

A Look At Recent Tinba Banking Trojan Variant

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



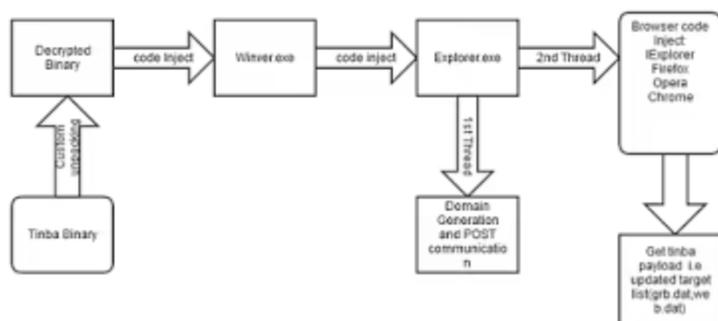
Introduction

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 IE Explorer, 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.




```

01A23598 807D 0C MOV EDI,DWORD PTR SS:[EBP+C
01A23599 80C7 07 ADD EDI,7
01A235A0 0045 00 MOV EAX,DWORD PTR SS:[EBP+8
01A235A3 03E0 0F AND EAX,0F
01A235A6 3C 0A CMP AL,0A
01A235A8 73 04 JNB SHORT 01A235A1
01A235AA 04 30 ADD AL,30
01A235AC EB 02 JNZ SHORT 01A235B0
01A235AE 04 37 ADD AL,37
01A235B0 0A STOS BYTE PTR ES:[EDI]
01A235B1 C1AD 08 04 ROR DWORD PTR SS:[EBP+8],4
01A235B5 3B7D 0C CMP EDI,DWORD PTR SS:[EBP+C
01A235B8 73 E6 JNB SHORT 01A235AC
01A235BA FC CLD
01A235BB 5F POP EDI
01A235BC C9 LEAVE
01A235BD C2 0800 RETN 8
01A235C0 55 PUSH EBP
01A235C1 09E5 MOV EBP,ESP

```

generation of name

Stack SS:[0125FFF4]=00F940AC
EAX=0000001B

Address	Hex dump	ASCII
01A23228	37 32 36 31 46 33 42 31 00 43 3A 5C 44 6F 63 75	72d1f301.C:\Docu
01A23238	60 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E	Folder name Sett
01A23248	67 73 5C 73 72 61 76 61 6E 5C 44 65 73 60 74 6F	gs\srwan\Desktop
01A23258	70 5C 64 31 37 35 34 64 34 64 35 61 65 65 62 38	p\4d1754d4d5aee08
01A23268	3a 31 69 62 38 3a 3a 35 32 61 31 3a 35 64 61 66	h1cb34b32a1b3daF

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.

```

00960082 31C0 XOR EAX,EAX
00960085 48 INC EAX
00960086 98 NOP
00960087 75 18 JNB SHORT 00960094
00960089 48 DEC EAX
0096008A 83EC 00 SUB ESP,0
0096008D EB 51E0000 CALL 009636C3
00960092 EB 5B15000 CALL 00963D13
00960097 48 DEC EAX
00960098 83C4 00 ADD ESP,0
0096009A 48 DEC EAX
0096009C 31C9 XOR ECX,ECX
0096009E FF15 6CF7FFF CALL DWORD PTR DS:[FFFFFFF0]
009600A4 EB 0000000 CALL 00960000
009600A9 5B POP EBX
009600AA 87EB C01E000 SUB ESI,001E000
009600B0 EB 0000000 CALL 00960000
009600B5 EB 4E00000 CALL 00961468
009600BA EB 8AF9FFF CALL 009606A2
009600BF 31C0 XOR EAX,EAX
009600C1 58 PUSH EAX
009600C2 58 PUSH EAX
009600C3 58 PUSH EAX
009600C4 0093 733B000 LEA EBX,DWORD PTR DS:[EBX+402073]
009600C8 52 PUSH EBX

```

Remote Thread function

atd11.70912078

atd11.RIFastSystemCallRet

Explorer remote thread

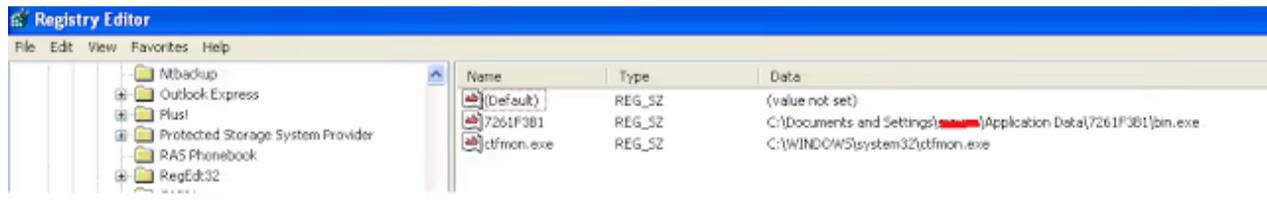
The Tinba binary is stored in a hidden folder which is created under %APPDATA% directory:

```

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

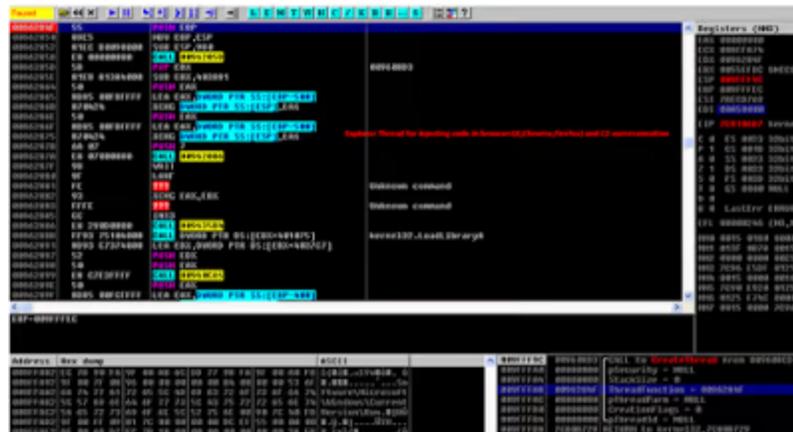
```

