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,…

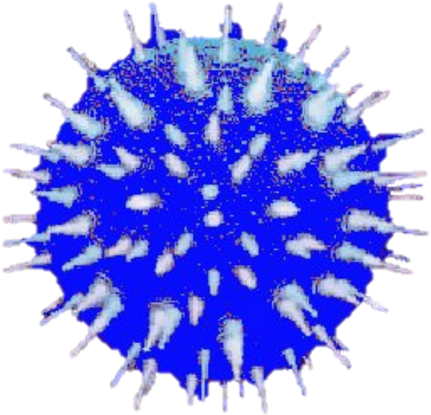
Many of the slides are courtesy David Brumley (CMU)

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

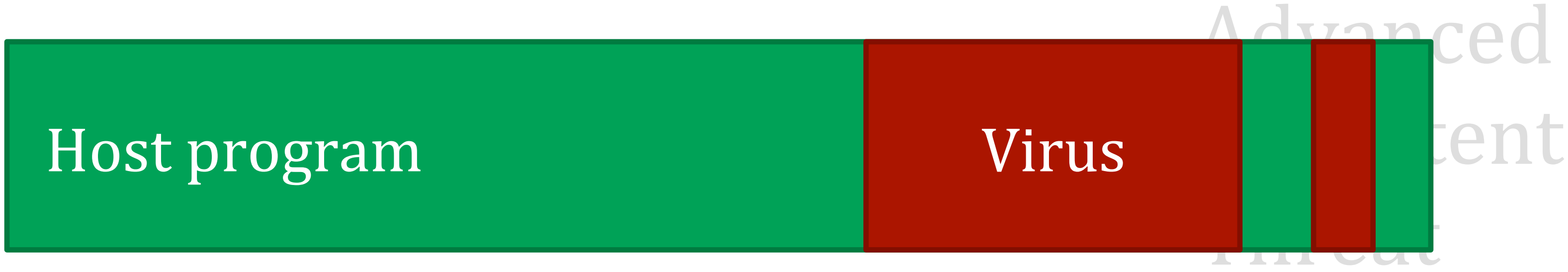
Spyware

Grayware

Triggered

Virus

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

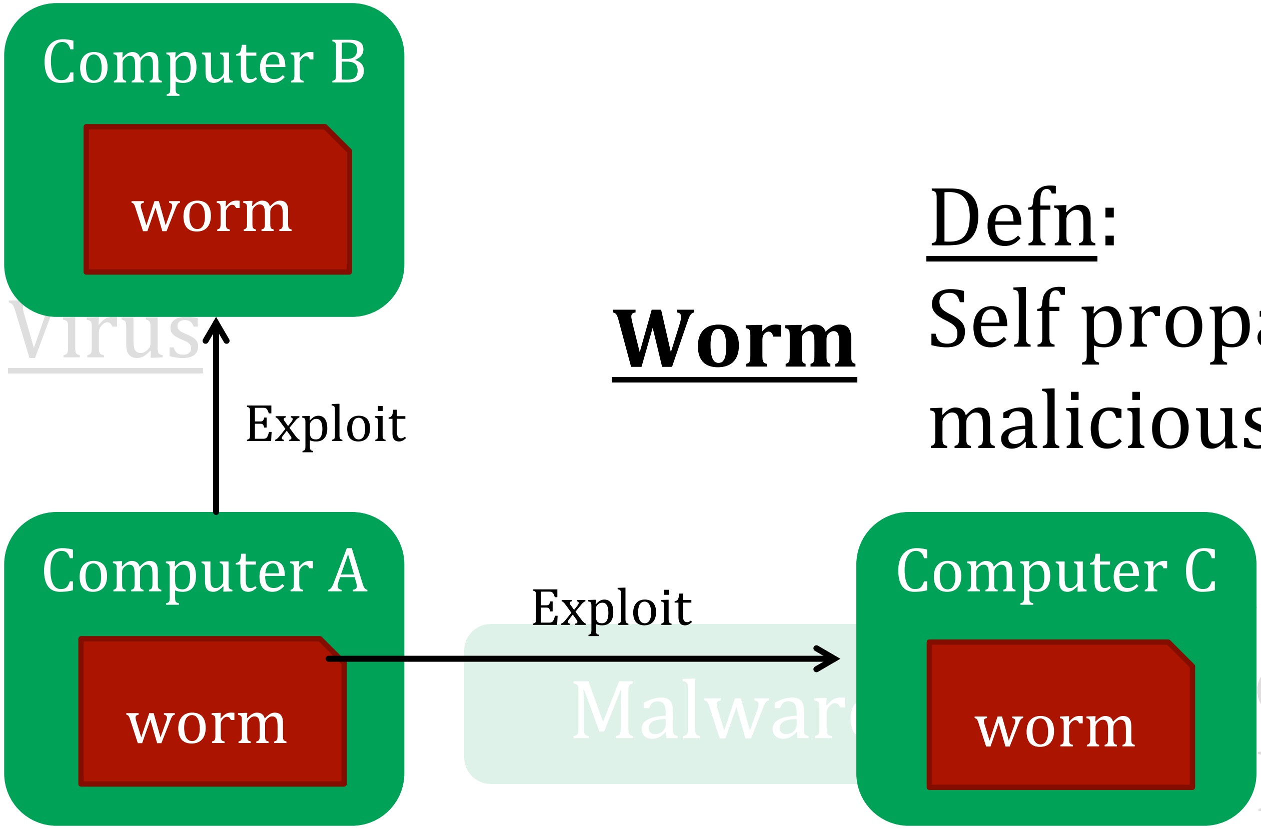


Notable example: “Elk Cloner”
First virus found in the wild
Written in 1981 by Rich Skrenta
of Mt. Lebanon High School, PA

riggered

Worm

Defn:
Self propagating malicious code



Step 1: Scan

Step 2: Attack

Step 3: Copy

Notable example: “Morris worm”, 1982
Robert Tappen Morris, first conviction of computer fraud and abuse act

