A Look At Recent Tinba Banking Trojan Variant

zscaler.com/blogs/research/look-recent-tinba-banking-trojan-variant



Introduction

Tinba is information stealing Trojan. The main purpose of the malware is to steal information that could be browsing data, login credentials, or even banking information. This is achieved through code injection into system process (Winver.exe and Explorer.exe) and installing hooks into various browsers like IExplorer, Chrome, Firefox and Opera.

Tinba has been known to arrive via spammed e-mail attachments and drive-by downloads. Recently, Angler Exploit Kit instances were also found to be serving Tinba banking Trojan.

Detailed Analysis of Tinba

Tinba is packed with a custom packer and uses well known anti-debugging technique using the WinAPI function "IsDebuggerPresent" to hinder reverse engineering of the binary image. The execution flow of the infection cycle for Tinba is shown below.



Execution flow of Tinba

The image below shows the custom packer code being used by the Tinba sample we were looking at.

Cityles - # 2514145ex1641e31403e316e7e32ea2018852Haar644Da	conduction - (CPU - main charait, module c0254644)	
The Test Delay Player Option Window 140		
Subscription Control Subscription	Decryption routine	Burgletary (199) C. 1 01
And the second s	Calling of the - 4000100 Falebane - 8011	515 e-gij 1,00000000000000000 517 e-gij 1,000000000000000000000000000000000000
Amp in Lann. Andren D-4 1/5 Amer. Andren D		212 Adda Cond 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Alteration A main A	

Tinba unpacking Routine

The unpacked binary image is shown below which upon execution will perform code injection into system processes like Winver.exe and Explorer.exe.

Address	Hes	du	mp														RSCII	
0040000	40	56	98	0.0	03	68	68	68	0%	08	00	00	FF	FF	08	98	128.8	
80488618	88	68	68		00	00	88	98	ALC:	60	88	88	88	88	00	00		
00400020					00	00	60	02	08	08	00			00		00		
80488838					0.0	08	68	66	66	08			80		80	88		
00100010	86	1F	BN	ØE.	68	81	89	CD	21	88	815	AC.	CD	21	54	6.8	BERE, ', It BLITTH	
00100050	69	72	28	78	72	6F	67	72	61	60	28	62	61	65	65	65	is program canno	
00400050	78	28	62	65	28	72	75	6E	28	6.9	6E	28	44	45	53	28	t be run in DOS	
00400070	60	ő۴	64	65	2E	80	80	6A	24	08	00	00			88	68	mode\$	
0240030	54	45	83	88	4C	01	81	68	46	16	6A				88	88	PEL	
82488898	88	818			EB	00	287	01	18	81	81	46			00	88		
80480010		88	00		68	00	00	68	68	10	88	88		18	00	88		Decounted Bloom Impre
60469669	88	88	00		00	99	40	69	08	18	88	88	88	82	00	88		man Abrea augus A musica
0010000	81	68		88	00	66	99	68	65	88	88	66		88		80	BB	
0040000	88	42	88	88	88	82	69	60	63	50	61	88	82	88	88	88	.8Ec\E.E	
02400050		18	88	88	88	18	88	88	68	68	61				80	88		
584596F 8	88	88	68	88	18	68	88	66	88	68	88	66	88	88	88	88	· · · · B · · · · · · · · · · · · · · ·	
00100100		68	68	88	88	99	69	65	88	68	66	66	88	88	88	88		
00400110			68	88	00	98	99	65	88	08	00	66	00	88	80	00		
88488128		88	88	88	00	00	09	06	00	00	00	88	00			00		
88488138				88	0.9	88	80	0.5	08	00	8				80	80		
80480140				00	00	00	08	66	08	08	00	88			8	80		
00400150		68	00		00	60	09	06	08	88	68	00	88	88	0.0	00		
00400160		68	68		00	69	00	99	00	88	88	60	88		00	00		
66466176		88	68	88	66	99	66	66		66	6C	61	74		00	99	Flat	
00400100		32	88	88	66	18	98	66	66	32	88	88	66	82	99	89	.2	
88488179			88	88	08	95	98	66	88	08	00	88	28	80	88	68	`	
88488168			88	88	96	.09	98	88	98	08	00	88	88	88	88	88		
89489189	14	88	88	88	98	96	99	0ê	00	08	88	00	88	88	88	99	* * * * * * * * * * * * * * * * * *	
8646610.6	88	88	88	88	88	08	99	99	08	08	00	88	88	88	88	88		
86488108				88	00	00	99	09	00	00	08	88		00	80	80		
<				-	-			-				-	-			-		

Unpacked Binary

It generates Mutex name using root volume information of the victim's machine as shown below.

