

May 31 - Tinba / Zusy - tiny banker trojan

Archived: 2026-04-05 15:23:57 UTC

[May 31 - Tinba / Zusy - tiny banker trojan](#)



Amazon.com 8" Gremlin

Tinba aka Zusy is an interesting tiny (18-20KB) banker trojan. It is not the smallest in use these days, Andromeda bot is 13 KB for resident and only 9 KB for non-resident versions. I got a few samples and hoped to come up with enough data for an IDS signature but they did a good emulation of the real systems, so it is not trivial. One thing very consistent is 13 byte initial RC4 encoded request.

I am posting details here, if you come up with a signature, please share with Emerging Threats or here.

Peter's list of features

- It hooks into browsers and steals login data and sniffs on network traffic.
- Uses Man in The Browser (MiTB) tricks and webinjects in order to change the look and feel of certain webpages with the purpose of circumventing Two factor Authentication (2FA) or tricking the infected user to give away additional sensitive data such as credit card data or TANs.
- No packing or advanced encryption (yet)
- 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) dropped into the windows system folder.
- Tinba also injects itself into both "**explorer.exe**" and "**svchost.exe**" processes.
- Tinba uses primarily four different libraries during runtime: **ntdll.dll**, **advapi32.dll**, **ws2_32.dll** and **user32.dll**.
- The main components are copied into the **[%userprofile%]/Application Data/Default/bin.exe** and the encrypted configuration file "cfg.dat" accompanied by the webinject file named "web.dat".
- Tinba uses four hardcoded domains for its C&C communication.



Download



[Download the binaries listed above \(email if you need the password\)](#)

- thanks to Charles G for sharing



dakotavolandos.com

dak1otavola1ndos.com

dako22taval2andos.com

d3akotav33olandos.com

d4ak4otavolandos.com

wiecatinsu8.exe

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: 94e3fbcbf8d6f3fae34b1bc196c78082d35dc5a0084510c2c0b3ef38bc7b9cc2

MD5: debfdbd33d6e4695877d0a789212c013

Size: 19968

Sha-256: 0505f7e556f5fa5624e763fb72a769eb73c497ef8f855d706a0203848fd41c24

MD5: 8e8cd6dc7759f4b74ec0bfa84db5b1a5

Size: 20480

Sha-256: 4144bc0bf25e55fbc65c1c03831ab1a82bc9cb267f8dd6264f5d0c55585ffd55

MD5: d1c13acddb7c13d0cf5a5c49e53a2906

Size: 19968

Sha-256: 09478bf4833505d3d7b66d4f30ccce6b9fde3ea51b9ccf6fdeadc008efba43d8

MD5: b6991e7497a31fada9877907c63a5888

Size: 18432

=====

monsboys.biz

uwyhbgwiechgi.com

ieubietubviurb.com

Sha-256: e7db4b0d0ef2804d9161670908697a93032a4c1809066d54ec6f9bcc8befa341.exe

MD5: 0e252ec52d7f4604d6b8894e479de233

Size: 20480

Sha-256: c33b7e2da7e7746950615f04bca55603f6c9082dd2352efe12173f408494c660

MD5: b062be1e561c20b6fb829ad9a3303431

Size: 19456

=====

Sha-256: ed09eee5ff1de74f7af7d9666a321726e745ef12c5766753b75c20c00ed6dd9b

MD5: b4b9486d3eea4dc3b643b6bd89a4a67d

Size: 19456

basdinopowadoar.com

azonpowzanadinoar.com

sbasdinopowadoar.com



Traffic

POST /h/index.php HTTP/1.1

Host: dakotavolandos.com

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:12.0) Gecko/20100101 Firefox/12.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: identity

Connection: close

Content-Type: application/octet-stream

Content-Length: 13

y0J.....ii.HTTP/1.1 200 OK

Server: nginx/0.7.67

Date: Wed, 16 May 2012 18:20:16 GMT

Content-Type: text/html

Connection: close

X-Powered-By: PHP/5.3.3-7+squeeze3
Content-Length: 81363
Vary: Accept-Encoding

=====

POST /h/index.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: sbasdinopowadoar.com
Content-Length: 13
Connection: Close
Cache-Control: no-cache

4.`.....ii.HTTP/1.1 200 OK
Date: Mon, 04 Jun 2012 11:31:06 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.13-1~dotdeb.0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 30
Connection: close
Content-Type: text/html
..... `..ff.....p.....

=====

POST /nnt/index.php HTTP/1.1
Host: monsboys.biz
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:12.0) Gecko/20100101 Firefox/12.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: identity
Connection: close
Content-Type: application/octet-stream
Content-Length: 13

4.`.....j..9HTTP/1.1 403 Forbidden
Date: Mon, 04 Jun 2012 11:44:28 GMT
Server: Apache

Vary: Accept-Encoding
Content-Length: 396
Connection: close
Content-Type: text/html; charset=iso-8859-1

=====

POST /dataSafer3er/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: sbasdinopowadoar.com
Content-Length: 13
Connection: Close
Cache-Control: no-cache

4.ii HTTP/1.1 200 OK
Date: Wed, 06 Jun 2012 05:07:15 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.13-1~dotdeb.0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 30
Connection: close
Content-Type: text/html

Domain info

basdinopowadoar.com

azonpowzanadinoar.com

sbasdinopowadoar.com (sinkholed)

Andrash Bakkers admin@azonpowzanadinoar.com (or domain above)

+022.8260566 +022.8260566

Ahdv inc

Aleje Ujazdowskie 20-44

Warszawa,Warszawa,AF 00540

Domain Name:basdinopowadoar.com

Record last updated at 2012-05-26 12:54:16

Record created on 5/26/2012
Record expired on 05/26/2013

Domain servers in listed order:
ns1.dns-diy.net ns2.dns-diy.net

Other domains that belong to "Andrash Bakkers"

alfa-secure.com

wizestream.net /je/2fwygag.bin Zeus C2
denitraspetr.com Zeus C2
donotstoptillu.com /WCES7tT/forum.php 31.186.103.29 Known Spyeeye C2 (Zusy?)
escapefgtyuoi.com /WCES7tT/forum.php 31.186.103.29 Known Spyeeye C2 (Zusy?)
spacepushhere.com /WCES7tT/forum.php 195.210.47.230 Known Spyeeye C2 (Zusy?)
tropikana-tour.com
k-login.com
jackeydu.com
monsboys.biz

Domain Name: MONSBOYS.BIZ
Domain ID: D48970895-BIZ
Sponsoring Registrar: DIRECTI INTERNET SOLUTIONS PVT. LTD. D/B/A
PUBLICDOMAINREGISTRY.COM
Sponsoring Registrar IANA ID: 303
Registrar URL (registration services): www.publicdomainregistry.com
Domain Status: clientTransferProhibited
Registrant ID: DI_11711862
Registrant Name: Kimberly
Registrant Organization: Kimberly
Registrant Address1: 1 South Drive
Registrant City: Hyde Park
Registrant State/Province: New York
Registrant Postal Code: 12538
Registrant Country: United States
Registrant Country Code: US
Registrant Phone Number: +845.2290250
Registrant Email: