Malicious Code, aka, Malware

Vijay Ganesh
ECE 458, Winter 2013
University of Waterloo
Previous Lectures on Attacks

- Control-hijack attacks
- Exploiting buffer and integer overflow
- How the attacker can take control of a machine
- We also discussed techniques to prevent, detect and recover from control-hijack attacks
- But, what about the payload?
- The entire package is often called a virus, worm,...

Many of the slides are courtesy David Brumley (CMU)
Today’s Lecture

- Taxonomy of virus, worms,…
- How virus propagate
- How worms propagate
- Detailed discussion of Stuxnet and Aurora
- 3 phases of a successful attack:
  - Social engineering
  - Exploit
  - Propagate, install and create havoc
The first worm

Catch me if you can.

Name: “Creeper” worm, 1971
Author: Bob Thomas, BBN
Vector: ARPANET DEC PDP-10 computers
Taxonomy of malicious code

Virus
Worm
Rootkit

Trojan
Malware
Advanced Persistent Threat

Spyware
Grayware
Triggered
**Virus**

Defn: Executable code hosted in a larger program. Does not self-replicate

Notable example: “Elk Cloner”
First virus found in the wild
Written in 1981 by Rich Skrenta of Mt. Lebanon High School, PA
**Worm**

Defn: Self propagating malicious code

Notable example: “Morris worm”, 1982

Robert Tappen Morris, first conviction of computer fraud and abuse act
**Virus**

Defn: Program to hide attackers presence.

Example:

Notable example: “Brain Virus”, 1986
First PC virus, intercepted and redirected calls to read boot sector.

**Rootkit**

Kernel Space

System Call

User Space

Example: redirect calls to rootkit code
Defn: group with both the **capability** and the **intent** to persistently and effectively target a specific entity.

- **Advanced**: the adversary can operate in the full spectrum of computer intrusion.
- **Persistent** means the adversary is formally tasked to accomplish a mission.
- **Threat** means the adversary is an entity with an active goal.

**Defn:** malware requiring a specific trigger to activate, such as a specific date or piece of logic.

```c
while(1){
  if(date() == Jan 31, 2009){
    rm -Rf /*
  }
}
```

Notable example: Fannie Mae logic bomb set to go off Jan 31, 2009 and wipe out 4000 servers. *(Discovered before activation)*
**Defn:** applications with undesirable features packaged with desirable features.

**Grayware**
(aka Potentially Unwanted Program)

End User License Agreement:
1. No warranties.
2. We respect your privacy.
3. We install a program to monitor your internet connection, including sites you visit.
4. We reserve right to update EULA

Notable example: Kazaa Music sharing + spyware
**Defn:** collects information without user knowledge

**Spyware**

- Collects information without user knowledge (Keystrokes, web sites visited, etc.)

**Grayware**

**Triggered**

**Virus**

**Worm**

**Rootkit**

**Computer**

**Server**
**Defn:** Malware masquerading as legitimate program

**Trojan**

Notable example: Zeus Toolkit for creating trojans and spyware
Steals bank information

http://en.wikipedia.org/wiki/File:Troj_Horse.JPG
Cyber Theft Ring

Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.

Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.

Victims include individuals, businesses, and financial institutions.

How the Fraud Works

1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan
2. Victim infected with credential-stealing malware
3. Banking credentials siphoned
4. Hacker retrieves banking credentials
5. Remote access to compromised computer
6. Hacker logs into victim’s online bank account
7. Money transferred to mule
8. Money transferred from mule to organizers

Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:
- Malware coders
- Malware exploiters
- Mule organization

Zeus ring

- 100 people
- $70M stolen
Single malware can have features from each category
Targeted Malware
Stuxnet, Duqu and Flame

• Target is a state, bank or a company

• Target a class of infrastructure, e.g., programmable logic controllers (PLC)

• Designed to circumvent protection mechanisms

• Complex malware with rootkits, worms, detection, command and control module

• Often requires dozens of experts and lots of resources
Targeted Malware
Stuxnet (also, Duqu, Flame, Aurora)

Stage 1

Social-engineering

Stage 2

Client-side exploit

Stage 3

Install/Propagate malicious program
Stage 1 of Targeted Malware
Stuxnet (also, Duqu, Flame, Aurora)

