University of Stavanger

Malicious Software (Malwares)

Dr. Ravishankar Borgaonkar

DAT-510

23 October 2024

Malware

- What is Malware?
  - A Malware is a set of instructions that run on target system and make the system do something that an attacker wants it to do.
  - A program that is inserted into a system, usually covertly **(why?)**
  - Compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim’s system.

Malware as a threat today?

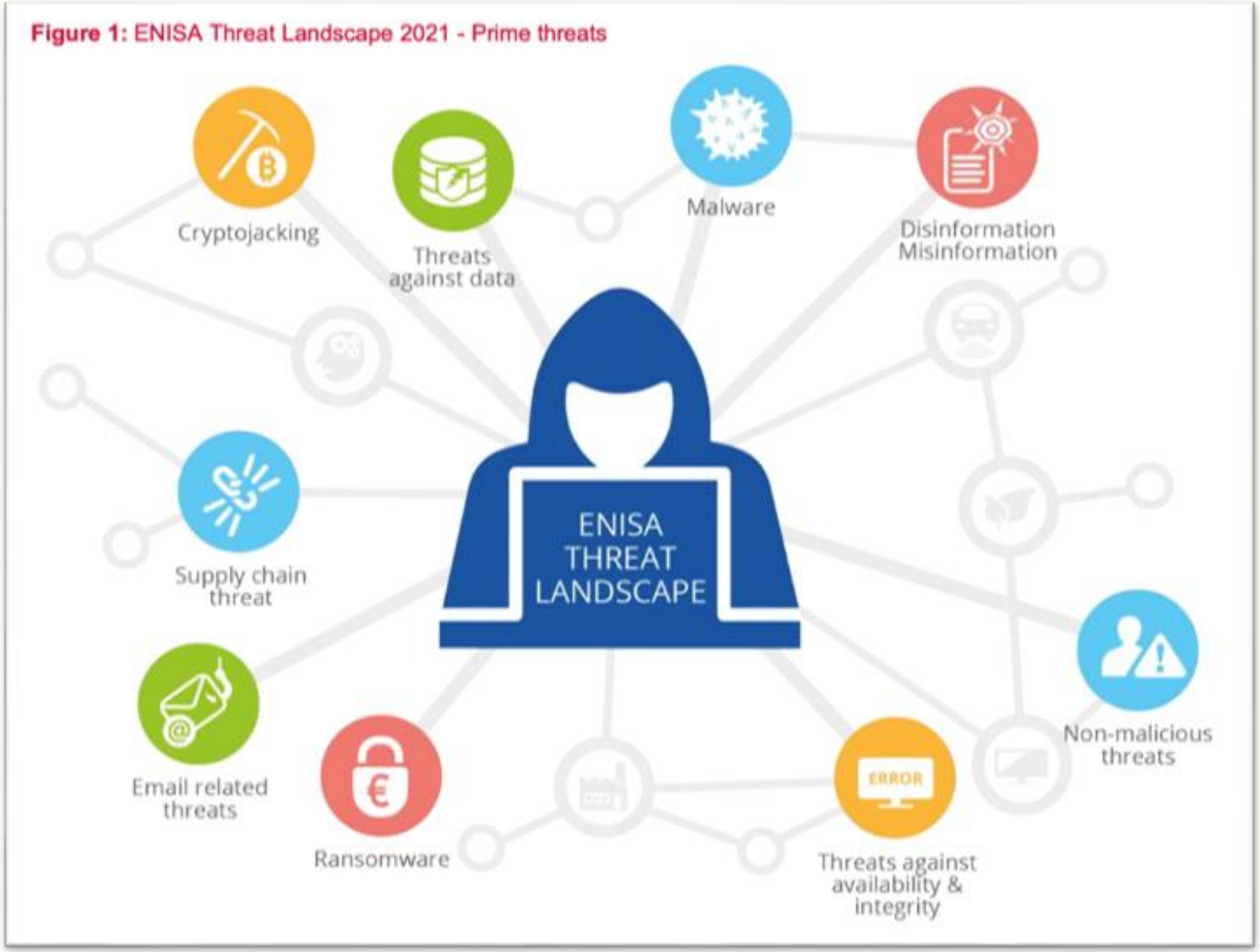


Figure 1: ENISA Threat Landscape 2021 - Prime threats

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Malware Classification

- Propagation
  - Virus, worms
- Concealment
  - Trojan horse, logic bombs, Rootkits
- Malware for stealing information
  - Spyware, keyloggers, screen scrapers
- Malware for profit
  - Dialers, scarewares, ransomwares
- Malware as a platform for other attacks
  - Botnets, backdoors (trapdoors)

Backdoor (or Trapdoor????)

- Secret entry point into a program
- Allows those who know access bypassing usual security procedures
- Have been commonly used by developers
  - a threat when left in production programs allowing exploited by attackers
  - Also typically added by malware
- Very hard to block in the operating systems
- Requires a good skillset of software development & update

Logic Bomb

- One of oldest types of malign software
- Code embedded in legitimate program
- Activated when specified conditions met
  - for example, presence/absence of some file
  - particular date/time
  - particular user
- When triggered typically damage system
  - modify/delete files/disks, halt machine, etc

Trojan Horse

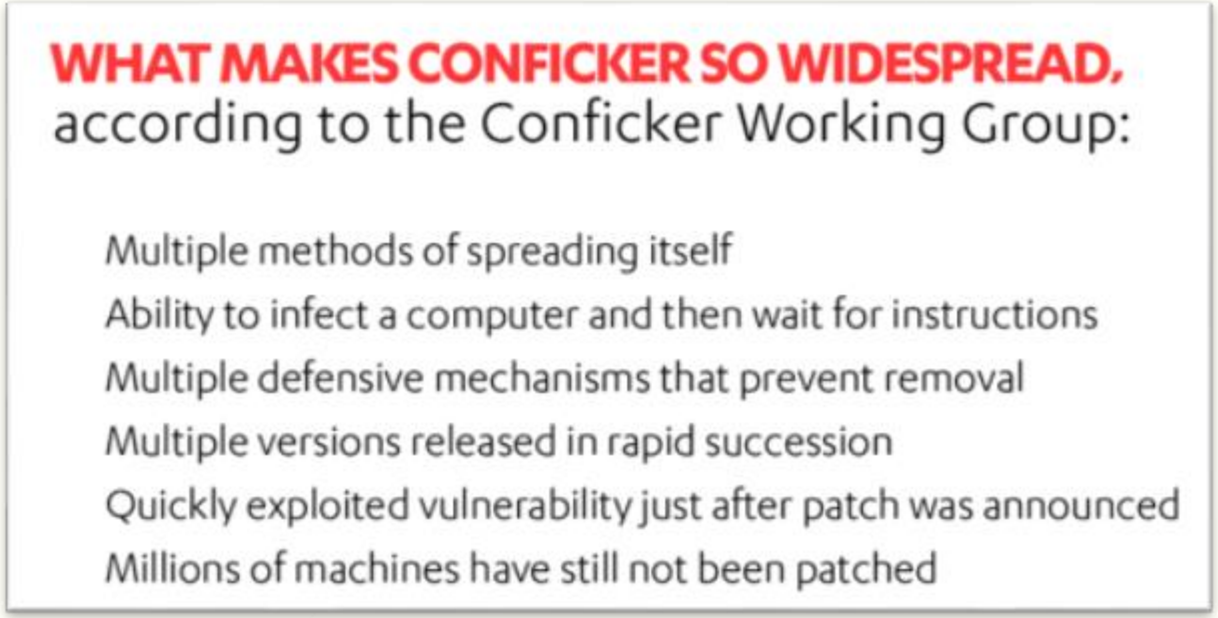
- Program with hidden side-effects
- Which is usually superficially attractive
  - e.g. game, s/w upgrade etc
- When run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- Often used to propagate a virus/worm or install a backdoor
- Also, simply to destroy data

Zombie

- (Strictly speaking more a consequence than malware)
- Program which secretly takes over another networked computer
- Then uses it to indirectly launch attacks
- Often used to launch distributed denial of service (DDoS) attacks
- Exploits known flaws in network systems

