# **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

(<u>https://www.welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs</u>), 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:

80405750	FERS CREWFIFE	10.00	54965 PTK 551189F-4363		
10112-331	15.20		185 E		
2010-110	ALL DODE ATMR	510	PAPER, BOURDEDC	UFOCTOR.	*C0.07*
80405175	FEBS CREEFFFF	100	2V0F2 FTN 11-180F-4000		
20103-027	怒跌		105 mm		
2026-021	32.26		AND TATAL MANY ALL		
80-607-080	CTUE HATBETTY D	ROU I	MOND PTA IN COMP-MC1.		
00000000	IN BUILDING COMPANY	10.00	2V0K2 FTR 201100F-4000		
2020103	10.00	<b>Printing</b>	102		
10109-0126	23 E4064308	10.0	maran. 80430684	INCOME.	"Gourst"
80407122	FFEC CONSPREY	POINT OF	2V0F2 PTN 012188P-43803		
100000000	22.03		The new		
1010-037	52°3a		4007 ELECTIN, 80407555		
80-40#120	CTUS DATEFTY 0				
000000000000000000000000000000000000000	TABLE CONTRACTOR	211	SADES ALL STREET, STRE		
20202023	60°	1000	100		
80407041	65 //8064388	100	maraa, 80430670	INCOME.	"Govinge"
B0407-046	TTEL CAPTURET	100	2MDP2 FTR CG/TERP-4300		
20403-042	8500		EPHT, DOT		
80400050	26.00	đ.	(8)7 (1) (1) (0) (0) (0) (0) (0) (0) (0) (0) (0) (0		
B0407052	CTUS OF WALL O		MONO POR SELECTION		
004071052	FF BS CAP AFTER	-	ERIT		
10405365	W	811)H	DHI		
20102025	60 PT0064000	100	TICLE, BOADDATC	PROCESSE	"Oc 1945"
804071270	PPD6	-	Second File Sociation - Capital		
ET THE YEAR	No. C.		Dett. Dett		
10006334	THE ADDRESS A	÷.,	AND DICKS AND DISCOUNTS AND		
10100-0005	PPER OBSERVER	PLICE	SMORE FIR DIS TROP-41003		
00405036	10,211		5011		
2003-000	25 orreunee	50	THEFT BOARD	0400000	Wassess also P
2020-016	PERS CAPTURE	10.0	SMORD FTN SS-TESP-4560		CONTRACTOR D
80407054	PP 24		B12		
100000	No. of the second se		Della Della Distancia della de		
8040r084	CTUS ABUTUTT 0	10.0	3000 PM 551000-4581		
80405384	PPES CAREFUT	100	SMORD FTN 65-TERP-4565		
10000	100	Post line	501 507		
20403.060	60 28074988	100	01010.00400700		*11o8/e/#
80405082	MAR OBJECT	100	Swong PTN 55-185P-4560		
00407180	#112.0		DAT DAT		
10102185	24.08	. E	4007 04244,0040F9C9		
20102-095	CHE SCREETE O				
10000	PPES OF FITT	1000	Balling Film Sociation - Cock		
004051000	10	10.00			
20405-003	10.19025000	100	ELLIS, BOAREPOR	INCOME.	"ESET HODIZ"
2020-022	NEW CONTRACTOR	-	ALL AND A		
004071000	8120		D/d, D/d		
2012/03/2	the owners of		CONTRACTOR AND AND AND AND A		
2020-015	WE SHEWY	Provide	Souther with the Time Alasy		
advader/JPD	1123		Dell		
and a starting the	100 x 100 x 100 x	100	DPE POLICE	She have been as a second	Reference and R
10000	Marc Gardeter	3.2	Sound FTE Son [ DOP-4300]	OT A DUE	1.004.000
actual test	17.26		651		
80407142	BALO D		End , End		
10000	COS SCREETE 6		and the second se		
10-01-5-5	MEC Gerbrinn	Provide and			
and the second	17.80		100		
BOMON INC.	NO 50074080	1	11/14 . 004 (CTN)	UPICCODE	"Bitteriesder"
10105756	FERS OR BEFFF	200	\$4949 FTR \$40180F-4000		
and the second second	FT 100				