- Targets are PLCs
- Not connected to the internet
- LAN Links
- USB memory stick

Stage 1

Social-engineering

Stage 2

Client-side exploit

Stage 3

Install/Propagate malicious program
Stage 1 of Targeted Malware
Social Engineering Stage

- “Final Target” may be well secured
- However, connected laptops, phones may not
- Laptops running Windows may have many vulnerabilities
- Target this weak link first
- Social engineer through webpages, emails,…
- Figure out ways to get malicious code to removable media
- **Lesson:** Security is an end-to-end problem
Stage 2 of Targeted Malware
Stuxnet (also, Duqu, Flame, Aurora)

- Zero-day vulnerabilities
- Avoid detection
- Can remain undetected for sometime

Stage 1
Social-engineering

Stage 2
Client-side exploit

Stage 3
Install/Propagate malicious program
# Stage 2 of Targeted Malware

## Client-side Exploit Phase

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Aurora</th>
<th>Stuxnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploitation vector</td>
<td>MS10-002 (0-day)</td>
<td>MS10-046 (0-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS10-061 (0-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS10-073 (0-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS10-092 (0-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE-2010-2772 (0-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS08-067 (patched)</td>
</tr>
</tbody>
</table>

Source: [www.eset.com](http://www.eset.com)
## Stage 2 of Targeted Malware

**Client-side Exploit Phase**

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>MS10-002</th>
<th>MS10-046</th>
<th>MS10-061</th>
<th>MS10-073</th>
<th>MS10-092</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerable versions</td>
<td>Microsoft IE (6,7,8)</td>
<td>MS Windows (XP, Vista)</td>
<td>MS Windows (XP, Vista)</td>
<td>XP and Win2000</td>
<td>Vista and Win7</td>
</tr>
<tr>
<td>Remote code execution</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Only XP)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Layered Shellcode</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Other vectors</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

source: www.eset.com
Stage 3 of Targeted Malware
Stuxnet (also, Duqu, Flame, Aurora)

Stage 1
Social-engineering

Stage 2
Client-side exploit

Stage 3
- Rootkits
- Connected to server to download components
- Broken digital signature scheme

Install/Propagate malicious program
Stage 3 of Targeted Malware
Rootkit Propagation and Installation

Removable devices/MS10-046

Local Network/MS08-067, MS10-061

Win 2000, XP/MS10-073

Vista, Win 7/MS10-092

Stuxnet Propagation/installation

Privilege Escalation

source: www.eset.com
Rootkit Propagation

LNK Exploit using Shortcut Icon Load Vulnerability

• MS10-046 Vulnerability (CVE-2010-2568)

• .LNK files specify shortcuts to programs (or DLLs)

• The vulnerability is that when the Icon of a specially crafted .LNK file is merely displayed, it gets executed.

• Icons on USB drives are automatically opened by Win Explorer

• Similar to DLL Hijacking Vulnerability

source: www.eset.com
Stage 3 of Targeted Malware
Rootkit Propagation and Installation

- Removable devices/MS10-046
  - Local Network/MS08-067, MS10-061
  - Attack Vectors
  - Propagation

- Win 2000, XP/MS10-073
  - Vista, Win 7/MS10-092
  - Privilege Escalation
  - Installation

Source: www.eset.com
Rootkit Installation
Privilege Escalation

• Okay, so the attacker can execute malicious code with user privileges using LNK exploit

• But his goal is to install rootkit with higher admin privileges

• MS10-073 (0-day in Win32k.sys)

• Specially crafted keyboard layout file

• Escalation of privilege occurs while dispatching input from keyboard

source: www.eset.com
## Targeted Malware

### Aurora vs. Stuxnet

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Aurora</th>
<th>Stuxnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Companies</td>
<td>Scada systems (state)</td>
</tr>
<tr>
<td>Multiple distribution vectors</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Payload</td>
<td>Download after infection</td>
<td>All in one malware</td>
</tr>
<tr>
<td>Code packing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Code obfuscation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-AV functionality</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom encryption of communication protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Legal digital signatures</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Updates</td>
<td>Yes, via WinAPI</td>
<td>Yes, via WinAPI without creating any files</td>
</tr>
</tbody>
</table>

source: www.eset.com
END