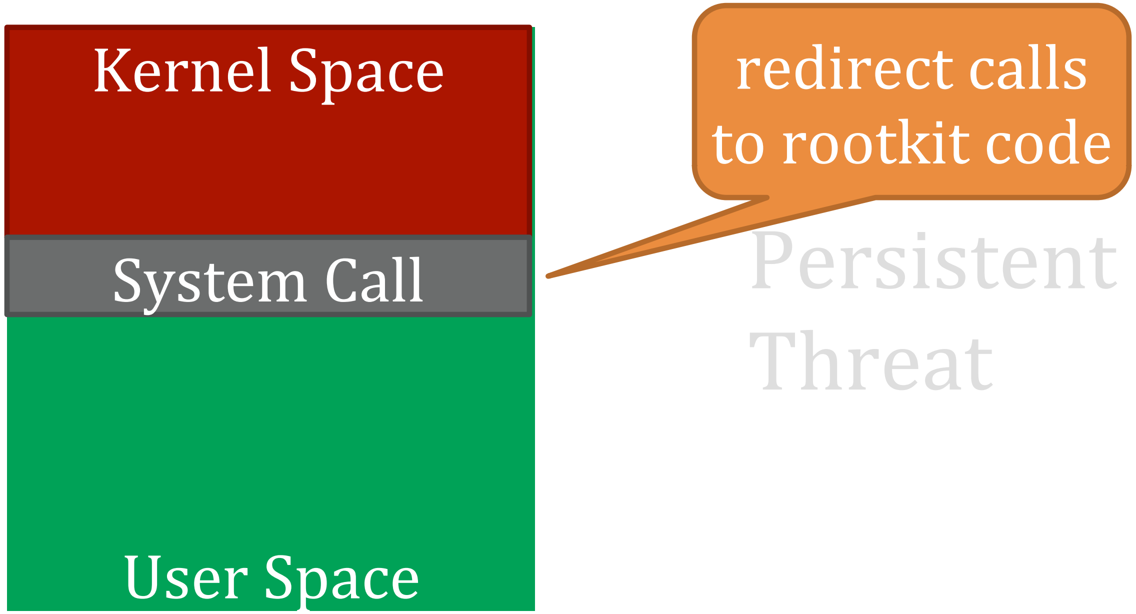
Virus

Defn: Program to hide attackers presence.

Rootkit

Example:

Trojan



redirect calls to rootkit code

Persistent Threat

Spyware

Grayware

Triggered

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

Defn: group with both the capability and the intent to persistently and effectively target a specific entity.

Virus Worm Rootkit

- **Advanced**: the adversary can operate in the full spectrum of computer intrusion.

Advanced Persistent Threat

Trojan Malware

- **Persistent** means the adversary is formally tasked to accomplish a mission.

Spyware Grayware Triggered

- **Threat** means the adversary is an entity with an active goal.

Source: http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

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

Virus

Worm

Rootkit

Trojan

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

Advanced Persistent Threat

Notable example: Fannie Mae logic bomb set to go off Jan 31, 2009 and wipe out 4000 servers.
(Discovered before activation)

Triggered

Defn: applications with undesirable features packaged with desirable features.

Virus

Worm

Rootkit

Notable example: Kazaa
Music sharing +
spyware

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

Spyware

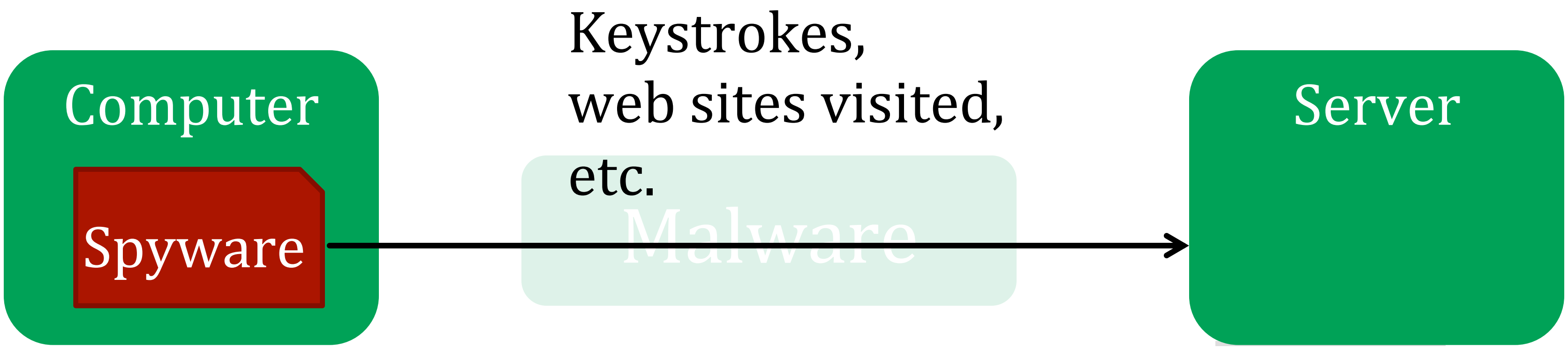
Grayware

Triggered

(aka Potentially Unwanted Program)