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



Auto start registry entry

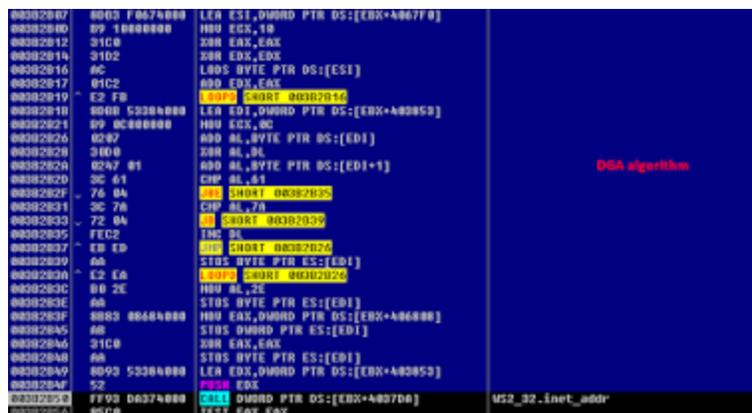
Another thread is also created in Explorer process which is responsible for generating DGA (Domain Generation Algorithm) domains and injecting code into browsers like Explorer, Chrome, Firefox and Opera.



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.



DGA routine

<i>targetHost</i>	<i>targetIP</i>
eudvwwwrmyqi.in	89.111.166.60
eudvwwwrmyqi.in	95.163.121.94
jrhiuuwgopx.com	176.31.62.78
jrhiuuwgopx.com	176.31.62.77
norubjjpsvfg.ru	210.1.226.15
norubjjpsvfg.ru	104.223.122.20
norubjjpsvfg.ru	104.223.15.16
scpxsbsjjqe.ru	5.178.64.90
scpxsbsjjqe.ru	192.198.90.228
scpxsbsjjqe.ru	5.178.64.90
wgwnmffclqv.ru	192.198.90.228
wgwnmffclqv.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.

```

01002587 60 PUSHAD
01002588 0075 00 MOV ESI,DWORD PTR SS:[EBP+0]
01002589 0040 0C MOV ECX,DWORD PTR SS:[EBP+4]
0100258C 0070 10 MOV EDI,DWORD PTR SS:[EBP+10]
010025C1 8C LOHS BYTE PTR DS:[ESI]
010025C2 3A CC XOR AL,CC
010025C4 0A STOS BYTE PTR ES:[EDI]
010025C5 ^ E2 FA XOR EAX,0FA
010025C7 61 POPAD
010025C8 59 LEAVE
010025C9 ^ E2 0000 XOR ECX,0
010025CC 55 PUSH EBP
010025CD 09E5 MOV EBP,ESP
010025CF 51 PUSH ECX
010025D0 57 PUSH ESI
010025D1 56 PUSH EDI
010025D2 0070 00 MOV EDI,DWORD PTR SS:[EBP+0]
010025D5 0075 0C MOV ESI,DWORD PTR SS:[EBP+4]
010025D8 0040 10 MOV ECX,DWORD PTR SS:[EBP+10]
010025DB 39F7 CMP EDI,ESI
010025DB ^ 76 00 JNE SHORT 010025E0
010025DF 0040E LEA EAX,DWORD PTR DS:[ESI+ECX]

```

```

Return to 01003071

```

Address	Hex dump	ASCII
02007001	6F 65 70 70 6C 6F 72 65 2E 65 70 65 51 97 7C 00	explores.exe[0]=
02007001	63 91 7C 00 00 75 C0 00 00 00 00 00 00 00 20	c:\B.BB.....[
02007001	F9 00 02 0C F0 00 02 00 10 10 03 30 F0 00 02 2C	0:00:00 00 00:00