Famous Conficker Case

- Also termed as worm and extends into a botnet
- Infected millions of PCs starting in 2008
- Creates a botnet consists of zombie computers
- Zombie computers can be used for crimilan activities such as spreading spam, scareware and malwares too



WHAT MAKES CONFICKER SO WIDESPREAD,
according to the Conficker Working Group:

Multiple methods of spreading itself
Ability to infect a computer and then wait for instructions
Multiple defensive mechanisms that prevent removal
Multiple versions released in rapid succession
Quickly exploited vulnerability just after patch was announced
Millions of machines have still not been patched

https://blog.f-secure.com/what-weve-learned-from-10-years-of-the-conficker-mystery/

Mobile Code

- Program/script/macro that runs unchanged
  - on heterogeneous collection of platforms
  - on large homogeneous collection (Windows)

- Transmitted from remote system to local system & then executed on local system

- Often to inject virus, worm, or Trojan horse

- Or to perform own exploits
  - unauthorized data access, root compromise

Multiple-Threat Malware

- Malware may operate in multiple ways
- Multipartite virus infects in multiple ways
  - eg. multiple file types
- Blended attack uses multiple methods of infection or transmission
  - to maximize speed of contagion and severity
  - may include multiple types of malware
  - E.g. Nimda has worm, virus, mobile code or conficker too
  - can also use instant messaging & P2P file sharing

Ransomware - 1

- “type of attack where threat actors take control of a target’s assets and demand a ransom in exchange for the return of the asset’s availability and confidentiality”
- Three main elements – assets, actions, & blackmail
- Four actions LEDS – Lock, encrypt, delete, & steal

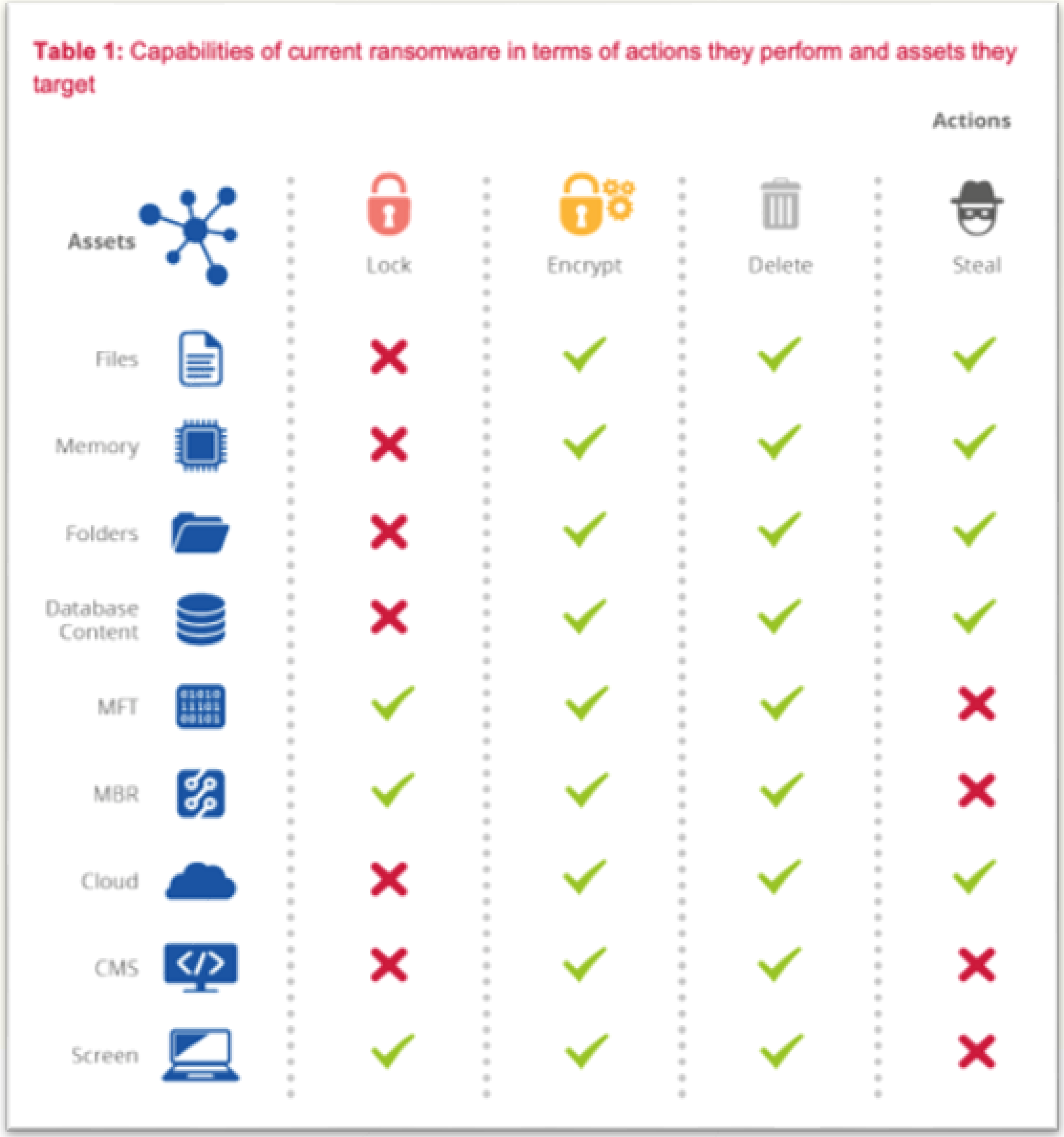


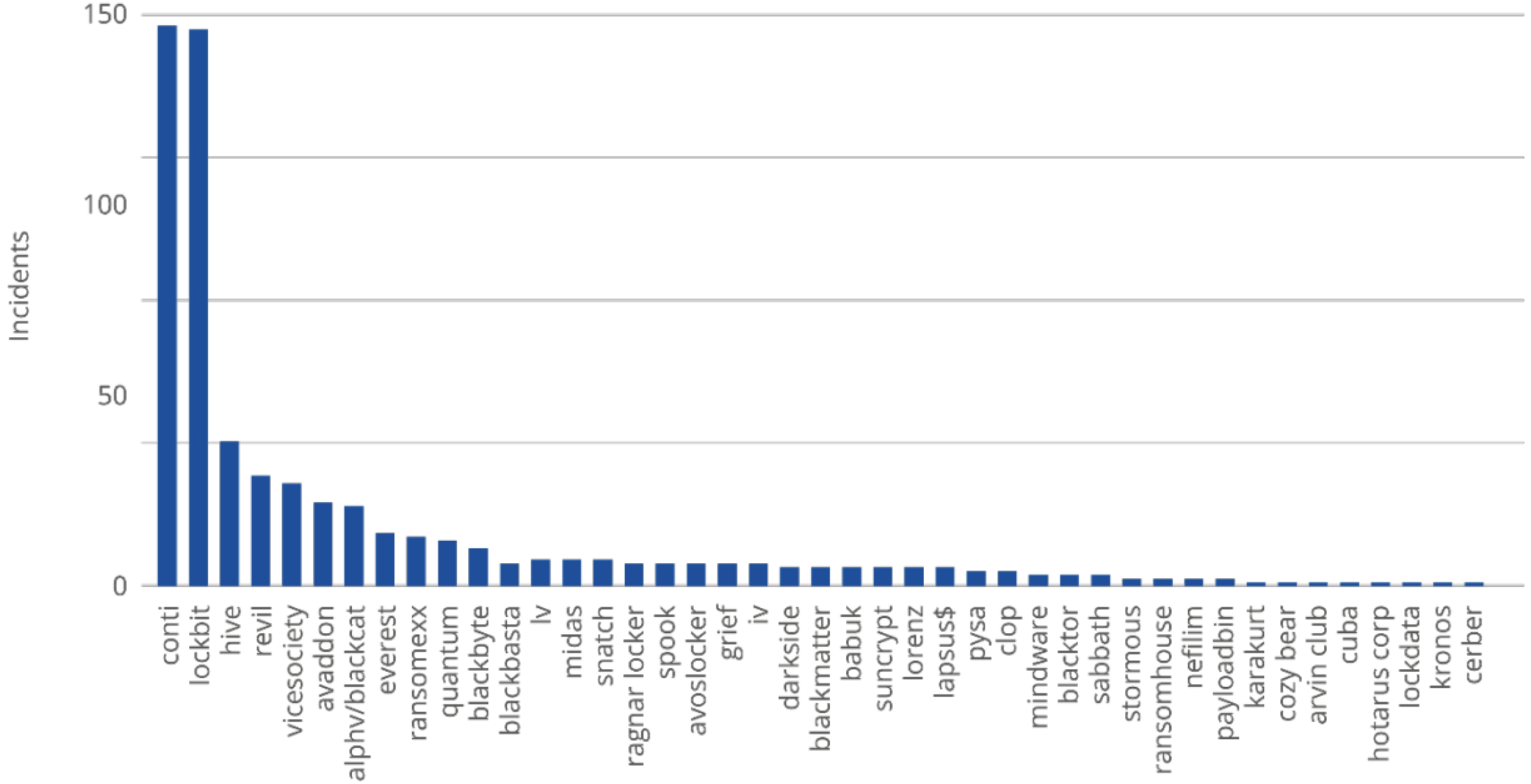
Table 1: Capabilities of current ransomware in terms of actions they perform and assets they target

