Exposition of Flame

Upcoming Cyberwarfare?

GYMNASIUM NOVUM, VOORBURG

February 1, 2013
Author: Adriaan de Vos
6VWO – Mr. Nuijten – Mrs. Rolvink

TABLE OF CONTENTS

Introduction

Reason for choosing this subject

I have chosen this subject for various reasons. Computer Science is one of my biggest hobby's so it sounded logical to choose a computer subject. I am very impressed with the computer security researchers at various locations over the world and I am getting information from them through twitter and blogs. Last year there was an enormous development on cyber warfare. Stuxnet got discovered and it was one of the most sophisticated viruses. It was made to slow the progress of uranium enrichment in Iranian nuclear power plants. After half a year of research they discovered a new virus, Flame, it was a bit more sophisticated and it was focused on espionage in the middle east. This subject intrigued me, so I have read a lot of information about it. The oncoming cyber warfare is a social issue of every citizen. Computers are used everywhere and are very important in the current age. Every company works with computers, traffic lights work with computers. Hackers could hack power plants or water supplies and disable them and much more. It is very important to know the dangers of this digital era. I am writing this research paper in English because I am planning to publish it on the internet for a bigger audience.

Small & brief explanation of Flame

Cyber security experts have uncovered the so-called "Flame" malware, the largest and most dangerous piece of spyware known to man. (Counts, 2012) Flame is created, supposedly, by United States and Israeli researchers. The main goal of Flame is to espionage high-target computers. Flame is not made to quickly distribute itself. It has been made to be small, silent and unnoticed. If Flame infects a computer it will use all the available resources to get information and send it back to the malware writers. He will use webcams, microphones, files, screenshots, browse history, keyboard input and much more. Flame uses various 0-day exploits to infect silently. 0-day exploits are exploits that are not publically known and available. Researchers think that Flame has been running since 2008, so the malware writers have captured a lot of valuable information. The analysis of Flame was very difficult because Flame used more than five different encryption methods.

Comparison with Stuxnet-family

Flame is part of the Stuxnet-family. Stuxnet is the first one of the family. The development of Stuxnet began in 2006 (Gates, 2012) Stuxnet has been made to infect Iranian nuclear plants and silently sabotage the centrifuges involved in the enrichment process. It was so unnoticeable that Iran was thinking of normal hardware failure by the fabricate process or **wearing**.[1] Duqu is the second one of the family. Duqu has been made to send to one computer and create a backdoor for information stealing. A backdoor is a way of infiltrating a pc without notice of the user. Stuxnet and Duqu have many similarities in the code. But their purpose is different (sabotage/espionage).

[1] Slijten, engels woord?

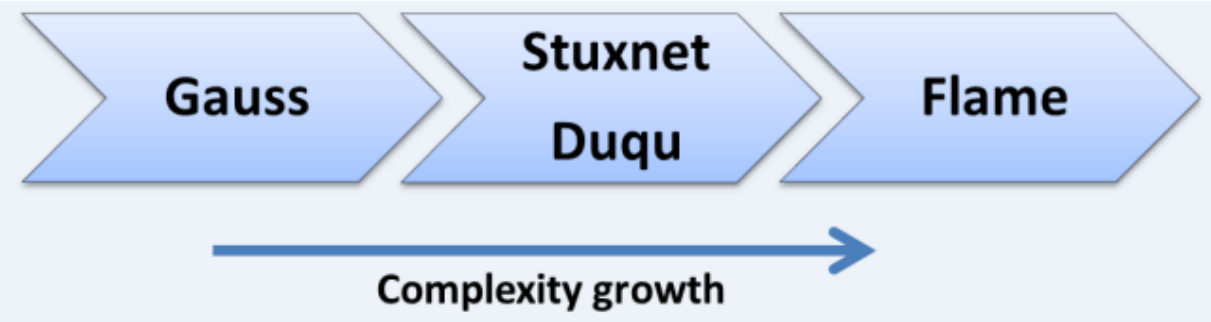


Figure 1: Complexity of Stuxnet-family (Rodionov, 2012w)

Flame is the third one of the family. Flame is more widespread than Duqu, but has not more than a few hundred infections. Flame is very similar to Duqu. Duqu wil only send info on request. Flame will send it automatically and on request. Flame is able to spread itself in the network and to collect much more information than Duqu. Gauss is the fourth and newest discovery. Gauss is the ancestor from Stuxnet. Gauss is partially still encrypted so I will not talk about it in this research paper. As seen by figure 1, Flame is the most complex and sophisticated virus in this family.

