
shell	Do nothing
run	Executes a command using WinExec

reboot	Restarts the computer
kill	Ends a process
process	Not implemented

In addition to all of these commands, the Sykipot Trojan accepts an '-uninstall' command-line switch that allows for it to be uninstalled. Doing so also ends the processes that were injected by the malware.

The Sykipot samples analyzed also contain Chinese language error message strings that appear to correspond to a tool used to package the threat.

The English translation is:

> Binding document,
> Read the first file to bind error! Binding document,
> To bind file to read the second error! Binding document,
> Open the file you want to bind the second error! Binding document,
> Open the first file to bind error! Binding document,
> Create a binding file generated after synthesis Error! Binding document,
> Error cannot locate the file itself! Binding document,
> Cannot read the contents of their file error! Binding document,
> Error opening the file itself! Binding document,
> Error distribution of the length of the file itself! Binding document,
> Its zero-length file error! Error

Some known Sykipot domains are as follows:

In addition to the aforementioned domains, we have data that leads us to believe the following sites are also a part of this long-running campaign:

Attacker Profile

Attributing the attack to a particular entity is generally difficult; however, long term campaigns such as this one provide enough traits to give a rudimentary profile of the attackers.

While the back door Trojan itself isn't very sophisticated or well-coded, the attackers are skilled enough to have discovered multiple zero-day vulnerabilities. Given the long list of command and control servers being used for controlling the botnet, the attackers are unlikely to be a single person, but rather a group of people.

Thus, the Sykipot attackers are likely to be an organized and skilled group of individuals. Given their persistence and their long-running campaigns, the attackers are likely to have consistent funding for their efforts.

Summary

The goal of Sykipot attackers is to obtain sensitive documents to high level executives within a variety of target organizations, of which the vast majority have been defense related. Considering the long-running campaign history of the attackers and their previous use of zero-day exploits, future versions of Sykipot that are delivered using another zero day are likely.

Symantec products detect Sykipot Trojan files as Backdoor.Sykipot, Files attempting to exploit the Adobe Acrobat and Reader U3D Memory Corruption Vulnerability (BID 50922) are detected as Bloodhound.Exploit.439 and malicious PDFs trying to create and execute files are detected using SONAR proactively.