Assets	Lock	Encrypt	Delete	Steal
Files	✗	✓	✓	✓
Memory	✗	✓	✓	✓
Folders	✗	✓	✓	✓
Database Content	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Cloud	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Screen	✓	✓	✓	✗

https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

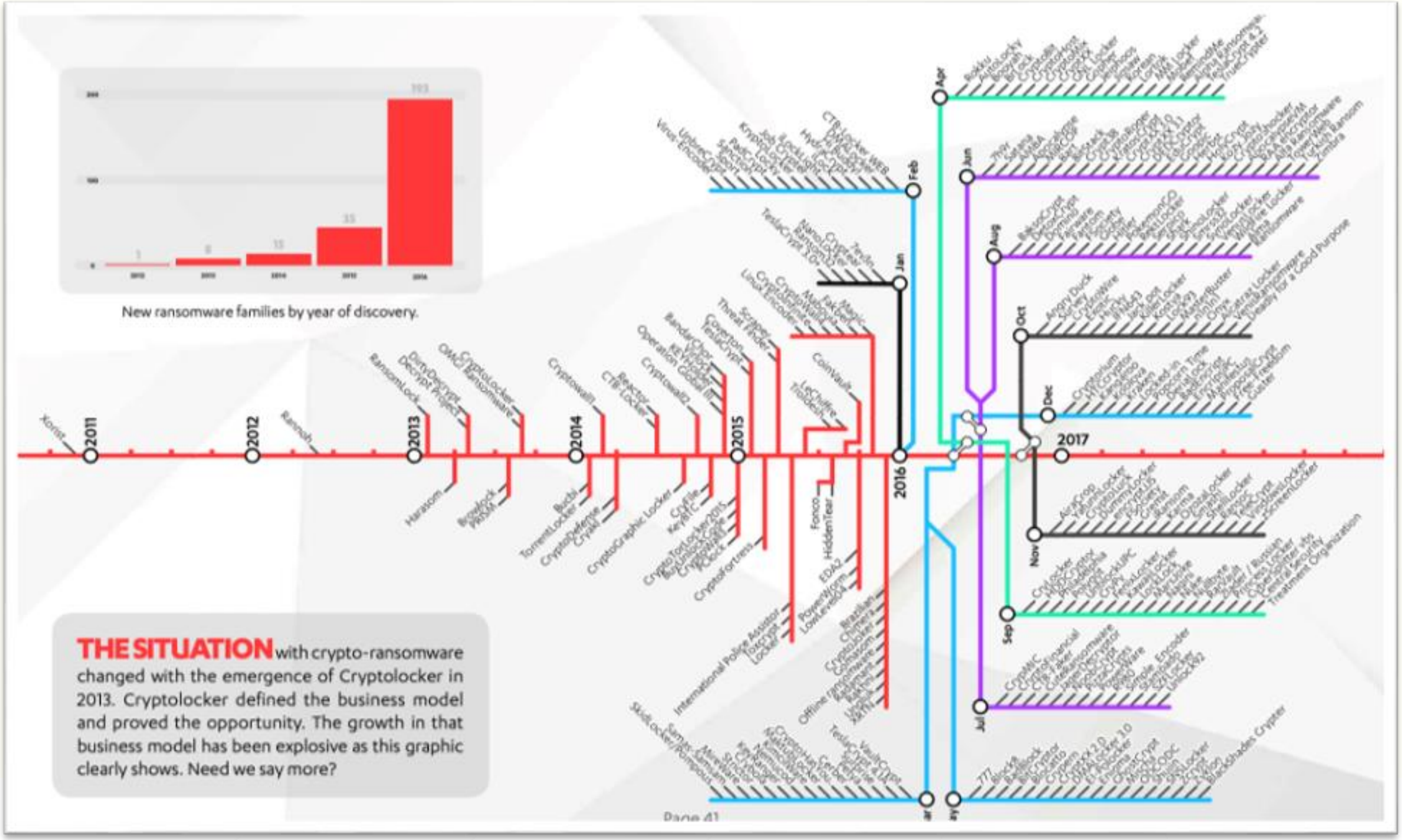
Ransomware - 2

Figure 4: Number of ransomware incidents caused by each threat actor



https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

Ransomware - 3

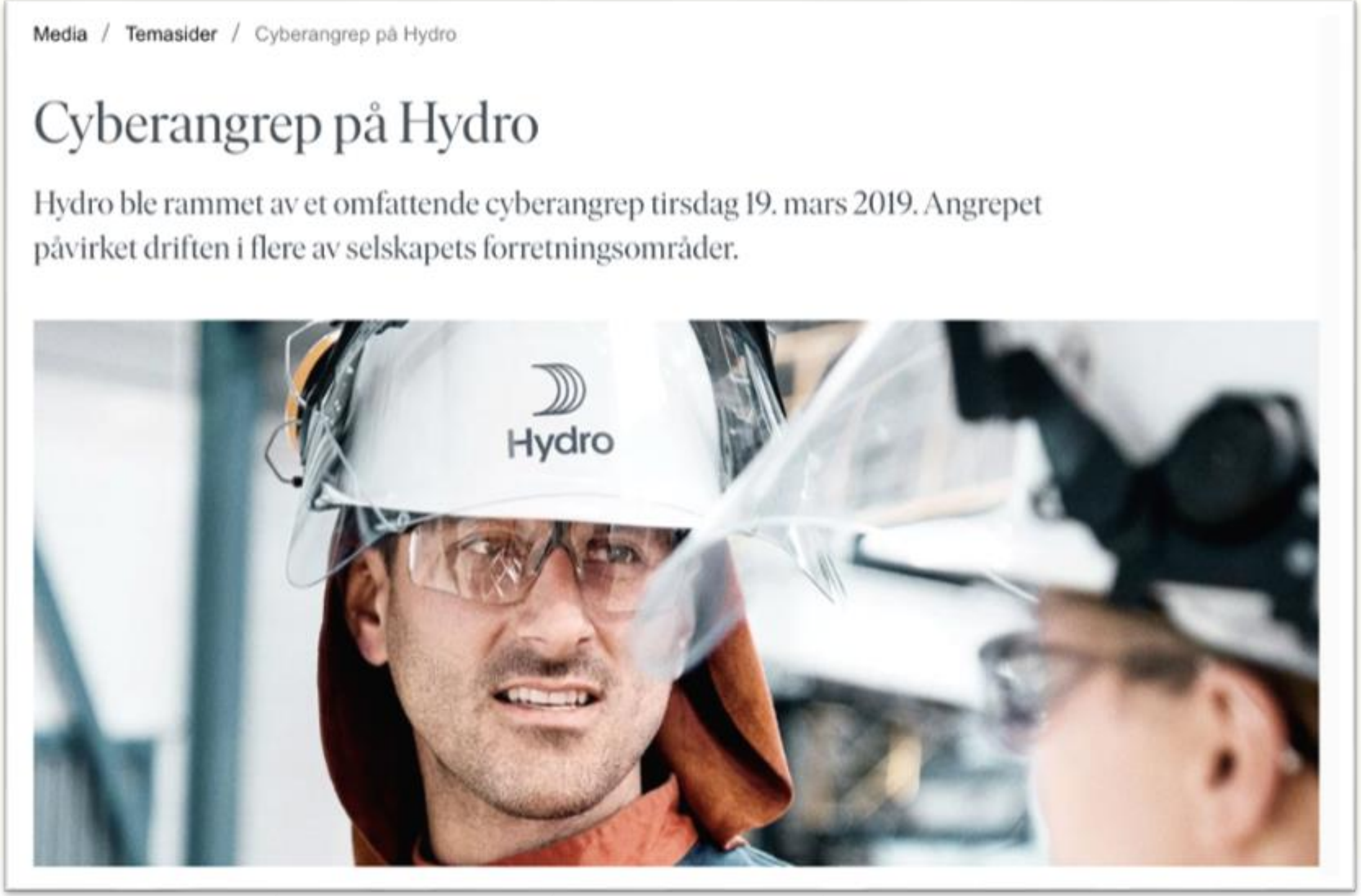


New ransomware families by year of discovery.

THE SITUATION with crypto-ransomware changed with the emergence of Cryptolocker in 2013. Cryptolocker defined the business model and proved the opportunity. The growth in that business model has been explosive as this graphic clearly shows. Need we say more?