01623596 8870 0C 01623596 83C7 07	ADD EDI.7	
01A235A0 8845 88	HOU EAX, DWORD PTR SS:[ERP+8]	
01823583 83E0 0P 01823586 3C 08	CHP AL.00	
01A235A8 _ 73 84	JNE SHORT @1A235AE	
01A235AA 04 38	ADD AL,38	
01823586 EB 02 01823586 Bb 37	ADD 81-37	generation of name
01A235B0 AA	STOS BYTE PTR ES:[EDI]	
01A235B1 C14D 08 84	ROR DWORD PTR SS:[EBP+8],4	
01623585 3870 0C 01623588 * 73 56	CHP EDI, DWOHD PTH SS: EBP+C	
01A2358A FC	CLD	
01623588 SF	POP EDI	00F94808
016235BC C9	LEAVE	
01623500 55	PUSE EBP	
01023501 8965	HOU EBP,ESP	
Stack SS:[0125FFF4]=00F94 EAX=0000001B	840	
Address Hex dump	ASCII	
B1A2322B 37 32 36 31 46 3	3 42 31 00 43 30 5C 44 6F 63 75 7261F3B1.	C:\Decu
0192323B 60 65 6E 74 73 2	0 61 66 64 20 53 65 74 74 69 66 Midts and	Settin Deskto
01623248 67 73 5C 73 72 6 01623258 70 5C 64 21 37 3	5 34 64 34 64 35 61 65 65 62 38 0\d1754da	d5aeeb8
01023268 34 31 63 62 33 3	h 3h 33 32 61 31 3h 33 6h 61 66 h1cb3hb32	a1h3daF

Mutex name generation

Remote Thread in System Process

A remote thread is created inside Explorer process that is responsible for creating a copy of Tinba Binary in %APPDATA% & auto start registry entry in Registry hive.

Running	₩X ► 11 5	HHHHH H H LEMIWHCZI	K B R S III II'?
89969883	3108	XOR EAX,EAX	
89968885	48	THC EAX	
00960886	98	NDP	
89968887	- 75 1B	JN2 SHORT 00960864	
00960889	48	DEC EAS	
8996688A	83EC 08	208 E25 18	
66692 9668D	20 51020000	CALL 08951613	
89968892	LB 50150000	ALL DOVE TOLY	Remote Thread function
000500077	40	455 C10 4	
8995 8998	40	AFC FAX	
00060890	3109	XOR FCX.FCX	
89958895	FF15 E&E7FFFF	COLL DWORD PTR DS:[FFFFF7E0]	
009606945	E8 88888888	CALL 0295-2989	
89968889	58	POP EXX	atd11.70912078
899688AA	81E8 C0184000	SUB_EBX, AB18CD	
00960880	E8 08030000	GALL 02252C80	
00960885	E8 AE080000	GALL 02951458	
00960888	E8 84FDFFFF	GALL 08958633	
8689 668 E	3100	XOR EAX,EAX	
899686C1	50	PUSH FAX	
8976-88C2	50	PUSH LAX	
899698C3	50	LEA FAN ANDER ATE DE FEAN LASATES	
0000 0000 0	6093 73364888	CER EDW, DAORD FIR DSI[EBX+483873]	abdll KifnabfuctorfallDat
eevolesca	26	CUSA EUX	acon and as cause meaning

Explorer remote thread

The Tinba binary is stored in a hidden folder which is created under %APPDATA% directory:

C:\Documents and setting \username \Application Data\mutexname\bin.exe

It also creates an auto-run registry entry to execute Tinba binary during every windows start-up as shown below:



Auto start registry entry

Another thread is also created in Explorer process which is responsible for generating DGA (Domain Generation Algorithm) domains and injecting code into browsers like IExplorer, Chrome, Firefox and Opera.