Defn: collects information without user knowledge

Virus Worm Rootkit



Spyware Grayware Triggered

Defn: Malware masquerading as legitimate program

Virus

Worm

Rootkit

Advanced Persistent Threat

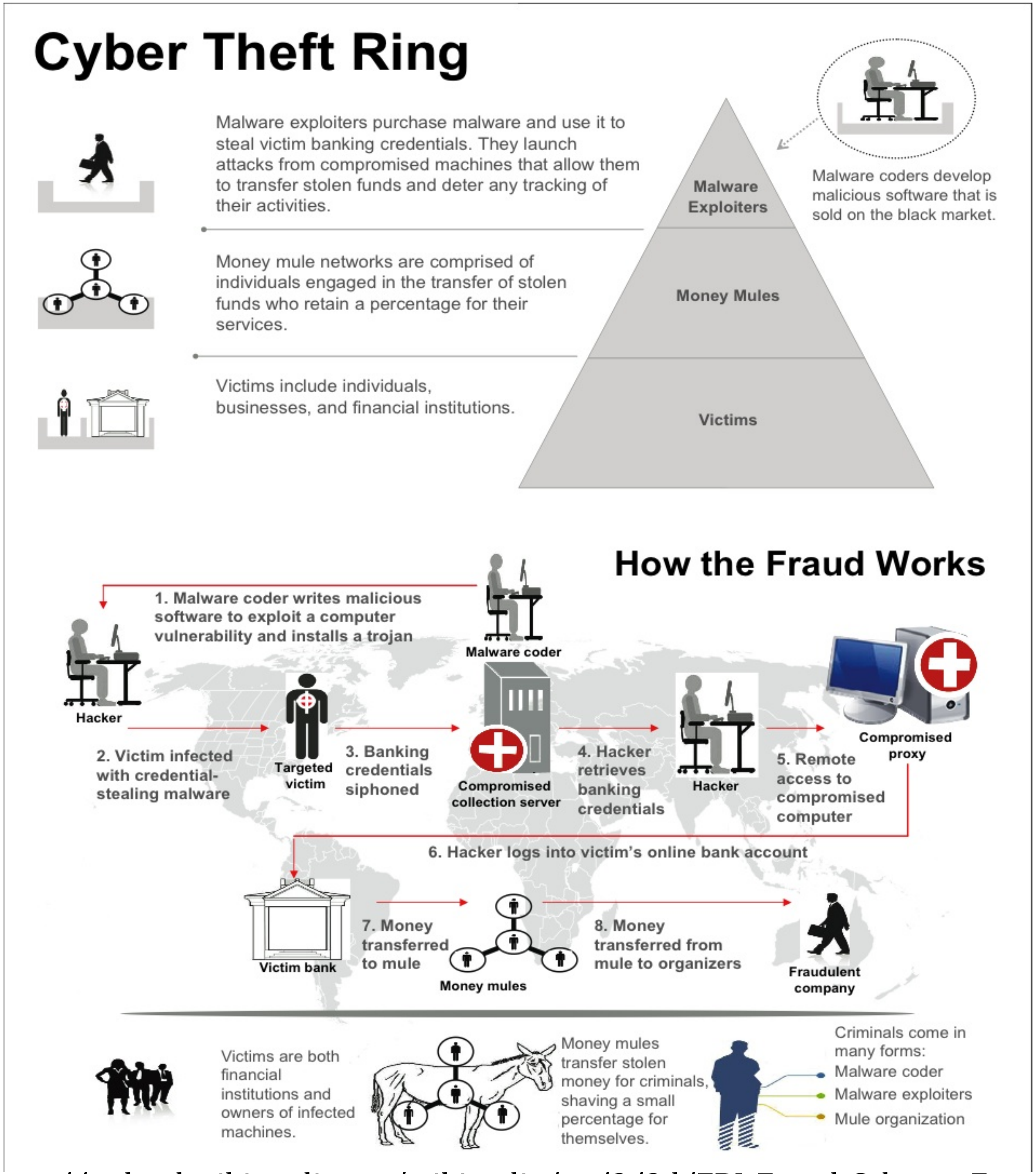
Trojan

Spyware

Graywa

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.

Malware coders develop malicious software that is sold on the black market.

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.