https://blog.f-secure.com/wp-content/uploads/2019/10/Cyber_Security_Report_2017.pdf

Ransomware - 4



Media / Temasider / Cyberangrep på Hydro

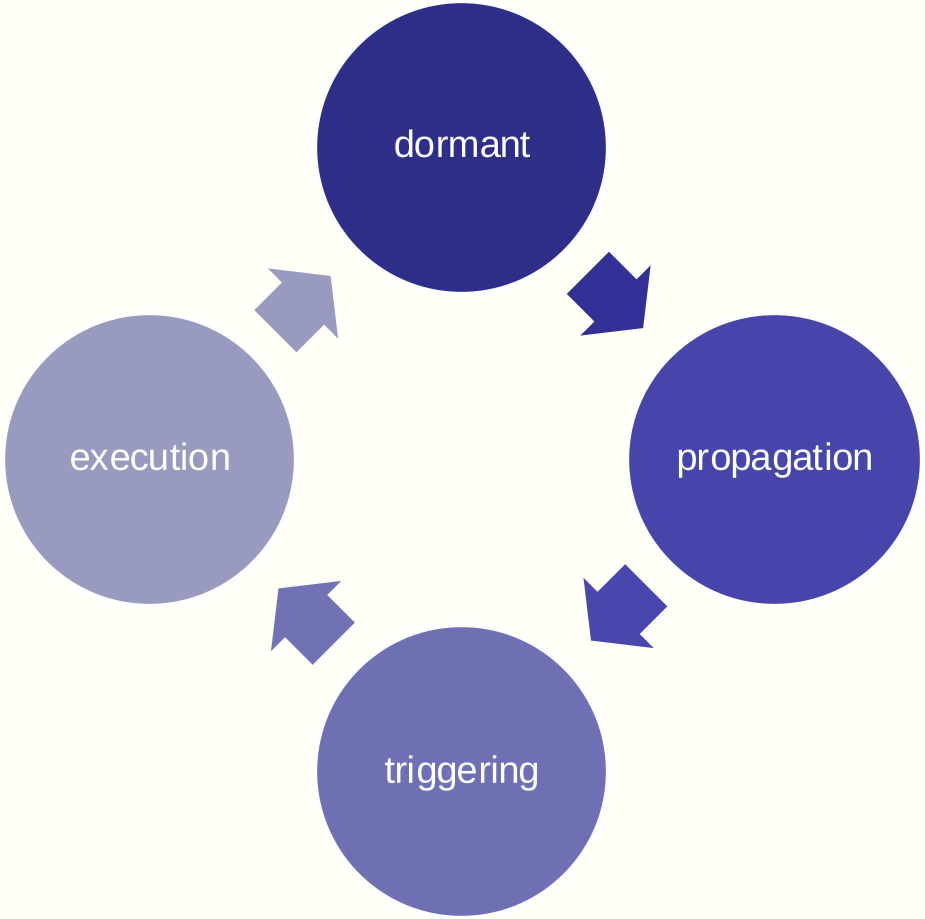
Cyberangrep på Hydro

Hydro ble rammet av et omfattende cyberangrep tirsdag 19. mars 2019. Angrepet påvirket driften i flere av selskapets forretningsområder.

https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Viruses

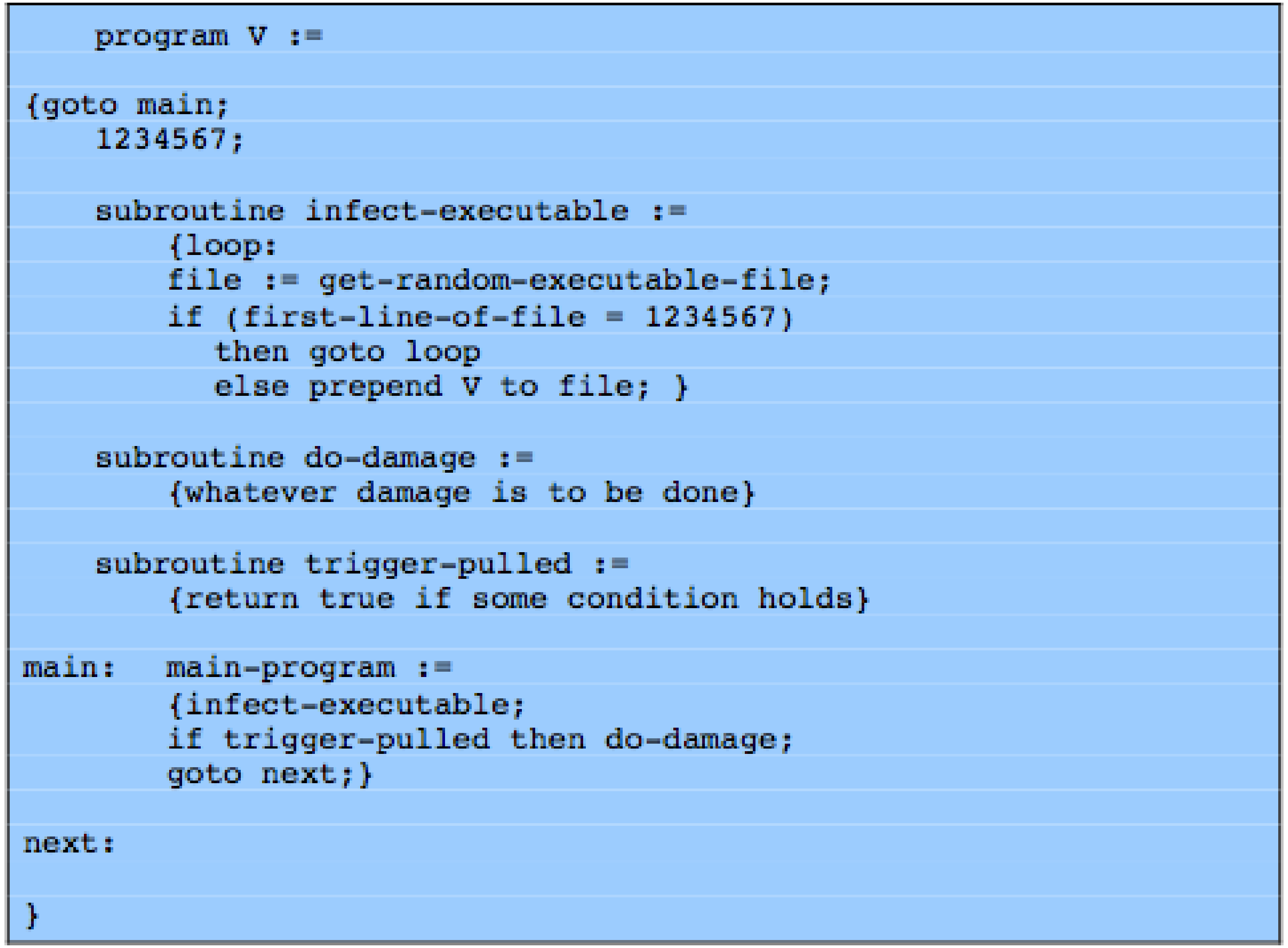
- Piece of software that infects programs
  - modifying them to include a copy of the virus
  - hence, it executes secretly when host program is run
- Specific to operating system and hardware
  - taking advantage of their details and weaknesses
- A typical virus goes through phases of:
  - dormant
  - propagation
  - triggering
  - execution