Distribution

Startup Sequence

The main module from Flame is called “msgsecmgr.ocx”. When Flame is started it begins with loading msgsecmgr.ocx. When that is finished it will create several files on the disk and starts to give instructions to services.exe (Windows program used by all background programs). Services.exe will load two new files and places three more. Finally winlogon.exe & explorer.exe (Windows programs used for logging in and showing background) will load two of the remaining files. Flame is injecting itself in legitimate programs to get more privileges and to hide itself from the user.

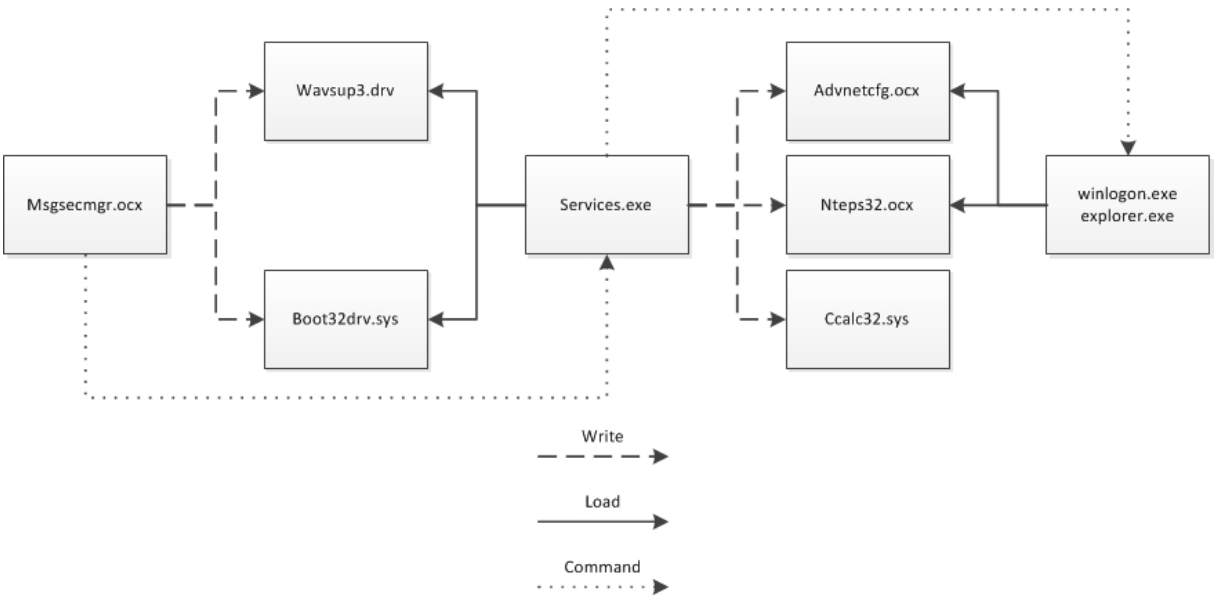


Figure 2: Startup Sequence. Left to Right.

Code injection

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Code injection can be used by an attacker to insert code into a computer program to change the course of execution. The results of a code injection attack can be disastrous. (Code injection - Wikipedia, the free encyclopedia, 2012) Code injection is mainly used by hackers and viruses. Flame uses code injection to nestle itself in valid windows programs. There are various methods of injection into other programs. Flame uses a method where it removes the origin of the code. This is very useful to slow the research and discovery of Flame. The researchers at Budapest University of Technology and Economics only discovered it because the permissions on a part of the memory has been changed to 777 (Read/write/execute).

Infection and propagation method

In this paragraph I am going to discuss the following picture. This picture has been made by Kaspersky Lab, a Russian multi-national computer security company.