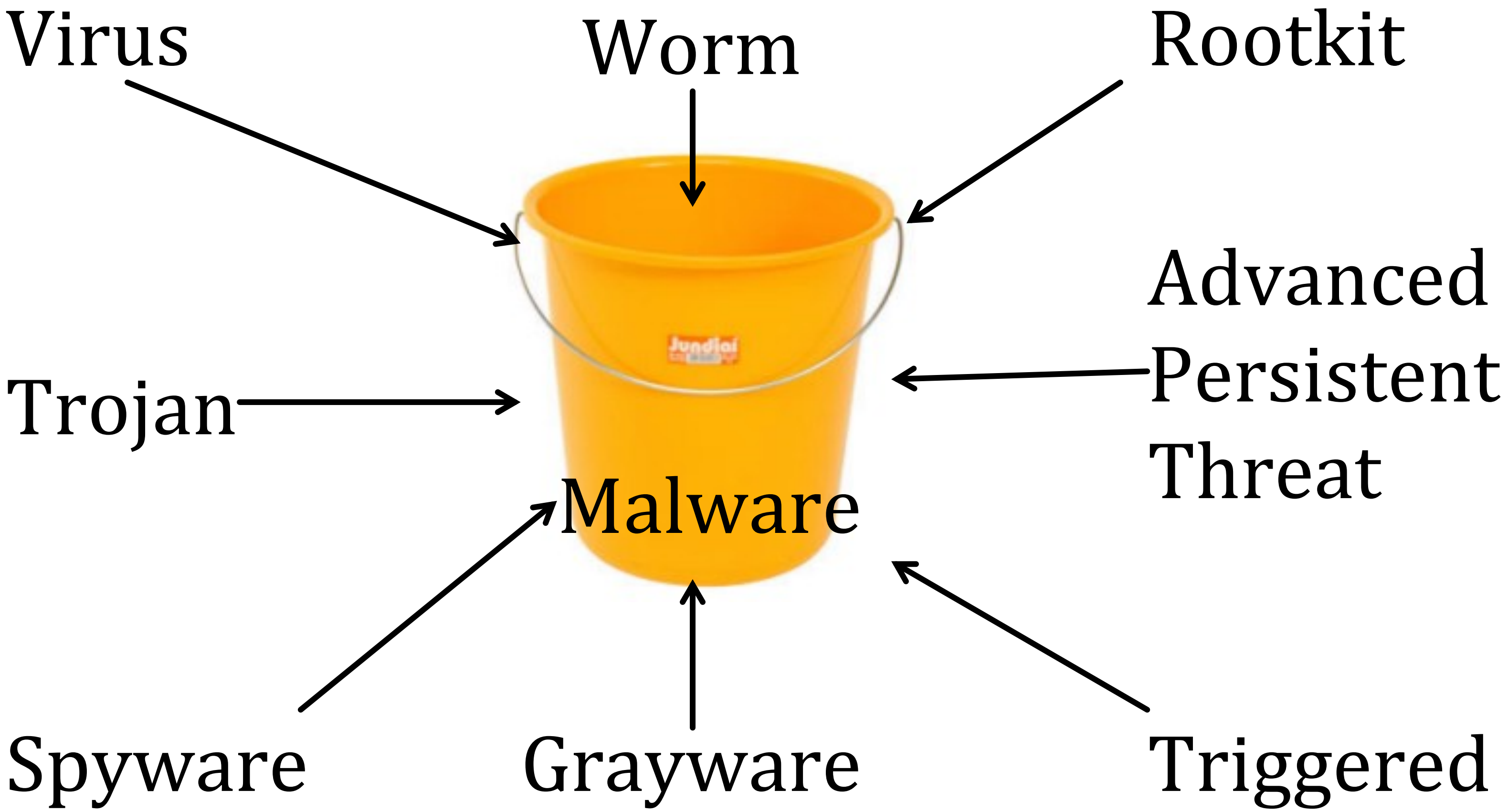
Criminals come in many forms:
- Malware coder
- Malware exploiters
- Mule organization