Virus Structure

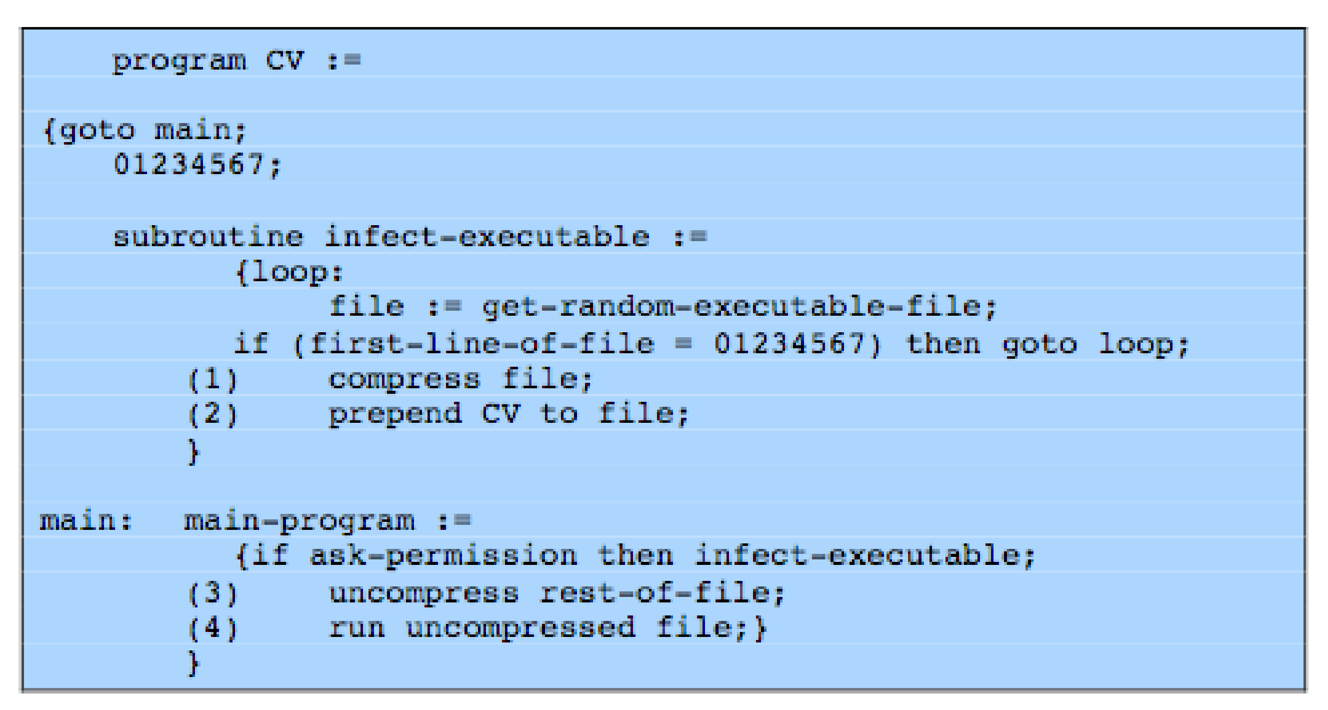
- Components:
  - infection mechanism - enables replication
  - trigger - event that makes payload activate
  - payload - what it does, malicious or benign
- Prepended / postpended / embedded
- When infected program invoked, executes virus code then original program code
- Can block initial infection (difficult)
- Or propogation (with access controls)

Virus Structure

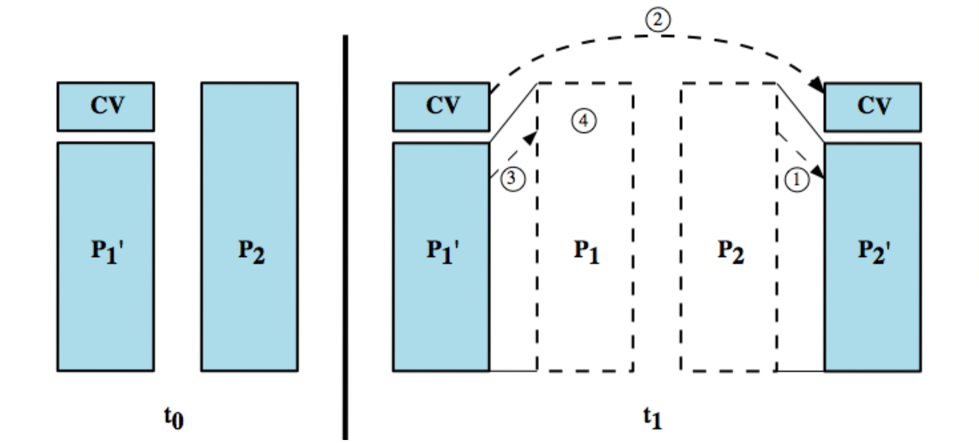


```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
           then goto loop
           else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Compression Virus



```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
           {loop:
                file := get-random-executable-file;
           if (first-line-of-file = 01234567) then goto loop;
        (1)     compress file;
        (2)     prepend CV to file;
        }