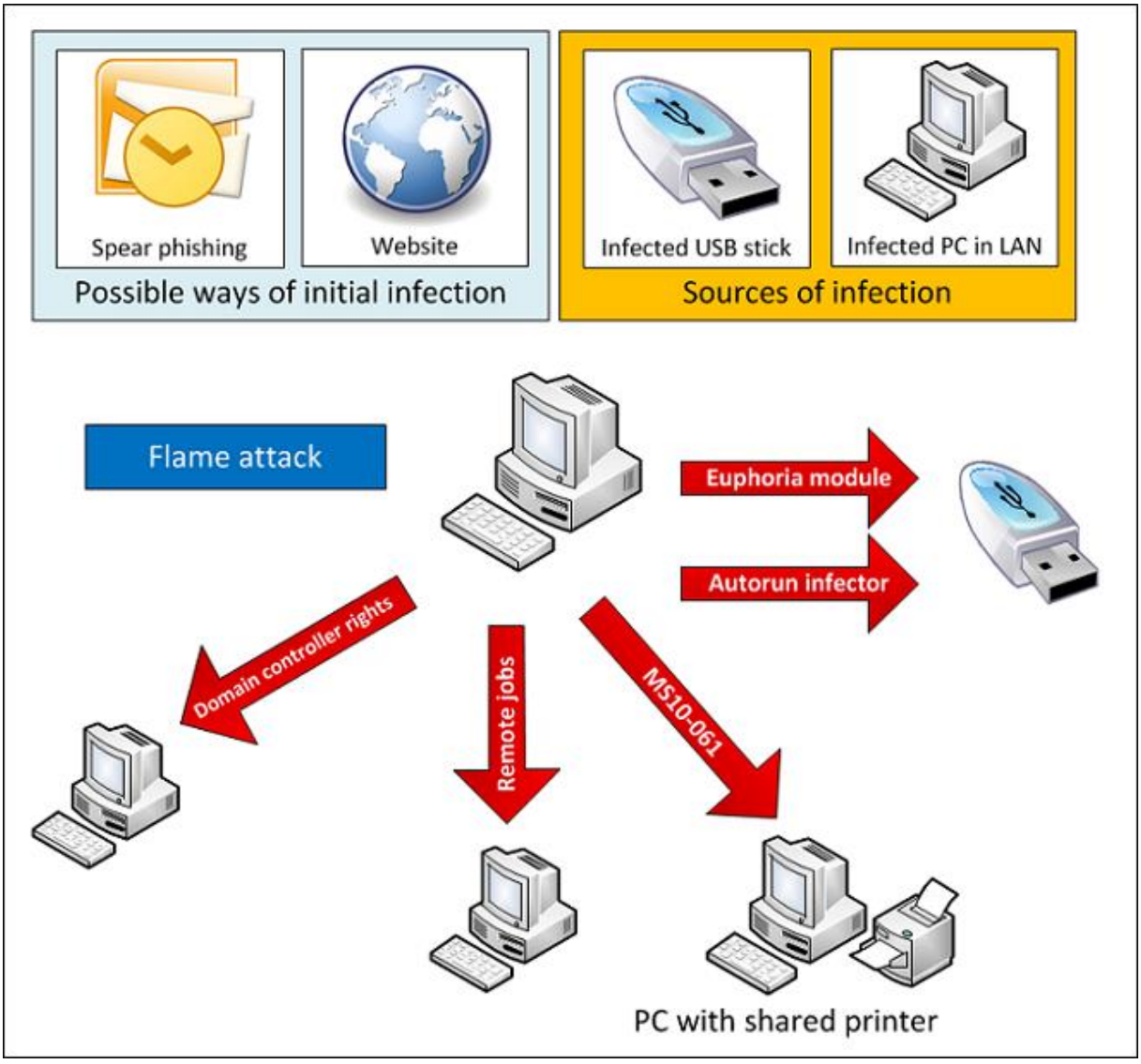


Figure 3: Infection and Propagation methods (Aleks)

There are several possible ways for the initial infection. We can only guess because it is not traceable. Researchers think that the initial infection has been caused by spear phishing or by visiting a webpage. Spear phishing is a way of sending an infected document to your target. The target thinks it is a valid document and opens it. The virus can infect the victims computer when the victim opens the document. Infection by a website is also a common used way of infection.

Figure 4: Dutch article about an infected website (Schoemaker, 2012)

The figure above is a Dutch article about the popular news-site “nu.nl”. The advertisement system from nu.nl got compromised and delivered malicious content to all the visitors of the site. 100.000 users got infected with this way of infection. Not only high-target users can be victims of malware, also average-day users can and will be infected.