Zeus ring

- 100 people
- $70M stolen

http://upload.wikimedia.org/wikipedia/en/2/2d/FBI_Fraud_Scheme_Zeus_Trojan.jpg

Single malware can have features from each category



Virus

Worm

Rootkit

Trojan

Advanced Persistent Threat

Malware

Spyware

Grayware

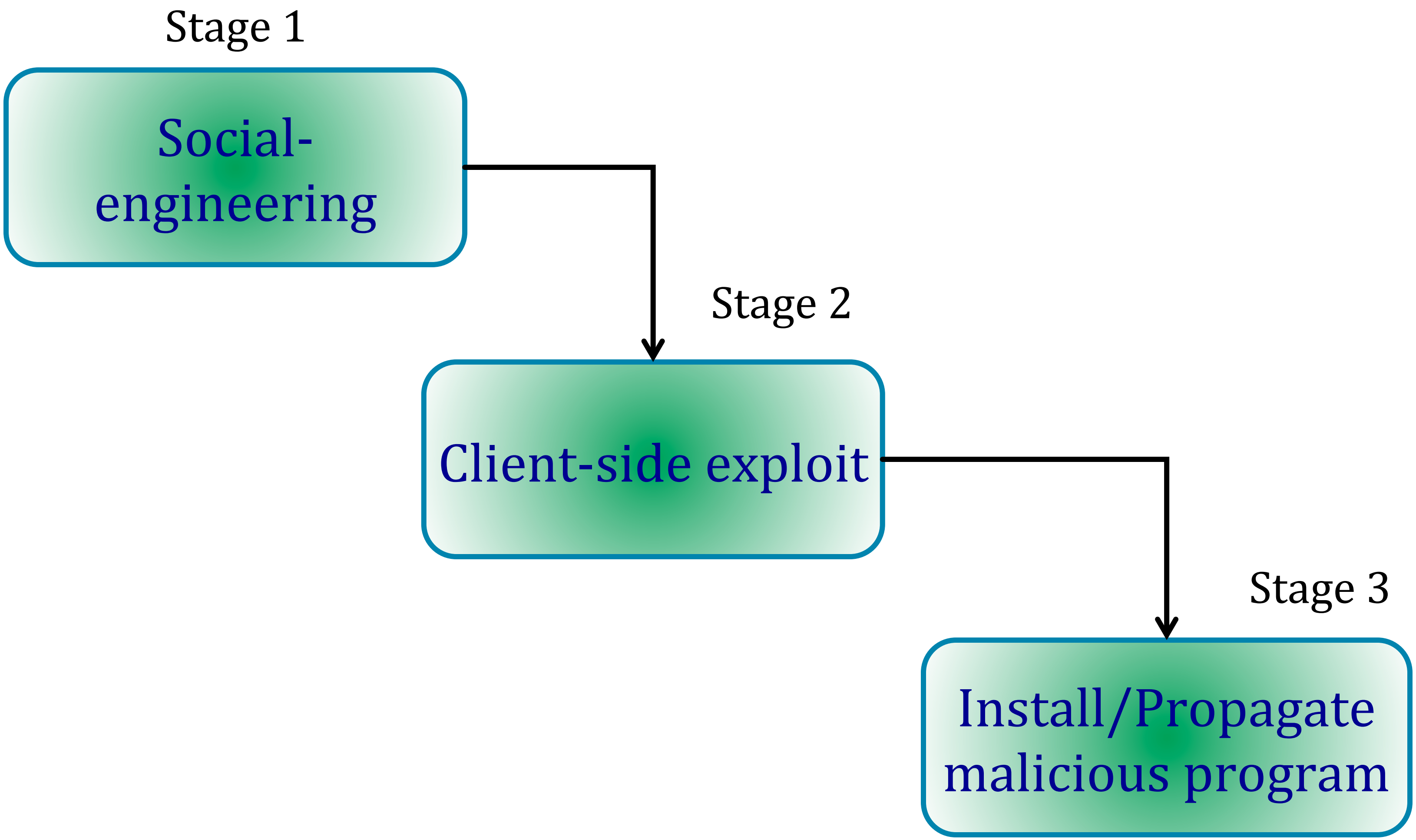
Triggered

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

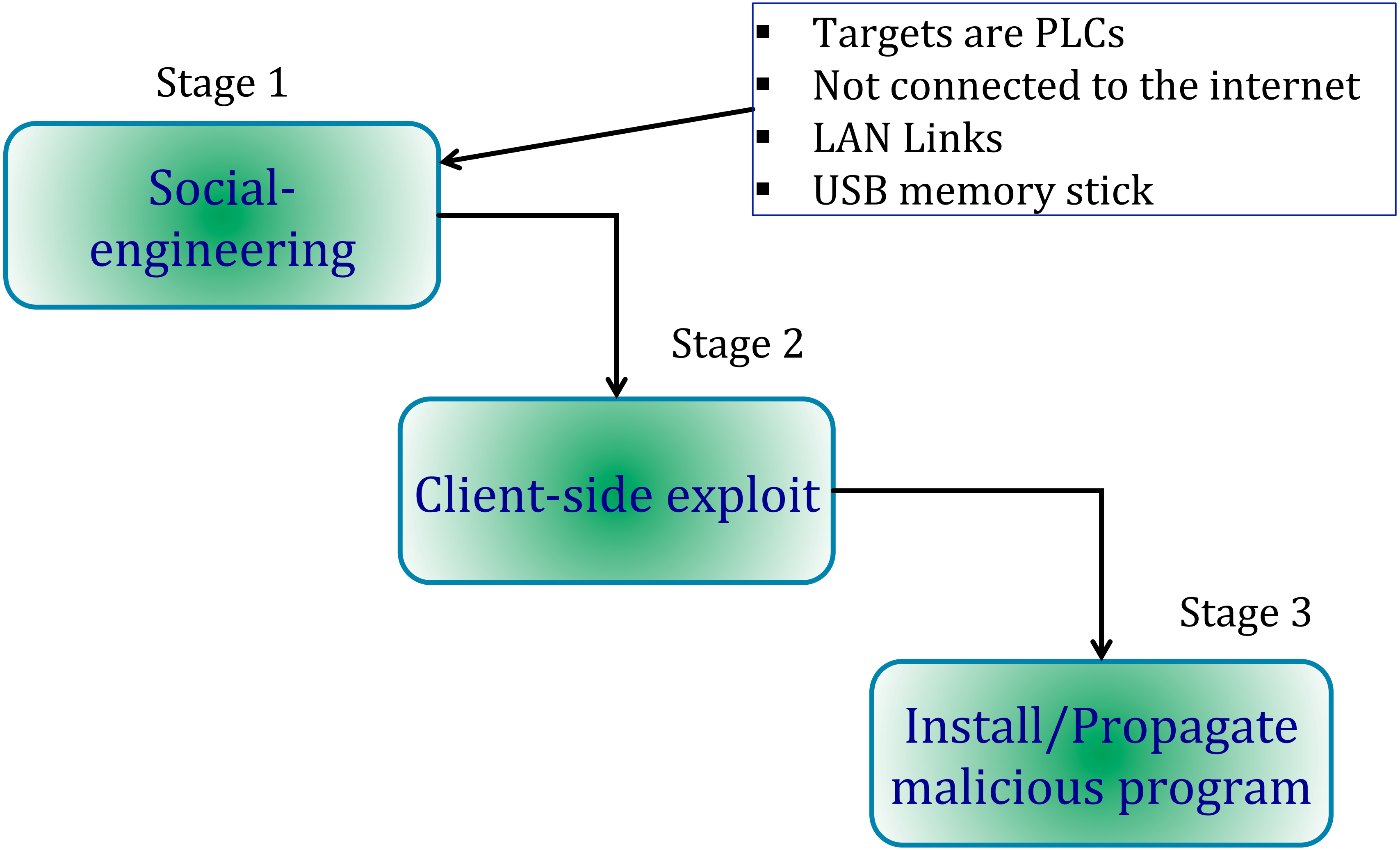
Targeted Malware

Stuxnet (also, Duqu,Flame,Aurora)



