# A Look At Recent Tinba Banking Trojan Variant

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

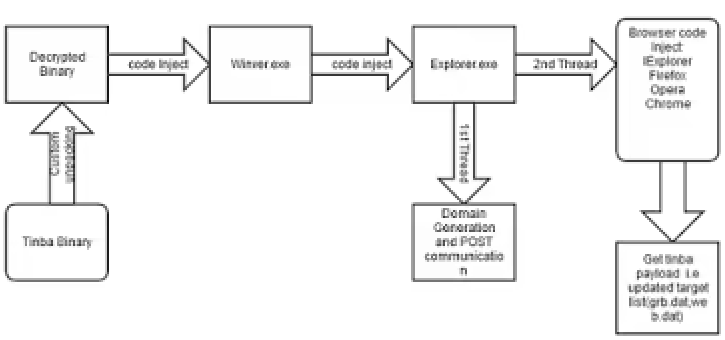
### Introduction

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

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

### Detailed Analysis of Tinba

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

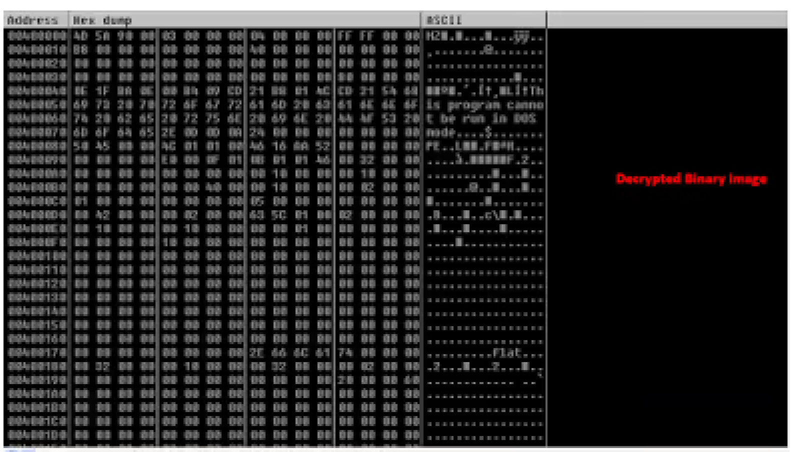


Execution flow of Tinba

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

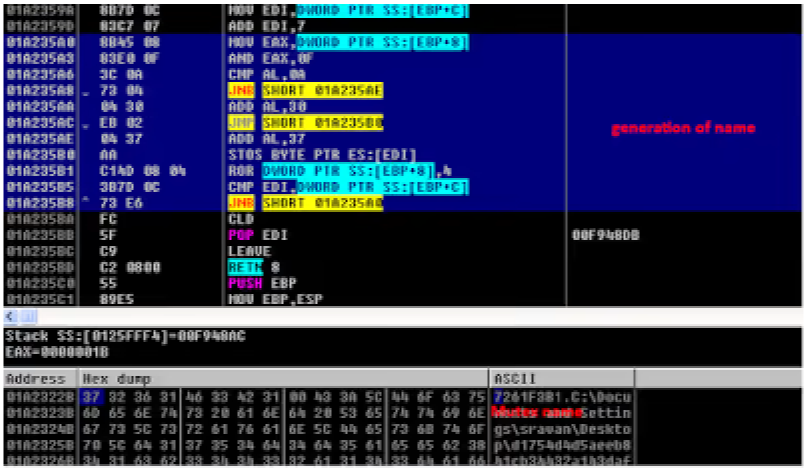

Tinba unpacking Routine

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




Unpacked Binary

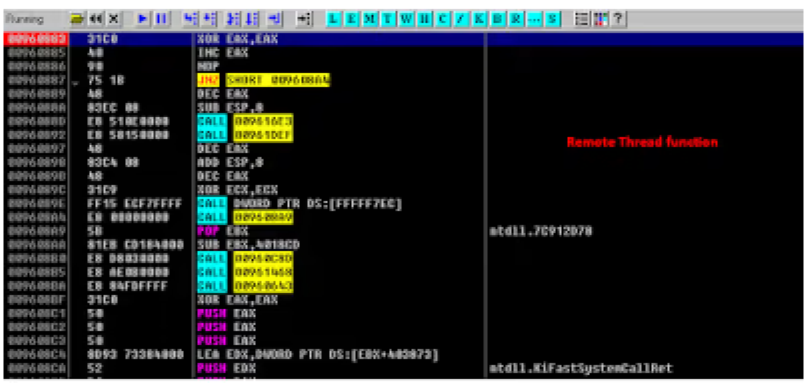
It generates Mutex name using root volume information of the victim's machine as shown below.




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.