When the target is infected there are several ways of propagation. Propagation is possible through USB or LAN. LAN is the Local Area Network, the network within a school/company/house. Propagation through USB is common use with malware that needs to spread on locations behind a firewall or locations without internet. Good examples are high-end corporations or important systems (nuclear reactor/water supply). Flame is using two different ways of propagation through USB.

The first way is to include a autorun.inf which will trigger a bug in the file system to run itself. Autorun.inf is a non-malicious way of automatically running any program of document from your USB. It is widely used by various users. Flame abuses this legit method to get the user to run the malware. This is called an exploit. This specific exploit was used only in Stuxnet and was not found in any other malware since.

The second way is with a junction point. This is a windows feature to create a symbolic link to a directory. You could imagine this as a simple sign near the road. For example: You want to go to a convention and the place of the convention changes every year. You do know where the sign (junction point) is. He points you in the right way, also when the place of the convention changes. In windows this is called a junction point and is used to make shortcuts to other directory’s. Flame exploited this feature to make it point to a program (Flame). When the shortcut is loaded, even when it is not clicked, it will load Flame.

In addition to these methods, Flame has the ability to propagate through LAN. It does so using three basic ways and one very special one. The first way is by using the exploit MS10-61[2]. This exploit refers to computers with a shared printer. This is often used in corporations. Flame sends a special crafted file to the listener on the target computer. The target computer receives it, reads it, and will try to print it. During the reading phase there is an exploit possible which allows remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

The second method is by using remote jobs on target computers. Remote jobs are a way of scheduling any script, program, or document to run at a time that is most convenient for you. This windows function is disabled by default but can be enabled by the system administrator to quickly send jobs to a lot of computers. Flame uses this method to add itself in an easy way to all the computers in a LAN.

The third method is a bit more difficult to explain. Flame is able to propagate through domain controller rights. This is an issue within the most company's. The domain controller ensures that all users within the system can log in and reset their password etc. It is the regulator of all the log-ins within the LAN. Flame is able to propagate through the domain controller when he infects a computer with administrative rights. Flame uses this rights to gain control over the whole network en to propagate to all the computers.

The most ground-breaking way of propagating is through Windows update. This method has never seen before and needs a lot of time for brute forcing (trying to guess a password) or it needs inside information. The developers of Flame were able to sign Flame with an spoofed official Microsoft security certificate. Flame then proceeds to offer itself through Windows Update as a legit update.

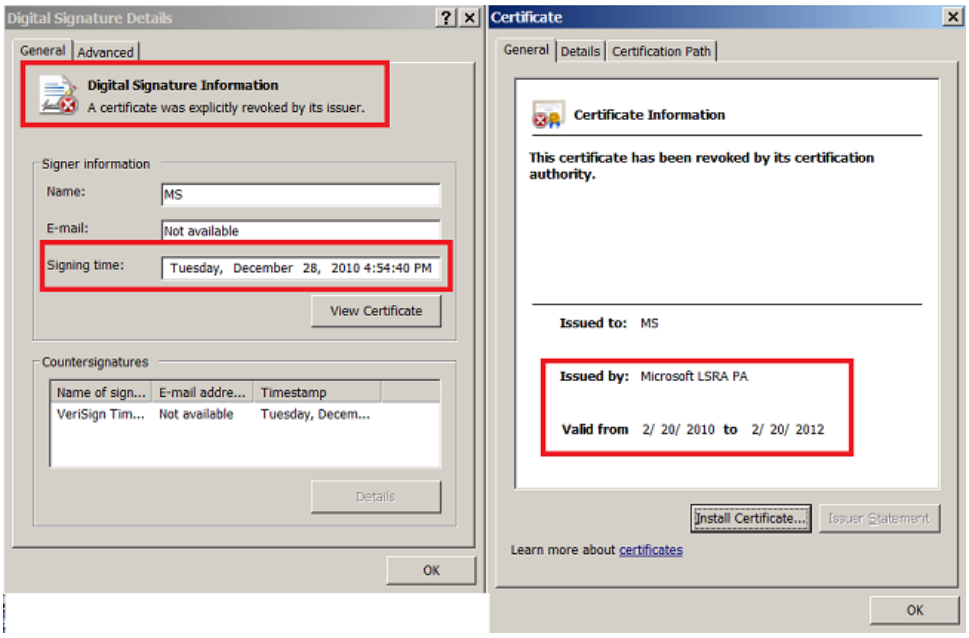


Figure 5: The now revoked signature from Microsoft. (Aleks)

[2] http://technet.microsoft.com/en-us/security/bulletin/MS10-061

The ability of Flame to offer itself through Windows Update can be called the Holy Grail in the malware world. Windows Update is used to receive updates to improve the user experience or to improve the security of your system. Updates are often automatically downloaded and installed. Flame abuses the most trustable source in Windows to spread itself.