main:   main-program :=
           {if ask-permission then infect-executable;
        (3)     uncompress rest-of-file;
        (4)     run uncompressed file;}
        }
```



Virus Classification

- Boot sector
- File infector
- Macro virus
- Encrypted virus
- Stealth virus
- Polymorphic virus (change appearance)
- Metamorphic virus (change appearance and behavior)

Macro Virus

- Became very common in mid-1990s since
  - platform independent
  - infect documents
  - easily spread
- Exploit macro capability of office apps
  - executable program embedded in office doc
  - often a form of Basic
- More recent releases include protection
- Recognized by many anti-virus programs

E-Mail Viruses - 1

- One of the primary target for attackers
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - and does local damage
- Then saw versions triggered reading email
- Hence, much faster propagation

E-Mail Viruses – 2

- E-Mail virus uses social engineering tactics to lure users in opening emails

- Generally, email virus arrives as executable files attached to fake emails

- It may contain payload than can carry different malware or backdoor to infect the machine

Virus Countermeasures

- Prevention - ideal solution but difficult
- Realistically need:
  - detection
  - identification
  - Removal
- If detect but can’t identify or remove, must discard and replace infected program

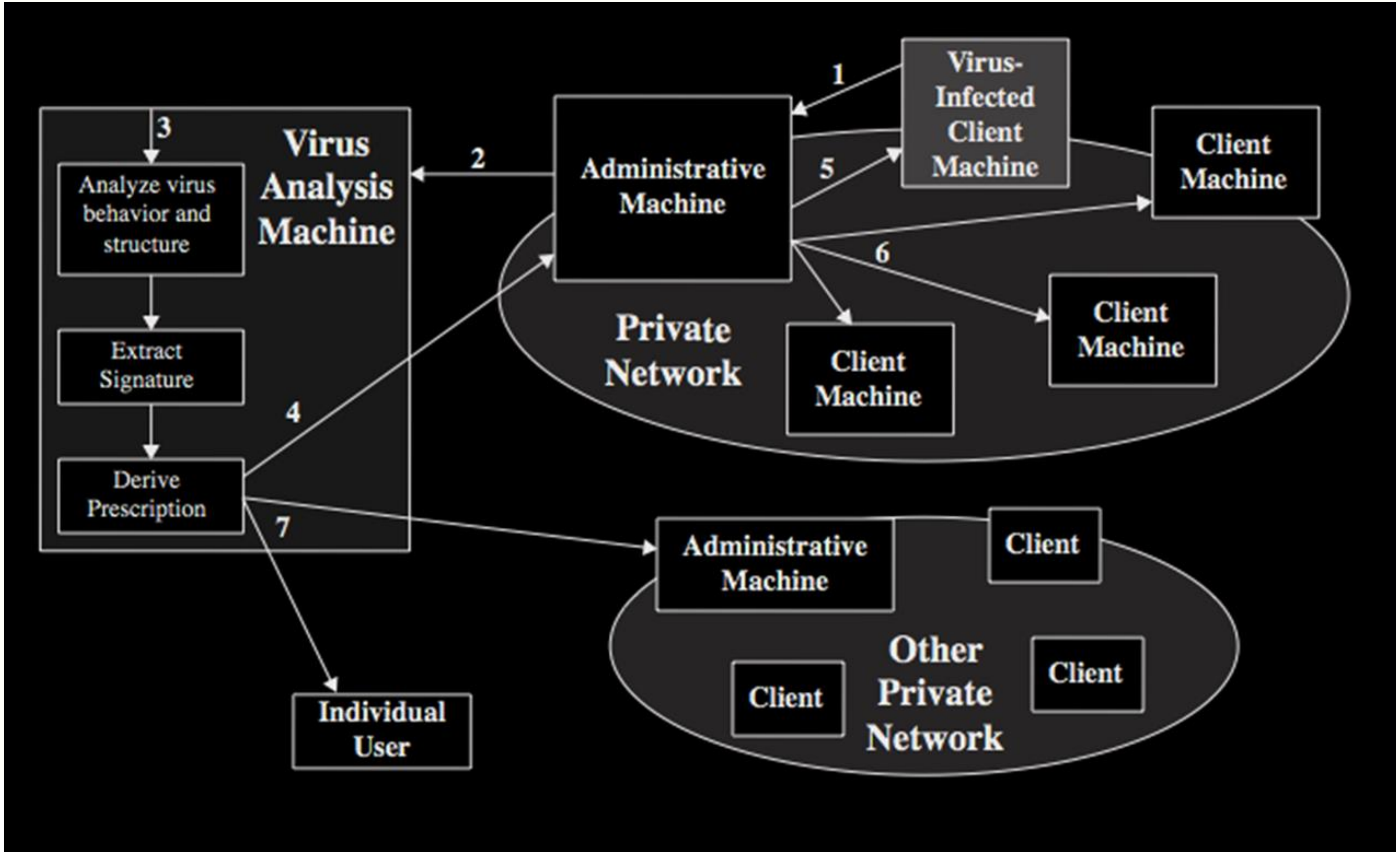
Anti-Virus Evolution

- Virus & antivirus tech have both evolved
- Early viruses simple code, easily removed
- As become more complex, so must the countermeasures
- Generations
  - first - signature scanners
  - second - heuristics
  - third - identify actions
  - fourth - combination packages

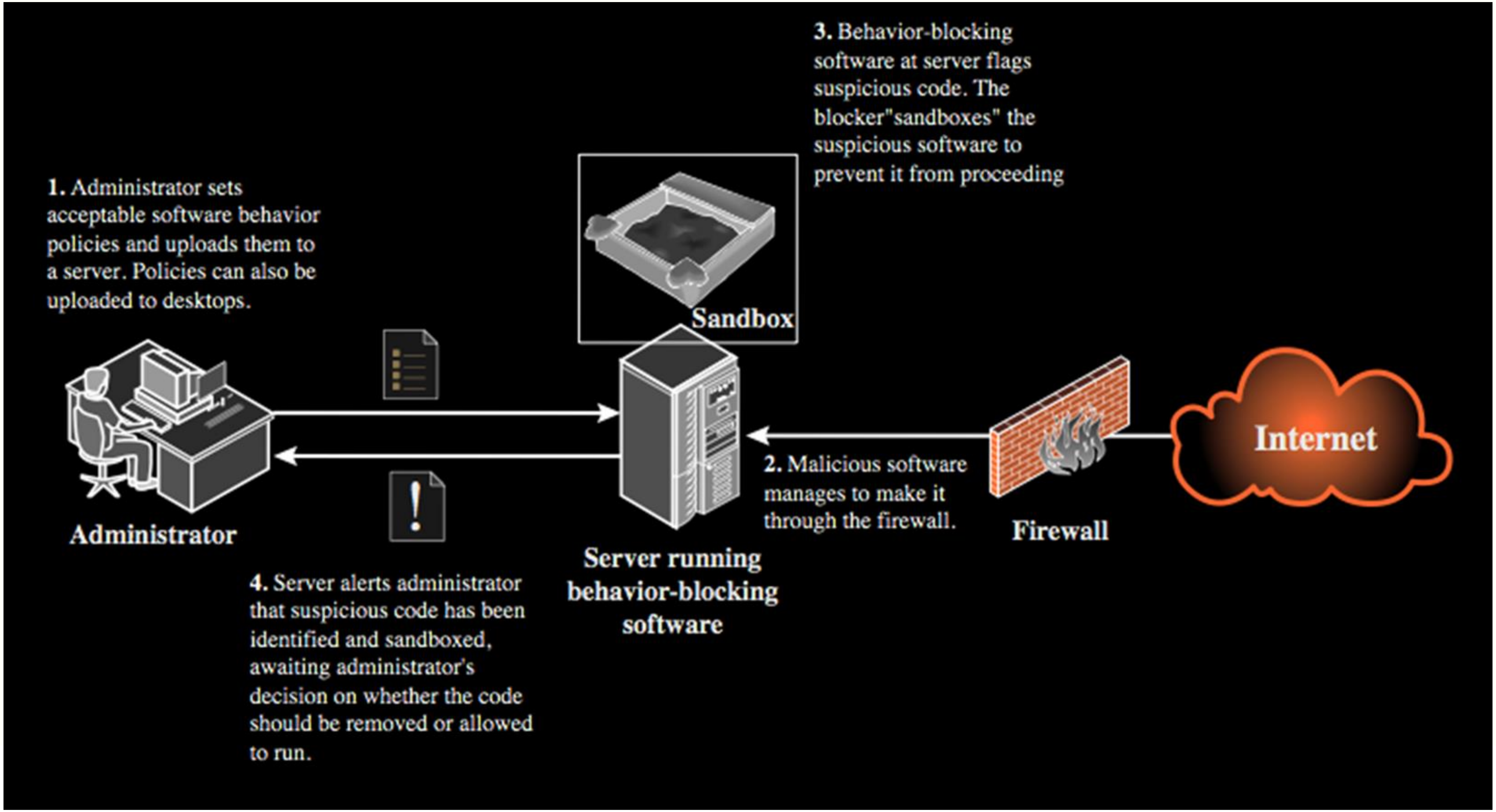
Generic Decryption (GD)

- Runs executable files through GD scanner:
  - CPU emulator to interpret instructions