Since 1 Since 1 Pick	Pased 9		14 NH 4 - N	HTWHCZEB					
BRIGGENES 5.8 Particle 16.4	00042054 00042054 00042052 00042052 00042052 00042052 00042052 00042052	55 8915 8116 8009000 58 8118 85364000 58 8045 80181777 8045 80181777 878425	HER COP. CSP HER COP., CSP STRE CSP, VAR STRE CSP, VAR HER CSR, VAR STRE CSR, VAR HER CSR, VAR	er (196513)	94.800		* 1980	Anters (Anters) Anters	
BIOLINI BIOLINI <t< td=""><td>0886/29437 0886/29437 0886/29437 0886/29437 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947</td><td>50 88955 88751777 834635 46 85 90 97 97 97 97 97 97 97 97 97 97 97 97 97</td><td>Pass inter (C.C. Care (June)) Seen Deals Fis (S.C.) Seen Deals Fis (S.C.) Seen Constant Seen Constant See</td><td>100-0000 (100-0000/17)</td><td>Anna la Ipalay na bian Anna conund Anna conund Parist conund</td><td></td><td></td><td>ES 00 ES 00 ES 00 ES 00 ES 00 ES 00 ES 00 EAUED 00000 00000 00000 00000 0000 0000 00</td><td>keynhil keynhil 32512 32</td></t<>	0886/29437 0886/29437 0886/29437 0886/29437 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947 0886/2947	50 88955 88751777 834635 46 85 90 97 97 97 97 97 97 97 97 97 97 97 97 97	Pass inter (C.C. Care (June)) Seen Deals Fis (S.C.) Seen Deals Fis (S.C.) Seen Constant Seen Constant See	100-0000 (100-0000/17)	Anna la Ipalay na bian Anna conund Anna conund Parist conund			ES 00 ES 00 ES 00 ES 00 ES 00 ES 00 ES 00 EAUED 00000 00000 00000 00000 0000 0000 00	keynhil keynhil 32512 32
and the second s		8285 885CIFF HC Res down C All 98 35 97 4 11 88 27 88 35 97 4 12 88 27 88 35 97 4 13 88 27 88 35 97 4 14 88 27 88 35 97 4 15 57 88 61 44 4	4 4 4 4 22 0 20 10 20 10 10 10 10 10 10 10 10 10 10 10 10 10	45(11 00 00 FB 10010-0170 00 50 70 1000-0170 00 50 47 8 1000-0170 01 50 75 7000-0170	ta, ta esta			8125 0 8915 8	142 8448 894 2016 816 8803

Explorer local thread

Domain Generation Algorithm

The following is the Domain Generation Algorithm (DGA) used by Tinba variant where every sample uses a hardcoded domain and seed to generate the DGA domains.