One of the modules of Flame is a proxy. He will announce itself in the network as proxy and the other computers will make their connections through the infected machine. A second module hijacks the Windows update requests and sends a response that they need to download a new "Update". The update is the "Gadget" module of Flame. This is a downloader that, when installed through Windows update, will download the Flame virus and complete the infection.

Main components

Modules

Flame is a huge package of modules comprising almost 20 MB in size. The reason why Flame is so big is because it includes many different libraries, such as for compression, database manipulation and a Lua virtual machine. Every module communicates with the other and serves a different purpose. The following module names have been discovered when decompiling Flame. I'll not talk about all the modules, only the most important ones.

Autorun_infector	Infects the USB drives with an autorun.inf file. This is the first way of USB propagation described a few pages earlier.
Beetlejuice	Bluetooth module to discover all the devices around the infected machine. This module is also able to send the status of the malware decrypted through Bluetooth.
Boost	This a web crawler for the local computer. This module will search and enumerates all the "interesting" files on the infected machine.
Boot_dll_loader	The configuration module. This will contain the list of all the additional modules that should be loaded and started.
Euphoria	Infects the USB drives with a junction point. This is the second way of USB propagation described a few pages earlier.
Frog	Works together with the Limbo module. Frog will use the accounts generated with the Limbo module to infect other machines.
Gadget	The Flame downloader that will be downloaded and installed through Windows update. Gadget will download Flame and complete the infection. This is the fourth way of propagation.
Gator	The module that will connect to home. This module will send all the collected data to the home servers. Gator is also able to download new modules and update existing ones.

Infectmedia	The module for selecting the USB module that will be used by propagation. It will not always use both ways of infecting, sometimes just one way.
Limbo	Works together with the Frog module. Limbo will use the third way of propagation to create user accounts on not-yet infected machines.
Microbe	Records audio from all existing hardware sources.
Munch	The webserver that will offer the "update" in Windows update. This is used in the fourth way of propagation.
Security	Identifies programs that may be hazardous to Flame, i.e. antivirus and firewalls.
Snack	The module that will create a proxy and will receive all the connections within the network.
Telemetry	Logging miscellaneous sources.
Weasel	Creates a listing of all the directory's on the infected machine.