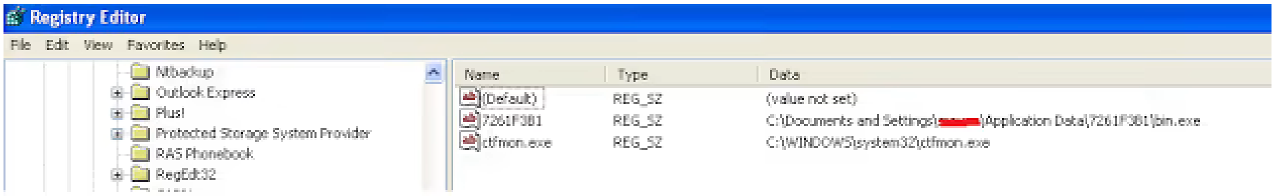



Explorer remote thread

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

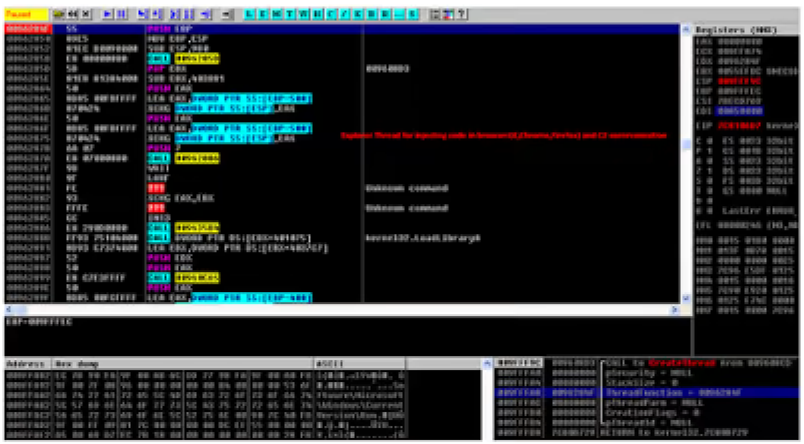
> *C:\Documents and setting \username \Application Data\mutexname\bin.exe*

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




Auto start registry entry

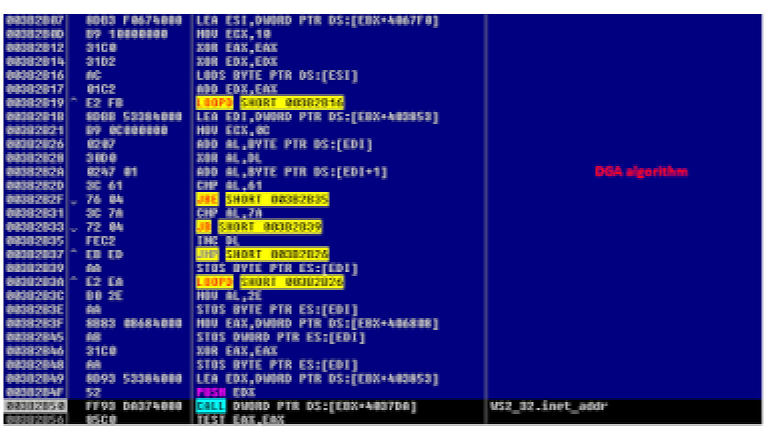
Another thread is also created in Explorer process which is responsible for generating DGA (Domain Generation Algorithm) domains and injecting code into browsers like IExplorer, Chrome, Firefox and Opera.