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	Hex dump	ASCII
04000004	68 74 74 70 73 3A 2F 2F 2A 20 50 00 0A 21 2A 6C	https://* P..!*1
04000014	6F 63 61 6C 68 6F 73 74 3A 32 36 31 34 33 2F 73	ocalhost:26143/s
04000024	68 79 70 65 63 74 6F 63 2F 76 31 2F 70 6E 72 2F	kypectoc/v1/pnr/
04000034	70 61 72 73 65 2A 20 47 50 00 0A 21 2A 6D 69 63	parse* GP..!*nic
04000044	72 6F 73 6F 66 74 2E 2A 20 47 50 00 0A 21 2A 67	rosoft.* GP..!*g
04000054	6F 6F 67 6C 65 2E 2A 20 47 50 00 0A 2A 61 63 63	oogle.* GP..*acc
04000064	6F 75 6E 74 73 2E 67 6F 6F 67 6C 65 2E 2A 2F 53	ounts.google.* /S
04000074	65 72 76 69 63 65 4C 6F 67 69 6E 41 75 74 68 2A	erviceLoginAuth*
04000084	20 50 00 0A 21 2A 66 61 63 65 62 6F 6F 68 2E 2A	P..!*Facebook.*
04000094	20 47 50 00 0A 2A 66 61 63 65 62 6F 6F 68 2E 2A	GP..*Facebook.*
040000A4	2F 6C 6F 67 69 6E 2E 70 68 70 2A 20 50 00 00 00	/login.php* P...
040000B4	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00B8F9AC	25 4C 4F 43 41 4C 41 50 50 44 41 54 41 25 5C 50	%LOCALAPPDATA%\P
00B8F9BC	61 63 68 61 67 65 73 5C 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 00 00 00	1F381\log.dat...
00B8F9EC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00B8F9FC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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.

```

0096359C 55          PUSH EBP
0096359D 89E5       MOV EBP,ESP
0096359F 8B55 00    MOV EDX,DWORD PTR SS:[EBP+8]
009635A2 8B4D 0C    MOV ECX,DWORD PTR SS:[EBP+C]
009635A5 8B45 10    MOV EAX,DWORD PTR SS:[EBP+10]
009635A8 3002       XOR BYTE PTR DS:[EDX],AL
009635AA C1CB 08    ROR EAX,8
009635AD 42        INC EDX
009635AE E2 F8     LOOP SHORT 009635A0
009635B0 C9        LEAVE
009635B1 C2 0C00   RETN 0C
  
```

Send Data Encryption

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

```

13884 815.872445192.168.221.131 166.78.144.80 TCP 158 [TCP segment of a reassembled PDU]
13885 815.872063166.78.144.80 192.168.221.131 TCP 60 http > bcs-broker [ACK] seq=1 ack=101 win=64240 Len=0
13886 815.872182192.168.221.131 166.78.144.80 HTTP 182 POST /fa088f11f088d/ HTTP/1.0
13887 815.873454166.78.144.80 192.168.221.131 TCP 60 RETP > bcs-broker [ACK] seq=1 ack=238 win=64240 Len=0
13888 804.274409192.168.221.131 192.168.221.2 HEAD 110 refresh no-dank=20>

-----
[Calculated window offset: 45131]
[Window size scaling factor: -2 (no window scaling used)]
# checksum: 0x70bb [x11dataion disabled]
# [msg/ack: analysis]
TCP segment data (111 bytes)
# (2 reassembled TCP segments (217 bytes): #13884(104), #13886(113))
# Hypertext Transfer Protocol
Host: /fa088f11f088d/ www.s.vu/vn
Host: wtooslabrae.com/vn
Content-Length: 157/vn
Full request url: https://wtooslabrae.com/fa088f11f088d/
[Data request 1/1]
Data (157 bytes)
Data: 0F20043C0693a3094e5d150a210b2749e24478020043c...
[Length: 157]

0220 0a 48 6f 73 74 3a 23 78 77 74 6f 73 4b 0b 61 62 - host: wtooslab
0310 72 83 65 2e 81 6f 68 68 0a 43 6f 64 74 65 84 74 - ree.com, Content
0340 20 4c 62 67 74 68 39 20 32 35 37 68 0a 08 0a - asarant: 157...
0370 0a 48 6f 73 74 3a 23 78 77 74 6f 73 4b 0b 61 62 - host: wtooslab
0380 09 53 44 74 67 20 03 3c 05 80 00 00 05 04 f0 - cabr: .....
0390 07 60 00 13 44 00 32 f6 2f 33 00 0a 21 01 82 70 - /u/MT/ : s...
03a0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 - /u/MT/ : s...
03b0 03 f3 4f 78 8f c9 23 4c 40 cd cd b7 10 13 3b 8a - /u/MT/ : s...
03c0 03 4b 74 67 01 71 23 4a 88 0a 03 77 08 31 1f - /u/MT/ : s...
03d0 09 8c 62 21 f4 f3 49 4a 90 38 4a 99 6f 24 43 69 - C.L.OJ |...|...
03e0 0a 8c 62 21 f4 f3 49 4a 90 38 4a 99 6f 24 43 69 - C.L.OJ |...|...
03f0 0a 8c 62 21 f4 f3 49 4a 90 38 4a 99 6f 24 43 69 - C.L.OJ |...|...
0400 0a 8c 62 21 f4 f3 49 4a 90 38 4a 99 6f 24 43 69 - C.L.OJ |...|...
  
```

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](#).