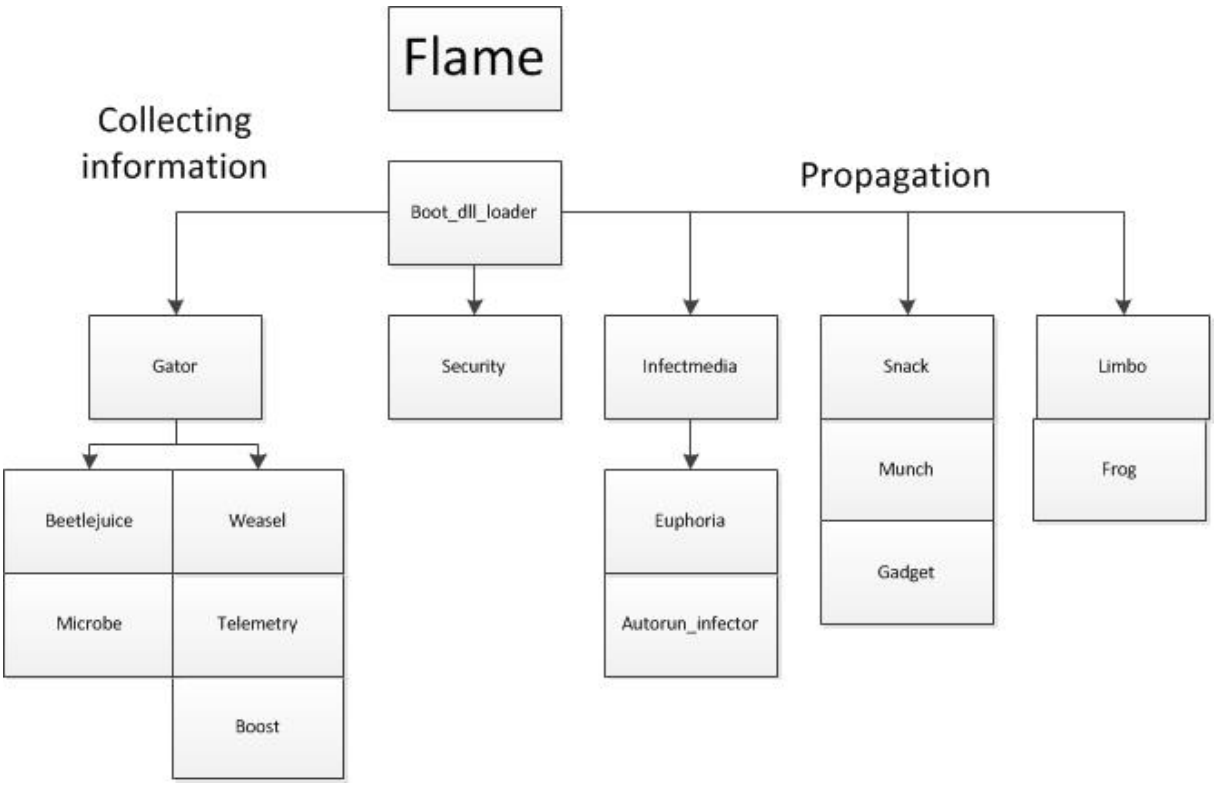


Figure 6: Visual representation of Flame modules.

This is a visual representation of the modules from Flame. On the left side are the modules which are used to collect and send information. On the right side are the modules which are used for propagation and infection.

Encryption

Flame is using various encryption methods. The source code is partially encrypted to slow the progress of the researchers and to avoid antivirus alerts. The logging of all the data is encrypted to be more hidden. And the communication with the home servers is also encrypted for eavesdropping.

One of the easiest encryption methods is the substitution table. Every character in the file is the equivalent to an encrypted one. For example, ABCDE will be UENGC. That means that BED will be encrypted to ECG. This method is not very secure.

The second encryption method is a bit more difficult but easy to reverse engineer. Every byte goes through a mathematical formula to form a new byte. For example, 256 will be 130. The formula is 256/2+2=130. There are several different formulas that will be used by Flame.

The third method is encrypted with a simple XOR. For example, the string "Wiki" (01010111 01101001 01101011 01101001 in 8-bit ASCII) can be encrypted with the repeating key 11110011 as follows: Source: Wikipedia XOR-cipher

```
  01010111 01101001 01101011 01101001
⊕ 11110011 11110011 11110011 11110011
  -----------------------------------
= 10100100 10011010 10011000 10011010
```

If the numbers are equal it translates to a zero. If the numbers are different it equals to a one. The difficult part in decrypting is to find the repeating key.

Compression

All the data that will be logged will be compressed and will be temporary stored on the hard drive. Flame creates .DAT/.HLV/.KWI files to save the data. The files are encrypted through various methods. First it starts with a PPMd compression format that is used by some programs like 7-zip and winzip. Second he will use zlib inflate compressed format, which is industrial standard for most compression of data. As third and last Flame uses a custom format to compress the data.

Logging

Flame is able to log a lot of data. For example the file list that is generated by the “Boost” module will be saved in a SQLite database. SQL databases are known for the efficiency and stability. Most data will be saved in a SQLite database. Flame is able to log various things:

- Screenshots
- Files
- Directory’s
- Bluetooth devices
- Running programs
- Audio recording

There are much more things that Flame is able to log but this are the most important ones. The controllers of Flame will know everything you do on your pc without exception.