Stage 1 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

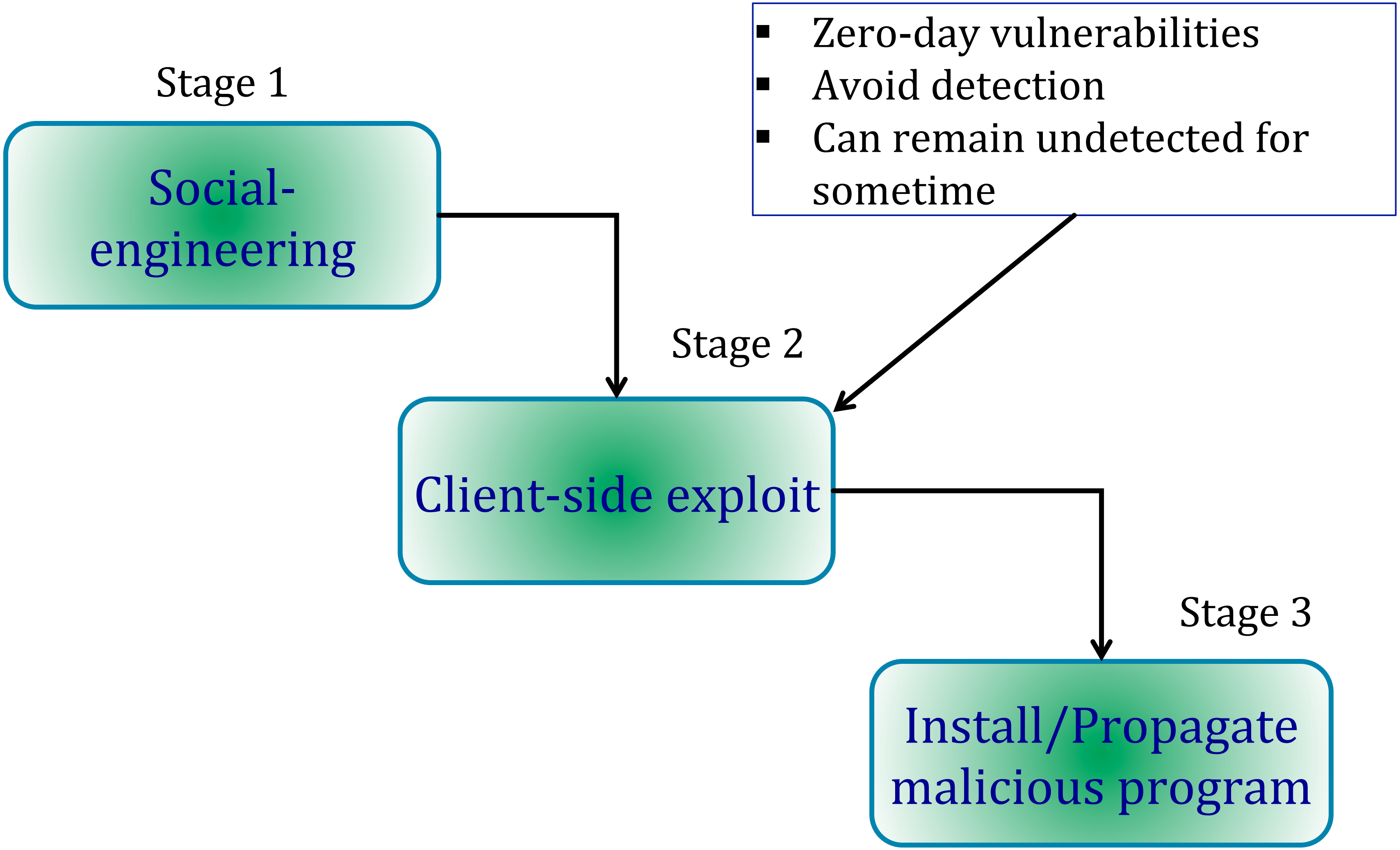
Stage 1 of Targeted Malware

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)



Stage 1

Social-engineering

Stage 2

Client-side exploit

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

Stage 3

Install/Propagate malicious program

Stage 2 of Targeted Malware
Client-side Exploit Phase

Characteristics	Aurora	Stuxnet
Exploitation vector	MS10-002 (0-day)	MS10-046 (0-day) MS10-061 (0-day) MS10-073 (0-day) MS10-092 (0-day) CVE-2010-2772 (0-day) MS08-067 (patched)

