A Misuse Pattern for Flame

Paul Lewis, Sanjay Singh, and Dr. Eduardo Fernandez
College of Engineering & Computer Science of Florida Atlantic University

What can the Flame malware do? What are Misuse Patterns and Security Patterns? How do these help mitigate attacks?

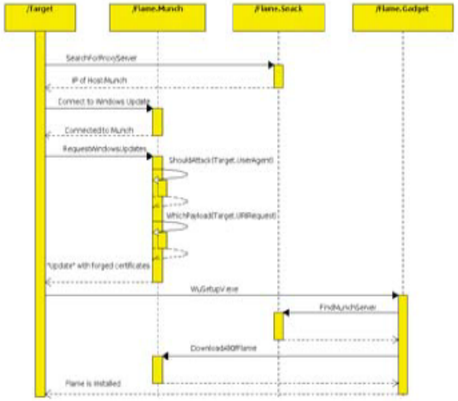
Introduction

- *Flame* is an attack toolkit that has been used to target Middle Eastern countries. Considered one of the most complex malwares ever found, it can record audio, screenshots, keyboard strokes, network traffic, and even erase itself from the machine.
- *Misuse patterns* describe how misuses are performed from the attacker's point of view. A *pattern* is a packaged solution for a recurring problem that can be cataloged and re-used in a platform- and implementation-agnostic manner. A *misuse* is the effect of unauthorized access of information.
- Misuse patterns help identify the environment in which the misuse is performed, countermeasures to prevent it, and provide forensic information to trace the attack(s).

Method

- Identify an attack or threat and understand the series of events that allow it to occur. This may be done through research of published material or hands-on analysis. The pattern shows the vulnerabilities that the attacker uses to accomplish her objectives. These are the Forces for the pattern.
- The environment(s) and preconditions in which the misuse occurs compose the Context set of the pattern.
- System components and their associations and interactions can be described with UML and can include deployment diagrams, sequence diagrams, and class diagrams.
- It is then possible to brainstorm solutions, or use established solutions, that protect systems against the attacks. The solutions consist of specific *security patterns*, which describe mechanisms to stop attacks.

Windows Update Attack Sequence



Properties of Misuse Patterns

$$M_k = \{C, F, SP\}$$

$C =$ Context of attack. Describes the environment and conditions in which misuse happens

$F =$ Forces, or what is required to start and/or stop the attack.

$SP =$ Security patterns to mitigate threats

$$F \times C \rightarrow SP$$

Properties of Security Patterns

$$SP = \{T, F, C, SPS, C_s\}$$

$T = \{ t_i : t_i$ is a threat or possible attack $\}$

$F = \{ f_i : f_i$ is a force not related to an attack $\}$

$C =$ Context, a description of the environment. May use a deployment diagram to precisely describe

$SPS =$ A mechanism to stop the threat(s)

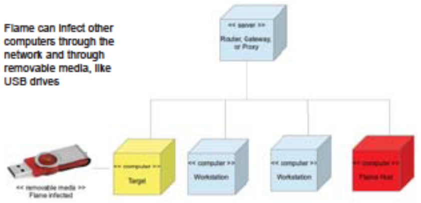
$C_s =$ Consequences such that
$C_T \cup C_F \subseteq C_s$ where
$C_T =$ Consequences of the threats occuring
$C_F =$ Consequences of the forces that influence the environment

$$T \cup (F \times C) \rightarrow SPS$$

Sou ce: Fe nandez, E.B. Yosh oka, N. Wash zak , H., Model ng M suse Patte ns, *Ava lab l ty Rel ab l ty and Secu ty 2009 ARES 09 Inte nat onal Confe ence on* , vol., no., pp.566,571, 16-19 Ma ch 2009

Contexts of Misuse

Flame can infect other computers through the network and through removable media, like USB drives



Once installed, Flame can record and access
- Keystrokes
- Information passed to connected devices like cell phones
- Audio through microphones
- Video through web cams
- Video on the monitor
- Stored files
- Bluetooth communication
- Internet traffic

Flame Modules

As described by researchers from Kaspersky Labs

Module	Description
Beetlejuice	Enumerates Bluetooth de ices around the infected machine. May turn itself into a beacon announces the computer as a disco erable de ice and encode the status of the malware in de ice information using base64.
Microbe	Records audio from existing hardware sources. Lists all multimedia de ices stores complete de ice configuration tries to select suitable recording de ice.
Infectmedia	Selects one of the methods for infecting media i.e. USB disks. A ailable methods Autorun infector Euphoria.
Autorun_infector	Creates autorun.inf that contains the malware and starts with a custom "open" command. The same method was used by Stuxnet before it employed the LNK exploit.
Euphoria	Creates a "junction point" directory with desktop ini and target lnk. The directory acts as a shortcut for launching Flame.
Limbo	Creates backdoor accounts with login "HelpAssistant" on the machines within the network domain if appropriate rights are a ailable.
Frog	Infects machines using pre-defined user accounts. The only user account specified in the configuration resource is "HelpAssistant" that is created by the Limbo attack.
Munch	HTTP ser er that responds to / iew.php and /wpad.dat requests.
Snack	Listens on network interfaces recei es and sa es NBNS packets in a log file. Has an option to start only when Munch is started. Collected data is then used for replicating by network.
Gadget	Communicates with Snack and Munch and pro ides facilities for handling different e ents that come from those modules. Together with Snack and Munch implements a replication method that is based on the Windows Update ser ice.
Boot_dll_Loader	Configuration section that contains the list of all additional modules that should be loaded and started.
Weasel	Creates a directory listing of the infected computer.
Boost	Creates a list of files using se eral filename masks
Telemetry	Logging facilities
Gator	When an Internet connection becomes a ailable it connects to the C&C ser ers downloads new modules and uploads collected data.
Security	Identifies programs that may be hazardous to Flame i.e. anti- irus programs and firewalls.
Headache	Attack parameters or properties
Bunny Dbquery Driller	The purpose of these modules was not known at the time of this writing.

Sou ce: Bencsáth B, Pék G, Buttyán L, Félegyház M. The Cous ns of Stuxnet: Duqu, Flame, and Gauss. *Futu e Inte net*. 2012 4(4) 971-1003.

Results

The results of this work are in progress as much can be accomplished by actors using Flame. Upon infection, many misuses are possible, perhaps limited by the imagination of the actor using Flame and the developmental resources required to extend its already great capabilities. However, the attention Flame garnered from its discovery has lead to thorough analysis, mitigations supplied from Microsoft, and detectability by anti-malware products

Completing this research will result in a misuse pattern that can be added to a catalog of patterns, where the value of patterns are in their reusability for a given problem. Studying these patterns can help remedy existing problems and help prevent new and similar misuses from occurring.

Discussion

1. Given the increase of discovery of complex malware on the state-sponsored scale, a pattern like this describing a specific malware can hopefully be adapted to apply to newly discovered malware with similar capabilities.
2. Understanding the possible attacks may lead to new defenses. Integrating security patterns into systems will make it harder for others to spy and abuse these systems and their information.

References

1. E.B.Fernandez, "*Security patterns in practice: Building secure architectures using software patterns*", Wiley Series on Software Design Patterns, 2013.
2. Aleks. "'Gadget' in the Middle: Flame Malware Spreading Vector Identified."*Securelist.com*. N.p., 04 June 2012. Web. 10 Mar. 2014.
3. Aleks. "The Flame: Questions and Answers." *Securelist.com*. N.p., 28 May 2012. Web. 10 Mar. 2014.
4. Zetter, Kim. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers" *Wired.com*. Conde Nast Digital, 26 May 2012. Web. 10 Mar. 2014.