  - virus scanner to check known virus signatures
  - emulation control module to manage process
- Lets virus decrypt itself in interpreter
- Periodically scan for virus signatures
- Issue is long to interpret and scan
  - tradeoff chance of detection vs time delay

Digital Immune System



Behavior-Blocking Software



1. Administrator sets acceptable software behavior policies and uploads them to a server. Policies can also be uploaded to desktops.

2. Malicious software manages to make it through the firewall.

3. Behavior-blocking software at server flags suspicious code. The blocker"sandboxes" the suspicious software to prevent it from proceeding

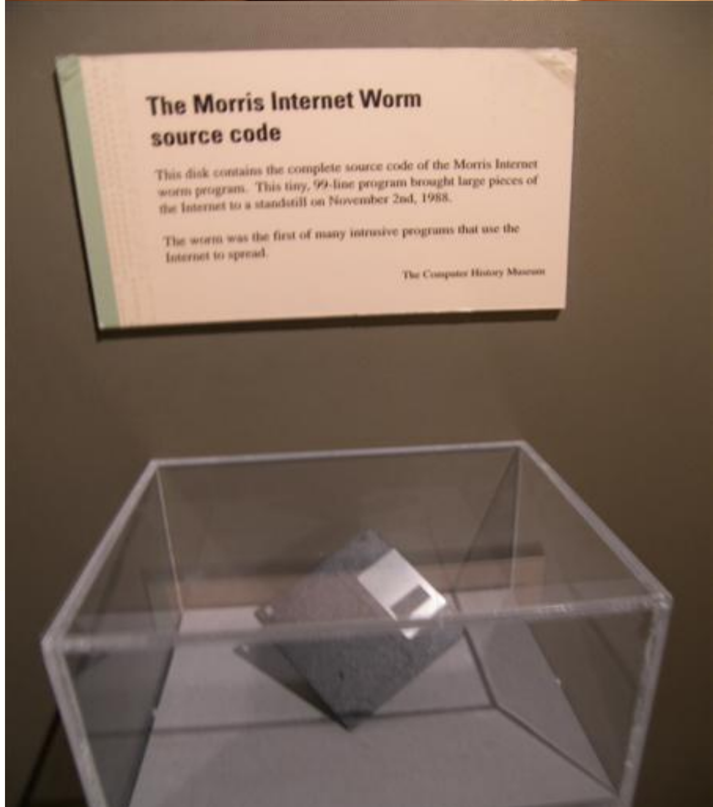
4. Server alerts administrator that suspicious code has been identified and sandboxed, awaiting administrator's decision on whether the code should be removed or allowed to run.

Worms

- Replicating program that propagates over net
  - using email, remote exec, remote login
- Has phases like a virus:
  - dormant, propagation, triggering, execution
  - propagation phase: searches for other systems, connects to it, copies self to it and runs
- May disguise itself as a system process
- Concept seen in Brunner’s “Shockwave Rider”
- Implemented by Xerox Palo Alto labs in 1980’s

Morris Worm

- One of best-known worms
- Released by Robert Morris in 1988
- Various attacks on UNIX systems
  - cracking password file to use login/password to logon to other systems
  - exploiting a bug in the finger protocol
  - exploiting a bug in *sendmail*
- If succeed have remote shell access
  - sent bootstrap program to copy worm over



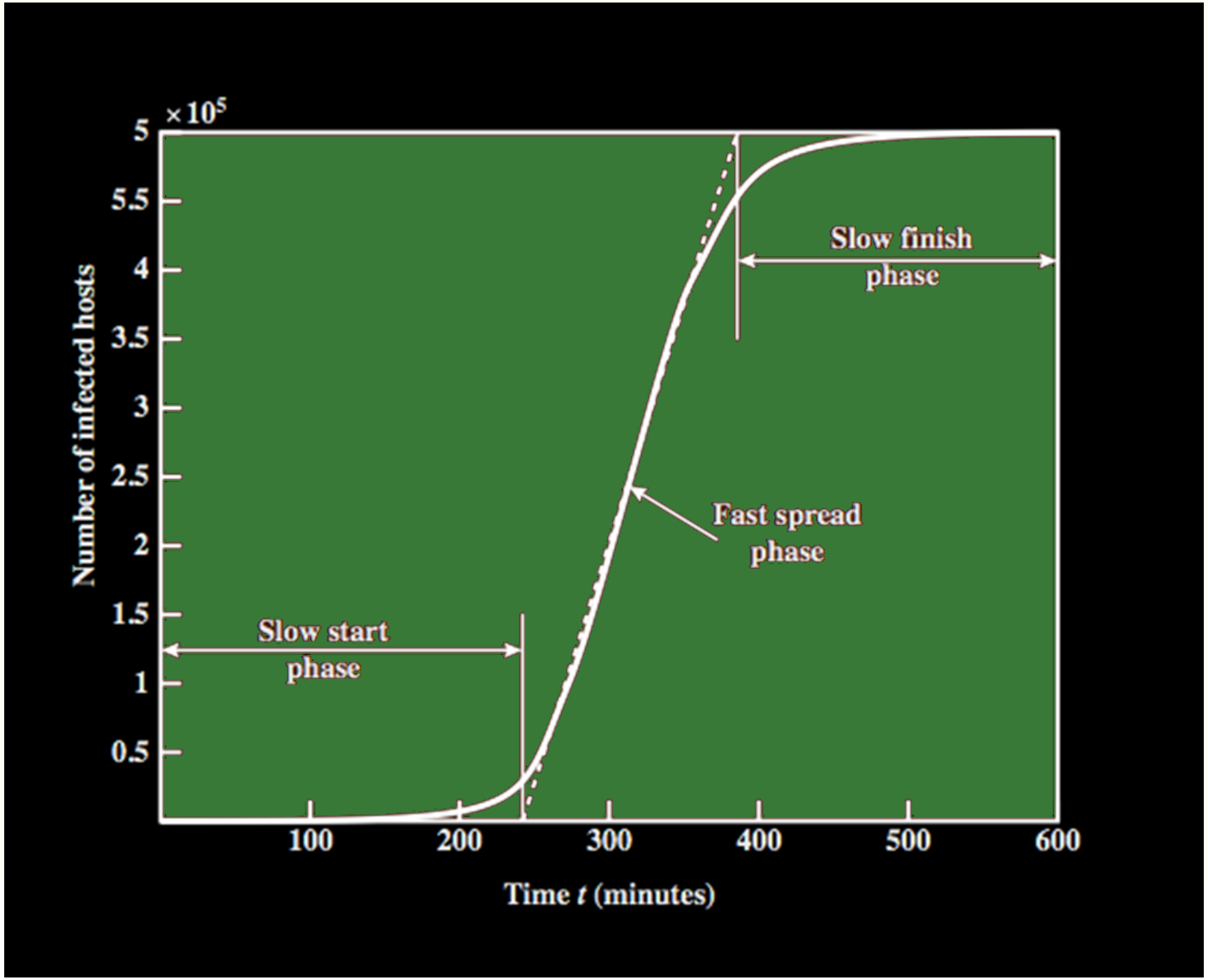
The Morris Internet Worm
source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

The Computer History Museum

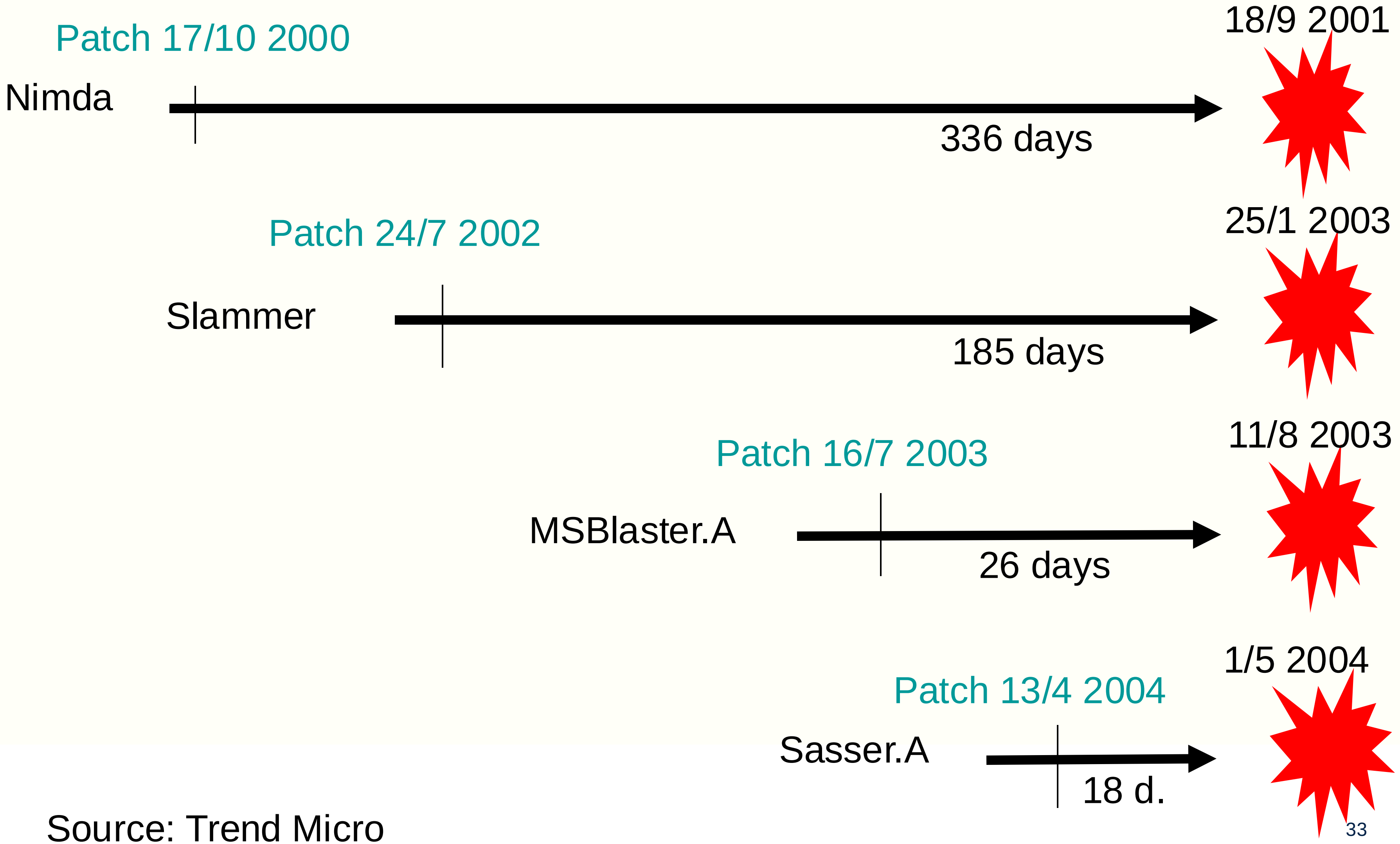
Worm Propagation Model



"Recent" Worm Attacks

- Code Red