source: www.eset.com

Stage 2 of Targeted Malware

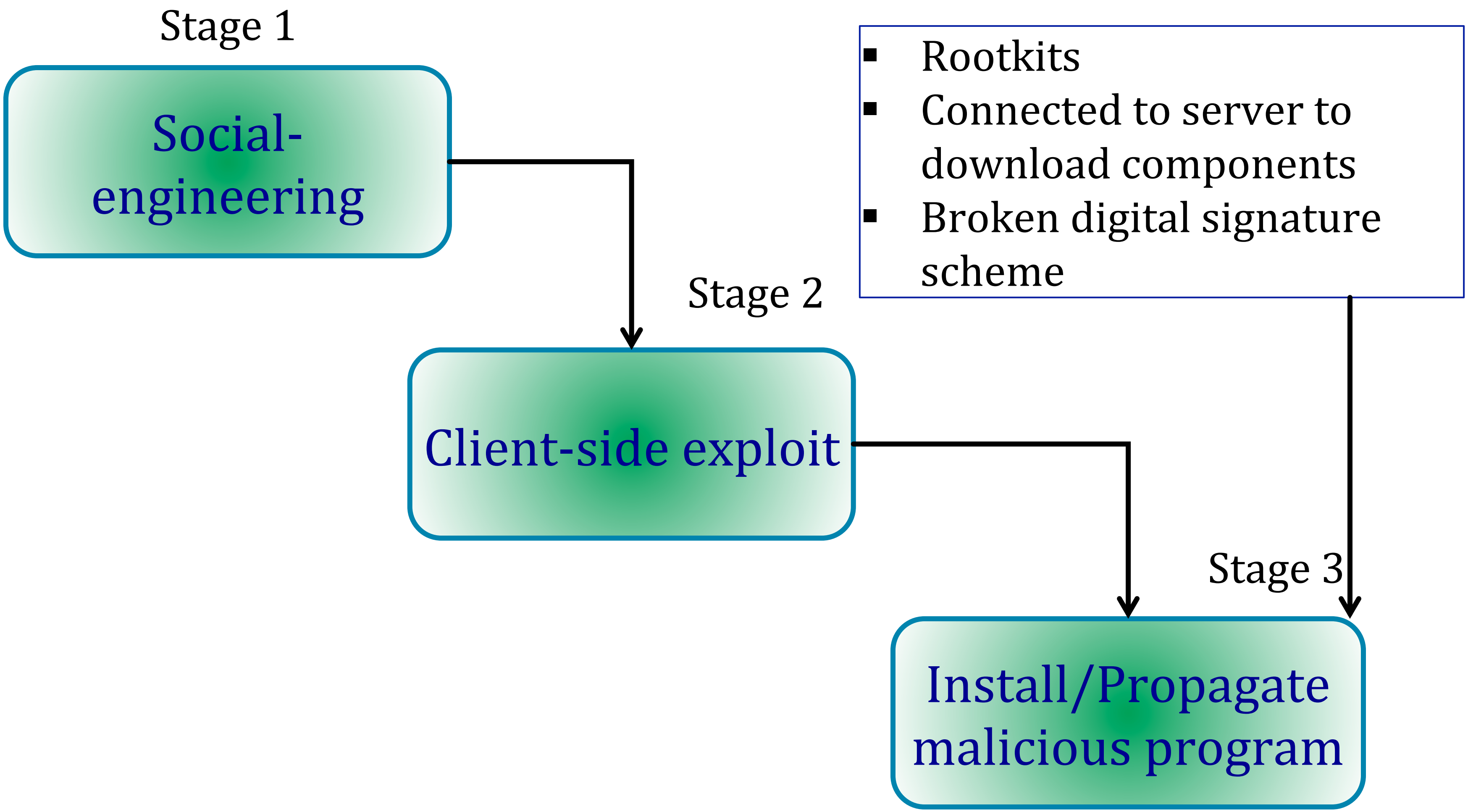
Client-side Exploit Phase

Characteristics	MS10-002	MS10-046	MS10-061	MS10-073	MS10-092
Vulnerable versions	Microsoft IE (6,7,8)	MS Windows (XP,Vista)	MS Windows (XP, Vista)	XP and Win2000	Vista and Win7
Remote code execution	Yes	Yes	Yes (Only XP)	No	No
Layered Shellcode	Yes	No	No	Yes	No
Other vectors	No	Yes	Yes	No	No

source: www.eset.com

Stage 3 of Targeted Malware

Stuxnet (also, Duqu,Flame,Aurora)



