Sykipot is back

July 2, 2012 | Jaime Blasco

It has been a while since we published information about Sykipot. The last time we blogged about it, we discovered a variant that was able to bypass two-factor authentication to access protected resources on the victim's network.

We have detected a new wave of Sykipot campaigns that has been running during the past weeks. There are several changes between the new Sykipot campaigns and the older ones.

The first difference is that in previous campaigns the Sykipot authors mainly used file-format exploits to gain access to the systems through spearphishing mails. This is the list of file-format exploits used in the past:

CVE	Date	Product
CVE-2007-0671	2007-02-02	Microsoft Excel
CVE-2009-3957	2010-12-01	Adobe Reader
CVE-2010-0806	2010-05-04	Internet Explorer
CVE-2010-2883	2010-09-08	Adobe Reader
CVE-2010-3654	2010-10-28	Adobe Flash Player
CVE-2011-2462	2011-12-06	Adobe Reader

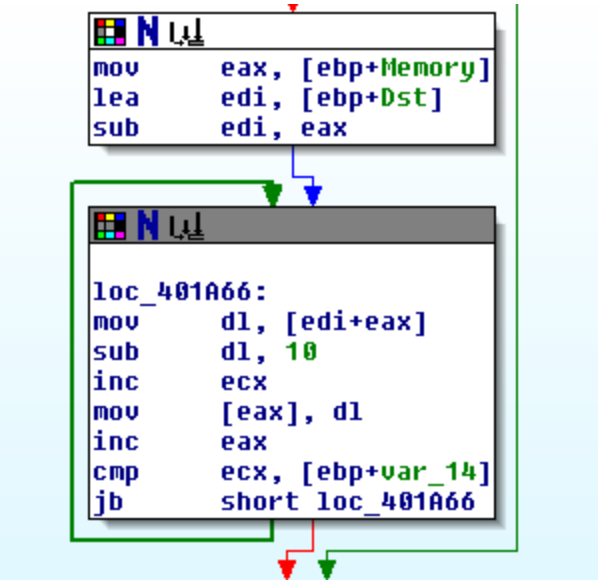
This time it seems they are mainly using drive-by-download exploits like CVE-2011-0611 affecting Flash Player or the new Windows XML Core zero-day vulnerability.

The CVE-2012-1889 vulnerability is related to Google's warnings on state-sponsored attacks.

Instead of attaching malicious files on e-mails, they send e-mails to the victims with a malicious link. Once the victim clicks on the link the malicious server tries to exploit a vulnerability on the user's browser.

The modus operandi of the group behind these attacks seems to be the same as in the past. The attackers hack US based servers and then install software to serve the malicious content or to redirect the connections to a remote server.

The malware continues using SSL to communicate with the C&C server. Once executed, the malware tries to get a configuration file from a remote server. On the older versions they used an underlying encryption using the XOR key “19990817” for the config files. The XOR obfuscation has been removed and in the new versions a simple byte subtraction routine is used.



The configuration file is requested from a remote server using the following URL format:

GET /get.asp?nm=index.dat&hnm=[HOSTNAME]-[IP-ADDRESS]-[IDENTIFIER] (SSL based)

They continue to use the hardcoded referer of ‘www.yahoo.com’ on the requests.

The new configuration format supports several commands and most of the previous names have changed. This is the list of supported instructions:

- porth - List of active connections (netstat-like)

- processh - List of processes running on the system

- tasklisth - List of processess (tasklist.exe-like)

- serviceslisth - List of running services and their status (running/stopped)

- starth - Starts a service

- stoph - Stops a service

- delh - Deletes a file

- gh - Gets a file from the C&C server

- ph - Uploads a file to the C&C server

- dir/h - Lists a directory/file

- dir/sh - Lists a directory/file

- runh -

- EXITH - Deletes the malware from the system

- info - Executes a command (Winexec)

- without param - Gets network info and startup time

- sleeph - Sleeps a number of seconds

Once the malware downloads the config file it executes every instructions, it saves the result and obfuscates the data using the subtraction routine. Finally it sends the result to the C&C server.

Some of the known Sykipot domains that are being used to serve malicious content or as C&C domains are:

- newcarstyle.com

- nhrasurvey.org

- quicksurveypro.com

- contractspt.com

- betterslife.com

- aeroconf13.org

- e-landusa.net

- photosmagnum.com

- reythy.com

Most of the domains have been registered during the last month and they have used the mail address jimgreen200088 [at] yahoo.com to register most of them.

The Netbox webserver used in previous campaigns is also present in most of the C&C servers .

Note the domain aeroconf13.org seems to be related with a spearphishing campaign against potential attendees of the IEEE Aerospace Conference (the International Conference for Aerospace Experts, Academics, Military Personnel, and Industry Leaders).

We will continue to offer more information on these new campaigns as long as we find more details. Stay tune for more information and apply your patches!

Share this with others

Tags: sykipot, ieee aerospace conference, cve-2012-1889