Communication with home

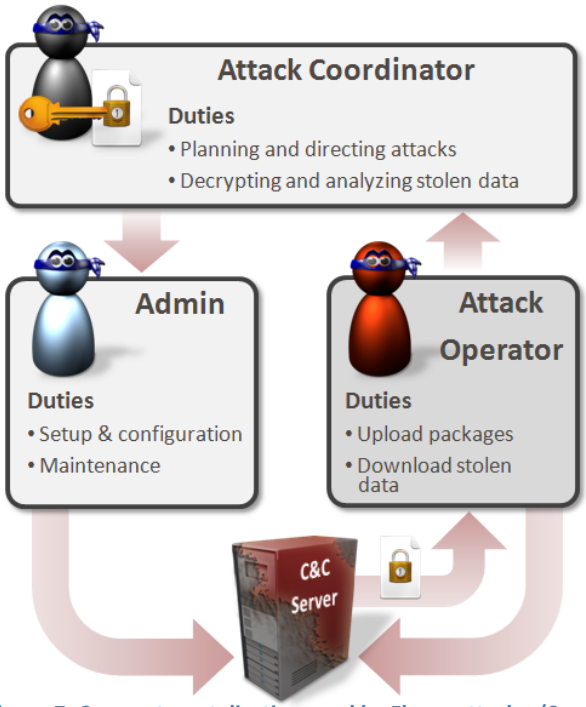
The Server

The researchers of Symantec got access to a few Flame servers a few weeks before the public announcement of the discovery. The servers had been set up to record a minimal amount of information in case of discovery. The servers were configured to disable any logging events and entries in the database where deleted on a regular basis. These steps were taken to stop any investigation should the server fall into the hands of researchers or law enforcement.

However, the source code and programs are not removed. Neither are a limited set of encrypted records in the database. The encrypted records in the database revealed that compromised clients had been connecting from the Middle East. The source code also contains the nicknames of four authors. There was also one encrypted file of stolen data left. That file is not yet decrypted.

The servers are running PHP/Apache for the webserver. MySQL for the database. And a home-made web application called “newsforyou”. It processes the Flame client interactions and provides a simple control panel. An interesting point about newsforyou is that the uploaded stolen data, as well as the updates for Flame, are encrypted, so infiltrating the server does not reveal the source code or the stolen data.

Flame is differentiating the internal structure to only allow certain rights to certain people. Researchers think there are three types of people involved in “newsforyou”. The Attack Coordinator is the leader of the whole project and might be a single person or a whole organization. He is able to plan and direct attacks and he knows the keys to decrypt the stolen data. The Admin are the people that may actually be completely unaware of the contents from the stolen data. The task of the Admin is to configure the server and to keep everything running. The Attack operator receives the stolen data and will upload new updates to the Flame clients. The following picture is a visual representation.



Figuur 7: Compartmentalization used by Flame attacks. (Symantec Corporation, 2012)

Home directory

The servers all have one home directory. I will give a brief description of the files and folders present in the user's home directory.

LogWiper_fixed.sh, This file contains all the commands to disable the logging and will delete all the current logs. This file makes it obvious that there are multiple servers because the Admins do not need to manually enter the commands each time. They will open this file to configure the logging.

RequestHandler.php, A file that is also used in the newsforyou application. This file is more recent modified and contains some small updates comparing to the running version. The modified parts are about the implementating of the RED protocol. (will get explained in the web application section.)

Delete.php, This script will be automatically run every few hours to ensure that the MySQL database is cleaned of files and entries.

Simulator/, This directory contains a set of script to test the newsforyou application.

Pycleanscr/, This directory contains scripts to free disk space.

Web application

The newsforyou application is written in PHP and contains the primary command-and-control functionality. The control panel is a basic user interface which allows updates to be installed on Flame clients. It also allows for the retrieval of stolen data that had been uploaded from these clients.

Newsforyou deciphers the incoming protocol and then logs, decodes and processes requests. Four protocols have been identified, of which three are in use. The RED protocol has not been implemented yet. The RED protocol has no connection to the Red October malware.

Newsforyou is able to it is able to communicate with four different kinds of malware. The most recent malware is called "IP" and it is yet unknown. The code is still in development. A new protocol called "PROTOCOL_RED" is not yet fully implemented.

Client	Internal ID	Protocol	Threat
CLIENT_TYPE_SP	1	PROTOCOL_OLD	Unknown
CLIENT_TYPE_SPE	2	PROTOCOL_OLD_E	miniFlame
CLIENT_TYPE_FL	3	PROTOCOL_OLD	Flame
CLIENT_TYPE_IP	6	PROTOCOL_SIGNUP	Unknown
N/A	N/A	PROTOCOL_RED	Unknown

The research of Symantec were able to corporate with GoDaddy and openDNS to create a sinkhole. A sinkhole is a technical redirection of all the connections from the infected server to a new and monitored server. When the sinkhole was in place there were a lot of incoming connections to the server from the researchers. See the following picture for statistics.