Address	160	(di	inp														ASC11	
80965718	FF	85	C®	74	56	80	78	13	88	45	CC 0	0:3	45	10	29	F8	ümitvexeme.mem)ø	
88965728	64	82	E8	62	88	88	88	60	98	58		E8	CB	DF	FF	FF	3020PWE033	
00965738	89	C1	68	68	50	81		88	FF	FF	FF	87	84	24	58	80	ñójaran jijijansén	
00965748	85	66	FF	FF	FF	87	84	29	64	66		88	88	88	99	65	8.00088\$j858V	
88965758	8.9	89	<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	88	45	88	85	E8	58	DE	FF	FF	57	EB	6A	₿E	120 ¥ µêxbijijilê jb	
88965768	FF	F F	83	¢7	88	29	F9	88	28	F3	ÂŔ	61	E8	89	69	88	ijjitçi)à" étab	
00965778	88	58		95	67	48	60	FF		18	FF	75	ec.	FF		88	.X-BoB.üuBüu.üuB	hardcoded domain
00965798	FF	98		hС	48	88	83	CA.	0¢	C9	63	98	66	61	đΕ	79	GEELO.EX.CXEFacy	
88965798	64	6F	άF	63	68	26	72	75	66	66	68	88	88	60	98	88	leeck.ru	
00965780	08	90	60	66	88	80	88	88	80	86	8	58	2F	66	61	38	P/Fa@	appended uri patten
00965780	38	38	đΕ	69	69	69	đΕ	38	28	36	đΕ	64	2F	80	69	88	SEniiin888md/	
88965768	00	80	60	68	80	88	00	69	60	80	88	08	68	32	ħά	76	jSFv	DGA seed
00965708	28	34	49	62	45	88	68	38	49	¢Ε	63	64	46	41	ι¥Ε	Ap by	p91bE3h81acjF#N0	
009657E0	80	90	60	88	63	6F	60	88	88	90		81	0C	80	E8	E 3		
009657F0	80	80	80	88	F7	91	88	E1		82	ΛC	Fő	89	58	88	80	■+*x-5ç1-302P ■	
80965808	58	48	9B	8C	36	98	EЦ	26	88	ЗŔ		28	85	82	41	5C	[X00.CBG68:0-58A\	
00965810	7E	50	F1	77	ec.		70	65	DB	F6	93	82	39	68		F3	"Pilu-#)#08##9`\$6	
00965820	94	782	BE	54	83	Fill	E.8	73	24	32	45	#F	70	E3	ЗŔ	8E	DOGTBORSB2E på:0	
88645838	191	10	100	80	100	1.0	75	10	1993	45	20	1.00	1.1	30	5.0	10	18888 188-of '30181	

Hardcoded Domain and seed

These DGA domains are fast flux domains where single domain is frequently switched to different IPs by registering it as part of the DNS A record list for a single domain.

targetHost	targetIP
eudvwwwrmyqi.in	89.111.166.60
eudvwwwrmyqi.in	95.163.121.94
jrhijuuwgopx.com	176.31.62.78
jrhijuuwgopx.com	176.31.62.77
norubjjpsvfg.ru	210.1.226.15
norubjjpsvfg.ru	104.223.122.20
norubjjpsvfg.ru	104.223.15.16
scpxsbsjjqje.ru	5.178.64.90
scpxsbsjjqje.ru	192.198.90.228
scpxsbsjjqje.ru	5.178.64.90
wgwnmffclqvu.ru	192.198.90.228
wgwnmffclqvu.ru	192.3.95.140

Remote Thread in browsers The Explorer thread searches for browser process either by checking path of the browser executable or by loaded application specific DLL (e.g. NSS3.dll for firefox.exe). If the targeted browser process is found, then the secondary thread is created in the process.

###35587 4.0 ###35588 B175 08 ###35588 B140 0C ###35588 B170 10 ###35588 B170 11 ###35588 B170 11 ###35586 B170 11 ###35567 A C ###35567 A C ###35567 C 20008 ###35567 C 20008 ###35567 C 9 ###35567 C 9008 ###35567 C 9008 ###35567 C 9008 ###35567 S 1 ###3556	FUENDAD FUENDAD FIENDADA NOU ESS. DUDDED FIEN SSS [CHP+U] NOU ESS. [CHP+U] NOU ESS. DUDDED FIEN SSS [CHP+U] NOU ESS.[CHP+U] NOU ESS. DUDDED FIEN SSS [CHP+U] NOU ESS.[CHP+U] NOU ESS.[CHP+U] NOU ESS.[CHP+U] NOU ESS.[CHPE] NOU ESS.[CHPE]	kerne132.76000729 ntd11.76910050 ntd11.2vQveryDirectoryFile kerne132.76000729
Genera to 01003571 601ress. Hex damp 82007001 69 65 79 70 60 6 82007801 69 65 79 70 60 6	p F 72 65 2E 65 70 65 E1 97 7C 00 1 5 C0 40 40 40 40 40 40 40 40 40 23 5	NCII coplore.exe≨ija ∭e.bio

Browser thread

This thread is responsible to get updated Bot configuration details like Target URL list and strings (BOTUID) from a remote C&C server. If there is no updated list of target URLs from C&C server, then it uses default targeted list of URLs which is stored in the injected code. The list of default target URLs after decryption is shown below.