Stage 1

Social-engineering

Stage 2

Client-side exploit

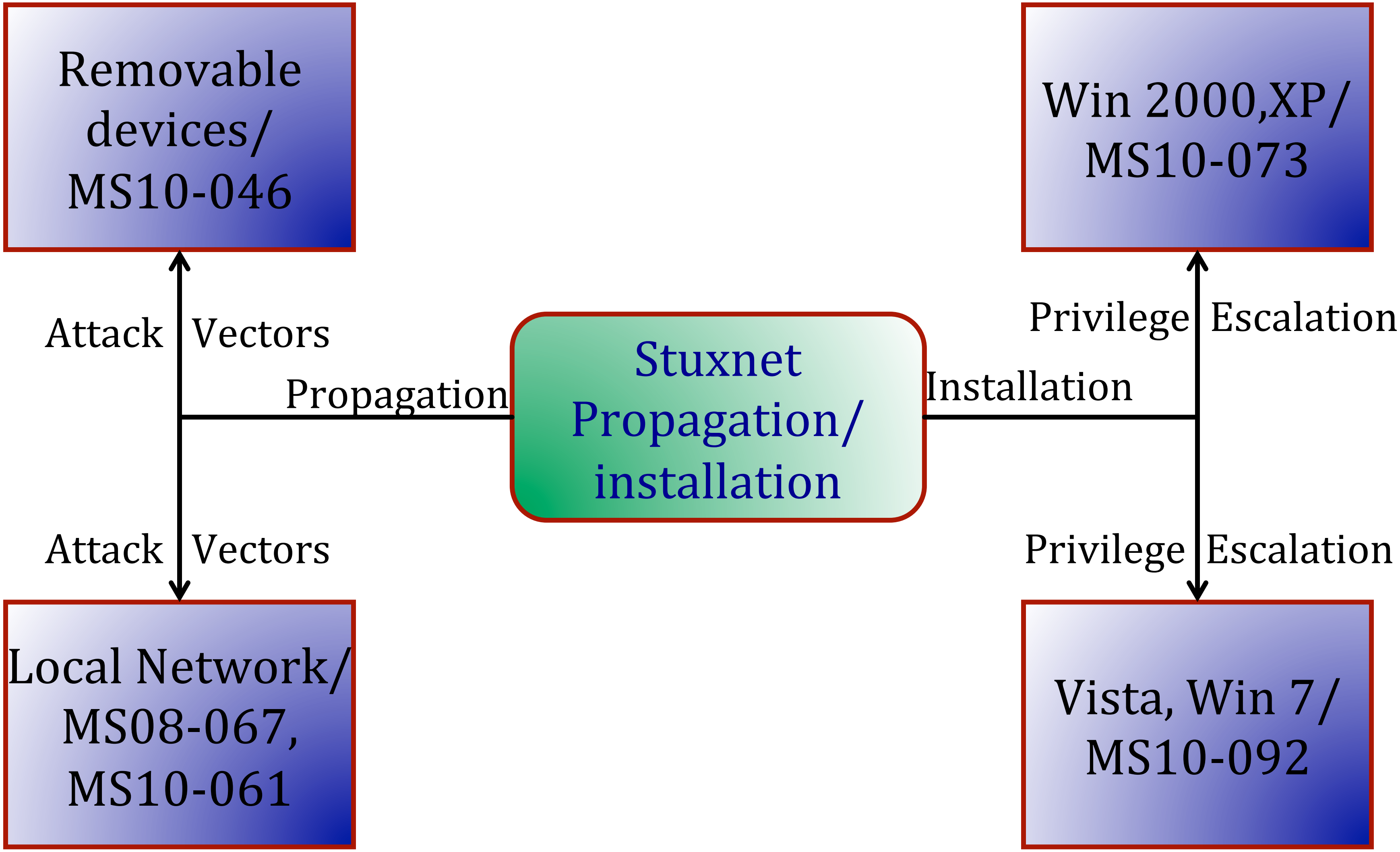
Stage 3

Install/Propagate malicious program

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

Stage 3 of Targeted Malware

Rootkit Propagation and Installation



source: www.eset.com

Rootkit Propagation

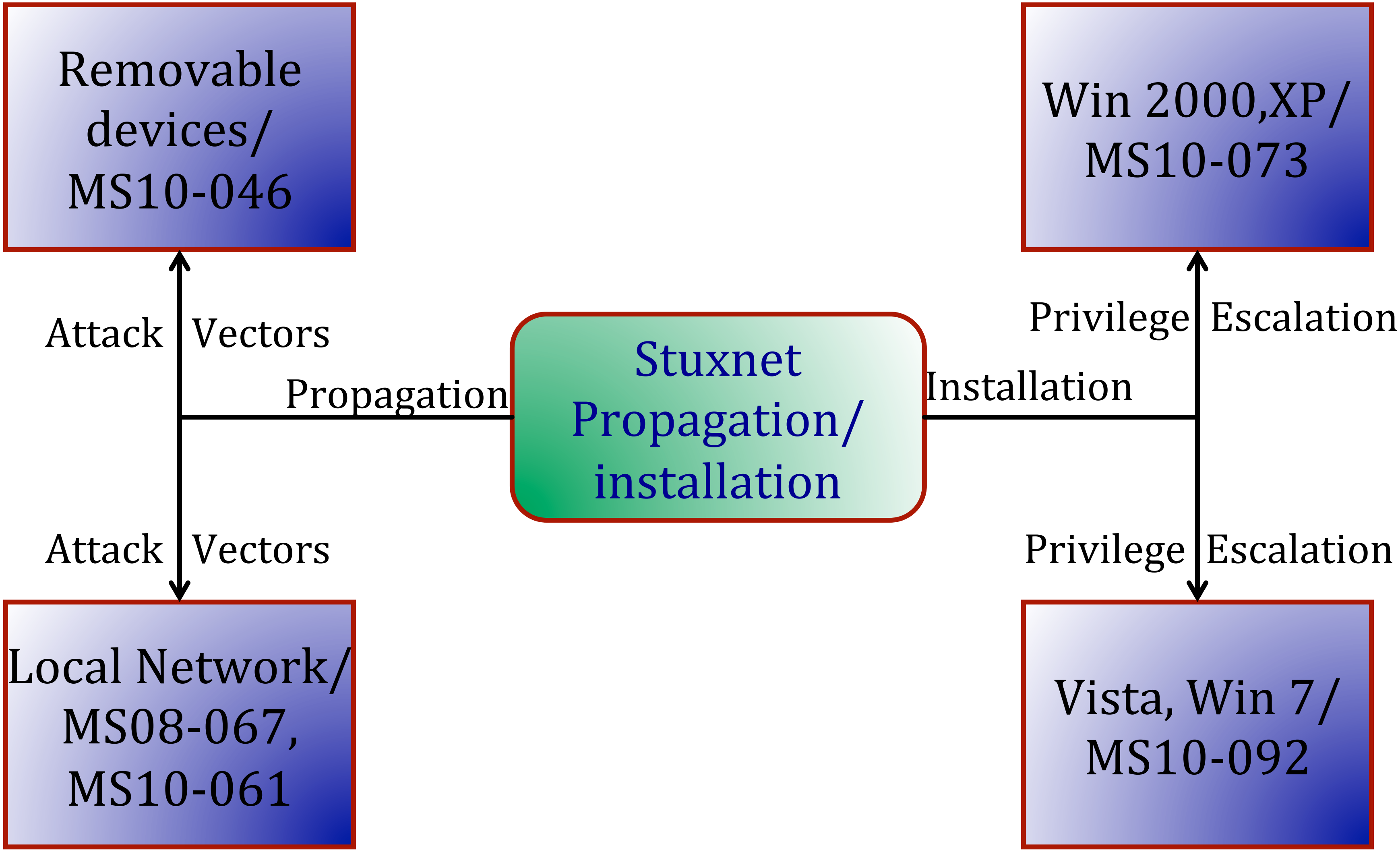
LNK Exploit using Shortcut Icon Load Vulnerability

- 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

Win 2000,XP/ MS10-073

Attack Vectors

Privilege Escalation

Propagation

Stuxnet Propagation/ installation

Installation

Attack Vectors

Privilege Escalation

Local Network/ MS08-067, MS10-061

Vista, Win 7/ MS10-092

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

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

source: www.eset.com

END