It’s obvious that the vast majority of targets are in the Middle East. It is important to point out that some victims might have used a proxy services to change the location. Some of the connections are pinpointed as being security researchers.

The infected clients did not notice the different server and they kept sending the stolen data. Such as malware version, malware configuration, a history of activities performed in the system, data extracted from documents and so on.

Country	Nr of victims
Iran	185
Israel + Palestine	95
Sudan	32
Syria	29
Lebanon	18
United States of America	11
Saudi Arabia	10
Egypt	5
United Kingdom	5
India	4
Iraq	3
Jordan	3
Austria	2
Latvia	2
Qatar	2
United Arab Emirates	2
Azerbaijan	1
Bahrain	1
Canada	1
Germany	1
Malaysia	1
Seychelles	1
Turkey	1

Evasion techniques

Security programs

The authors took extra precautions to evade detection by security products. It can clearly be seen that this malware was continuously developed over a long time period and it employs several tricks to evade security products. The malware uses .ocx as extension but this decision is based on what antivirus programs are installed. If the infected machine is running McAfee then the extension is changed to .tmp.

Flame will also try to trick the user in unconsciously adding all the virus file names to the whitelist of the antivirus program.

The antivirus reactions and recognitions are updated which every Flame update to ensure Flame to be hidden. Flame was able to run for several years unnoticed because of this many precautions taken against all the known antivirus programs.

Conclusion

A few hours after the public announcement of Flame by security researchers the whole project went dark.

The developers of Flame reacted very quick and issued a “suicide” module to all the Flame clients. This module was designed to completely remove Flame from the infected machines without leaving traces. Flame is now gone, but there are possibly more variants in the wild or in the making.

Flame was one of the most complex threats ever discovered. The geography of the targets and also the complexity of the threat leaves no doubt about it being a nation state that sponsored the research that went into it.

Flame might be the most sophisticated at this point. But he is one of many. At this moment there are rising viruses in every corner of the internet. Nations are creating defensive and offensive cybercrime units. The amount of digital attacks to spread chaos or to hurt civilians is also increasing. One could say there is definitely an upcoming Cyberwarfare.

We are lucky that there are many IT students that will become available in a few years to support the upcoming need. I have learned a lot from the research that went into this research paper and I will continue following updates about this topic.

Sources

Acknowledgements

I would like to offer my special thanks to Mr. Nuijten for his involvement in my topic and the guidance to keep continuing. I would also like to thank Mrs. Rolvink for the correction of my English language. Both helped me a lot with the process in writing this research paper.

I wish to acknowledge the help provided by Costin Raiu, Aleks Gostev and Mikko Hypponen by answering my questions and providing information.

I would also like to thank the staff of the following organizations:

- CrySyS Lab
- Kaspersky Lab
- Symantec Corporation

Sources

Code injection - Wikipedia, the free encyclopedia. (2012, november 29). Opgeroepen op januari 5, 2013, van wikipedia.org: http://en.wikipedia.org/wiki/Code_injection

Aleks. KasperSky Lab.

Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet, 2012*(4), 971-1003.

Counts, A. (2012, May 29). *'Flame', the world's 'most sophisticated cyber weapon', discovered | Digital Trends.* Retrieved Decembre 15, 2012, from Digitaltrends.com: http://www.digitaltrends.com/computing/flame-the-worlds-most-sophisticated-cyber-weapon-discovered/

Gates, G. (2012, June 1). *How a secret Cyberwar program worked - Graphic - NYtimes.com.* Opgeroepen op Decembre 15, 2012, van NYtimes.com: http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html

Rodionov, E. Figure 3 – The threats arranged according to its complexity. *Interconnection of Gauss with Stuxnet, Duqu & Flame.* Eset.

Schoemaker, R. (2012, maart 15). '100.000 computers besmet via NU.nl'. *Webwereld.nl*.

Symantec Corporation. (2012). Have I Got Newsforyou: Analysis of Flamer C&C Server. *Security Response*, 1-20.

Denning, D.E. Stuxnet: What Has Changed?, Future Internet 2012, 4, 672-687.

Boldizsár, B. The Cousins of Stuxnet: Duqu, Flame, and Gauss, Future Internet 2012, 4, 971-1003

CrySyS Lab, Technical report of Flame, May 31, 2012 http://www.crysys.hu/skywiper/skywiper.pdf