Address	He	c du	ınp														ASCII
04800004	68	74	74	78	73	3A	2F	2F	2A	28	50	8D	0A	21	2A	6C	https://* P!*1
04800014	6F	63	61	6C	68	6F	73	74	3A	32	36	31	34	33	2F	73	ocalhost:26143/s
04B00024	6B	79	78	65	63	74	6F	63	2F	76	31	2F	70	бE	72	2F	kypectoc/v1/pnr/
04B00034	70	61	72	73	65	2A	20	47	50	ØD	ØA	21	2A	6D	69	63	parse* GPt*nic
04800044	72	6F	73	6F	66	74	2E	2A	20	47	50	ØD	ØA	21	2A	67	rosoft.* GP!*g
04800054	6F	6F	67	6C	65	2E	28	20	47	50	0D	ØA	28	61	63	63	oogle.* GP*acc
04800064	6F	75	6E	74	73	2E	67	6F	6F	67	6C	65	2E	28	2F	53	ounts.google.*/S
04800074	65	72	76	69	63	65	40	óF	67	69	бE	41	75	74	68	2A	erviceLoginAuth*
04800084	20	50	6D	ØA	21	2A	66	61	63	65	62	őF	6F	óВ	2E	2A	Pt*facebook.*
04B 0 0 0 9 4	20	47	50	6D	ØA	2A	66	61	63	65	62	6F	6F	6B	2E	2A	GP*Facebook.*
04800004	2F	6C	6F	67	69	6E	2E	78	68	78	2A	28	50	89	88	88	/login.php* P
04800084	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Default Targeted URL list

The collected information form webmail, social media and the banking sites are stored in "log.dat" file.

00B8F99C	88	88	88	00	88	88	88	88	00	68	88	88	88	88	88	88	
00BSF9AC	25	чC	ЧF	43	41	4C	41	58	50	դդ	41	54	41	25	5C	58	\$LOCALAPPDATA\$\P
00B8F9BC	61	63	68	61	67	65	73	SC	77	69	6E	64	6F	77	73	5F	ackages\windows_
00B8F9CC	69	65	5F	61	63	5F	30	30	31	5C	41	43	5C	37	32	36	ie_ac_001\AC\726
00B8F9DC	31	46	33	42	31	5C	6C	6F	67	2E	64	61	74	88	88	88	1F3B1\log.dat
00B8F9EC	80	88	68	88	88	88	66	88	88	88	88	88	68	88	88	88	
88095050	68	88	88	88	68	88	0.0	88	68	88	88	88	88	88	88	88	

Log file path

C&C communication & Cryptography:

The POST request to C&C server contains encrypted system information like system

volume & version information. The cryptography routine is a simple byte 'XOR' with an 8 bit 'ROR' of the key after each write.

@896359C[55	PUSH EBP
0096359D	89E5	HOV EBP, ESP
0096359F	8855 08	HOV EDX, DWORD PTR SS:[EBP+8]
009635A2	8840 BC	HOU ECX, DWORD PTR SS:[EBP+C]
009635A5	8845 10	HOU EAX, DWORD PTR SS:[EBP+10]
009635A8	r3082	XOR BYTE PTR DS:[EDX],AL
009635AA	C1C8 08	ROR EAX,8
089635AD	42	INC EDX
889635AE	E2 F8	LOOPD SHORT 009635A8
00963580	69	LEAVE
88963581	C2 0C00	RETN OC

Send Data Encryption

A sample Tinba POST request to DGA domains with 157 bytes of encrypted data is shown below.



C&C POST Request

Geo distribution of C&C call back attempts that we blocked in past one month:



Geo Location

We have seen following C&C server IP addresses: Conclusion:

Tinba also known as small banking Trojan continues to be prevalent in the wild. The arrival method varies from e-mail spam, drive-by downloads and most recently Exploit Kit infection cycle. Zscaler ThreatlabZ is actively monitoring this malware family and ensuring coverage for our customers.

Stay up to date with the latest digital transformation tips and news.

By submitting the form, you are agreeing to our **privacy policy**.