#### 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.

100 cml, mess, 08400720	http://www.woftwaredevel.com/Mindowsi.ival/riter/web-2_8_thank_1.gif
NETO BILL AC	
TEN CHORE FTR SELECEP-EVEL. DEFEN. BOHECE	http://www.oduree.at/goog/theida/pictures/Taupendepthika_ppg
THE CHORE FIR SSICLEP-EVED STREET, BALLON	http://opaguleakdetias.com/blag/inaget/thate/state/cod/
HEAD CHARGE FITTE OS I CORP. DOM SUBJECT ON MON HEAD	http://crapileafdesiae.cov/5105/inades/thate/facebook.p/g
HERE GRADER FITE SALL CERF-SHE STREET	
NOT CHORE FIRE SECTION-EACLERS	
100 0M0H2 FTK SELECT-SEEL	bit tax //general account accordance by Tyracatar_ bit (Tation Provident Content of Content
THE OWNER FIR SELECTION CONTACT AND A	18 Text Area wat as converted at the Unit Present and Text Period Party (PEPOP) Ladobox ed 400 Text.
NEW CHORE FIRE SELECTION - SOUTH CHERTER, BOARCE	http://vfolaths.com/wp-content/vploads/2018/49/web-20-whit-is-2006/251.jpg
HEA GAORE FITE GENELED STUDENTS (BOADER	http://pafi.com/inariona/teitter.org
HED ONORS FITE SECTORE-STRUCTURES BOANCE	http://psfk.com/Lna/Loans/Facabook.psg
NEW CARRY FIRE SEALCHER-STATUSERERS, BOANCE	https://beaittpji/feroex.com/semplates/2008/inapes/beader_lope.jpp
TEN ONORS FITS SELECTION STREAM PLATE BOH SCH	bit tax //beatting Lifenoia, son/seeg Lates //DPV Leages/beades_Logic_Seg
THE OWNER FILE THE CARE-BEET COMPLEX.	http://hellandaddettl.cov/pages/toster/account.lpg
THE OWNER FOR SECOND - SEE SECOND - SEC	http://whollawdowdpett.com//wwdee/fogteg/gopownt/du/
HEAD CONTRACT FILE CONTRACTOR SCALE STREET BOARD	55104-009-85108-968108-160521-0-2004-01988819-5521211008
THE CHARGE FITS AN ADDRESS AND ADDRESS BOARD	http://watios.satios.ion/inductor/inductor/2012/12/12/22/208
	In the course provide the provide set of the
THE OWNER FILE TO CLERE STRATEGIES AND AND	ESTER / You Linet Lind Lines Lange , party Langes / Your etc. dellanaero, git
THE OWNER AND ADDRESS OF A DEPARTMENT OF A DEP	P.5 T24 / / 1015201020000001 915 / 21/08 / 21/08 / 21/08 / 22/08
	PK101/V101/02/10488/081/945/0108/2108/2202.208
the second s	2/2/10/2/2/2/40/40/41/4/81/81/81/2/4/#0/0/2/10/2/81/4/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/
the second s	PATER // Second Segreen Search Line, Story asset 1/ Pagers, green 18, and and 1
THE OWNER FIRE THE TRANSPORT OF A DESCRIPTION OF BUILDING	https://greed.srkalteantine.com/inages/greed.srkalteapir Doldingoas200-pit
	https://greenteiteatteatteant.ine.gov/inaget/greenteiteatteagt/ hotdingosaitet.git
AND REAL PROPERTY OF THE PROPERTY OF THE REAL PROPE	TK TDL - YOB   ING UNIT   TH TG, COM-TB, YINBORT / LODO, LOD
	PATER AND INTERNET INTERACTION AND INTERACT AND A DRIVEN AND A
	CONTRACTOR AND A DESCRIPTION OF A DESCRI
and the second sec	
	THE TARK A TOOL IN THE REPORT OF A DAMAGE AND A

### Figure 4

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



#### 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.

Renote P	n	Out	Direction	Sessions	Ports	Histnane	Bytes	Process
72.233.44.59	đ	7	Out	1	http	gnavabar.com	4 227	dver.exe
<b>1</b> 72.233. <b>44</b> .61	7	6	340	1	http	gravatar.com	1 464	conhost.eve
67.205.43.104	4	5	Out	1	http	ps4540.dreamhost.com	1 510	C0788.608
12.238.253.103	12	12	Out:	2	http	vwb.hollandandbavett.com	5 575	dvm.exe
4,125,39,147	45	38	Out	6	http	Ex-in-F147. be100unet	33 830	conhost.exe
74.125.39.99	28	10	Out	2	http	fx-in-P99.3e100.net	20.364	conhost.eox
88.25.132.128	13	15	Out	3	http	bravo669.startdedicated.com	3 241	conhost.exe
7 50.20.3.141	13	15	Out	3	http	host onlineinstitute.com	5 364	C8765.#X08
108.86.208 209.188.86	8	10	340	2	http	host.orazyleafdesign.com	3 381	conhost.eve
97.79.238.39	16	20	Out	4	http	gvo23839.gvodatacenter.com	5415	CIPEL-EXE
67.222.95.148	14	. 9	Out:	1	http	95-143.bluehost.com	15 872	dvm.exe
4,125,39,105	24	30	Out	6	http	Ex-in-F105. Le100uret	8 055	conhost.exe
<b>1</b> 74.125.39.106	36	29	Out:	+	http	fx-in-f106.te100unet	31,095	conhost.eve
173.203.101.8	4	5	Out	1	http	173-203-101-8.static.doud4	1.768	conhost.exe
68.170.232.100	5	5	Out	1	http	parkvebvin-vill.prod.mesa1	1.068	dven.exe
And a state when the state					been -	and the same and a subset of the	1.0004	and the second

#### Figure 6

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

14 Jul 2011 - 11:07AM

# Sign up to receive an email update whenever a new article is published in our <u>Ukraine Crisis – Digital Security Resource Center</u>

Newsletter

Discussion