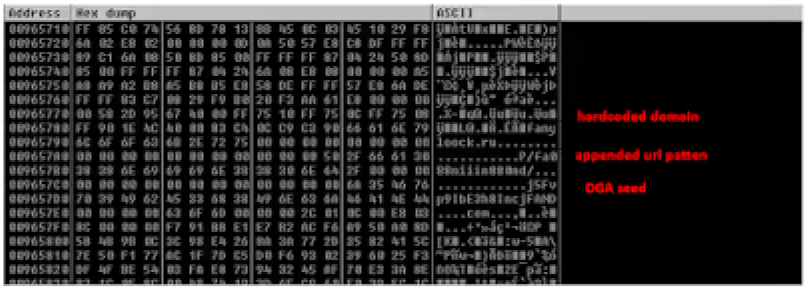
Explorer local thread

## 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

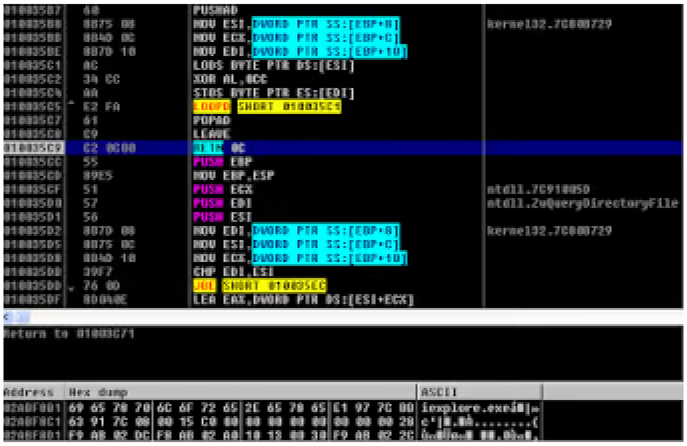



Hardcoded Domain and seed

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

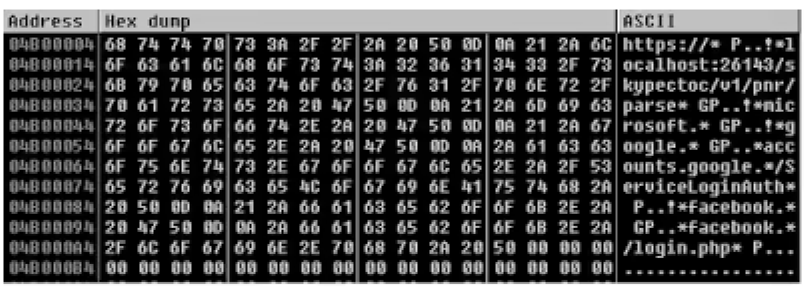
| *targetHost* | *targetIP* |
|---|---|
| eudvwwwrmyqi.in | 89.111.166.60 |
| eudvwwwrmyqi.in | 95.163.121.94 |
| jrhijuuwgopx.com | 176.31.62.78 |
| jrhijuuwgopx.com | 176.31.62.77 |
| norubjjpsvfg.ru | 210.1.226.15 |
| norubjjpsvfg.ru | 104.223.122.20 |
| norubjjpsvfg.ru | 104.223.15.16 |
| scpxsbsjjqje.ru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

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



Browser thread

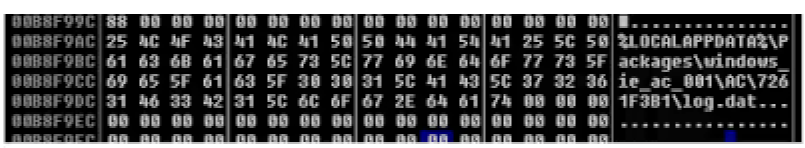
This thread is responsible to get updated Bot configuration details like Target URL list and strings (BOTUID ) from a remote C&C server. If there is no updated list of target URLs from C&C server, then it uses default targeted list of URLs which is stored in the injected code. The list of default target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



```
Address  Hex dump                                         ASCII
04B00004 68 74 74 70 73 3A 2F 2F 2A 20 50 0D 0A 21 2A 6C https://* P..!*l
04B00014 6F 63 61 6C 68 6F 73 74 3A 32 36 31 34 33 2F 73 ocalhost:26143/s
04B00024 6B 79 70 65 63 74 6F 63 2F 76 31 2F 70 6E 72 2F kypectoc/v1/pnr/
04B00034 70 61 72 73 65 2A 20 47 50 0D 0A 21 2A 6D 69 63 parse* GP..!*mic
04B00044 72 6F 73 6F 66 74 2E 2A 20 47 50 0D 0A 21 2A 67 rosoft.* GP..!*g
04B00054 6F 6F 67 6C 65 2E 2A 20 47 50 0D 0A 2A 61 63 63 oogle.* GP..*acc
04B00064 6F 75 6E 74 73 2E 67 6F 6F 67 6C 65 2E 2A 2F 53 ounts.google.*/S
04B00074 65 72 76 69 63 65 4C 6F 67 69 6E 41 75 74 68 2A erviceLoginAuth*
04B00084 20 50 0D 0A 21 2A 66 61 63 65 62 6F 6F 6B 2E 2A  P..!*facebook.*
04B00094 20 47 50 0D 0A 2A 66 61 63 65 62 6F 6F 6B 2E 2A  GP..*facebook.*
04B000A4 2F 6C 6F 67 69 6E 2E 70 68 70 2A 20 50 00 00 00 /login.php* P...
04B000B4 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 6B 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 38 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 ................
```

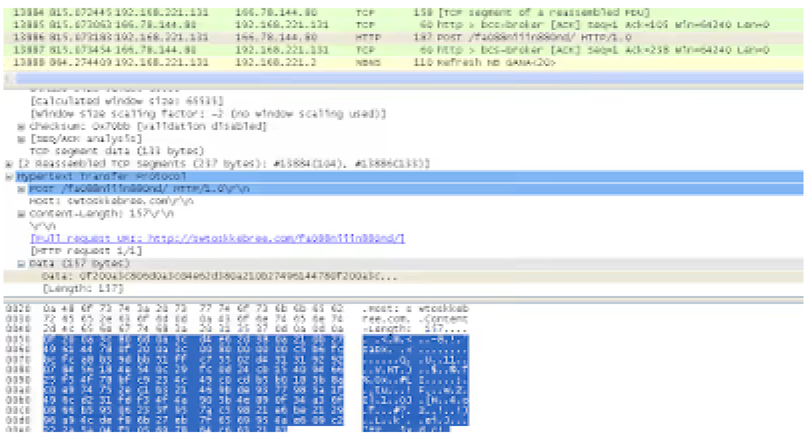
Log file path

**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.


Send Data Encryption

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



C&C POST Request

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


Geo Location

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

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

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