  - July 2001 exploiting MS IIS bug
  - probes random IP address, does DDoS attack
- Code Red II variant includes backdoor
- SQL Slammer
  - early 2003, attacks MS SQL Server
- Mydoom
  - mass-mailing e-mail worm that appeared in 2004
  - installed remote access backdoor in infected systems
- Warezov family of worms
  - scan for e-mail addresses, send in attachment

Patch-exploit cycle



Patch 17/10 2000

Nimda

336 days

18/9 2001

Patch 24/7 2002

Slammer

185 days

25/1 2003

Patch 16/7 2003

MSBlaster.A

26 days

11/8 2003

Patch 13/4 2004

Sasser.A

18 d.

1/5 2004

Source: Trend Micro

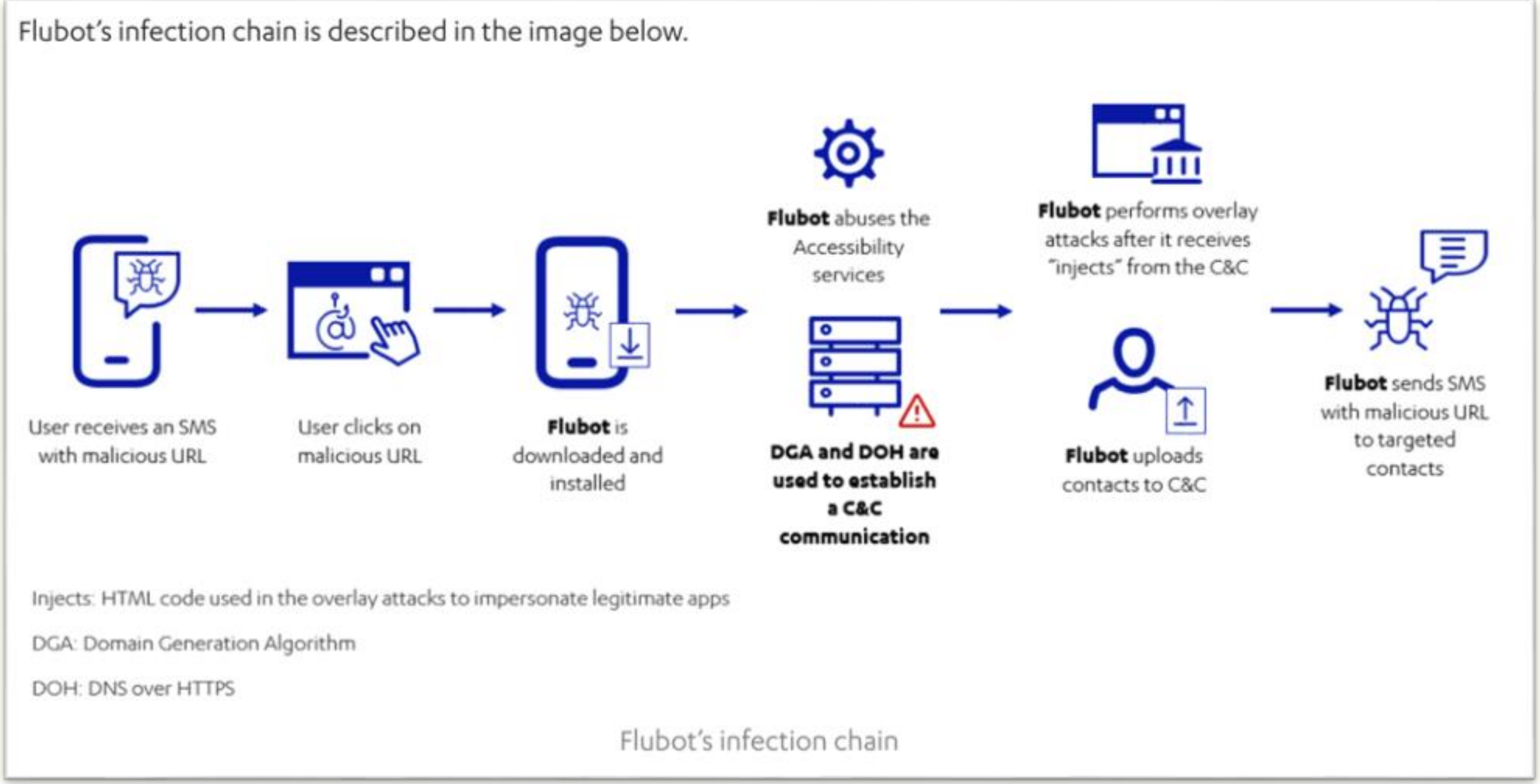
Worm Technology

- Multiplatform
- Multi-exploit
- Ultrafast spreading
- Polymorphic (how they look)
- Metamorphic (what they do)
- Transport vehicles
- Zero-day exploit

Mobile Phone Worms

- First appeared on mobile phones in 2004
    - target smartphone which can install s/w
- They communicate via Bluetooth or MMS
- To disable phone, delete data on phone, or send premium-priced messages
- CommWarrior, launched in 2005
    - replicates using Bluetooth to nearby phones
    - and via MMS using address-book numbers
- Worms on Android platform increasing
    - Difficult to push malicious app via App stores
    - Exploit social engineering tactics to lure user in installing malicious app
    - Android fragmentation issue

Android Banking Trojan Example



Flubot's infection chain is described in the image below.

User receives an SMS with malicious URL

User clicks on malicious URL

Flubot is downloaded and installed

Flubot abuses the Accessibility services

DGA and DOH are used to establish a C&C communication

Flubot performs overlay attacks after it receives "injects" from the C&C

Flubot uploads contacts to C&C

Flubot sends SMS with malicious URL to targeted contacts

Injects: HTML code used in the overlay attacks to impersonate legitimate apps

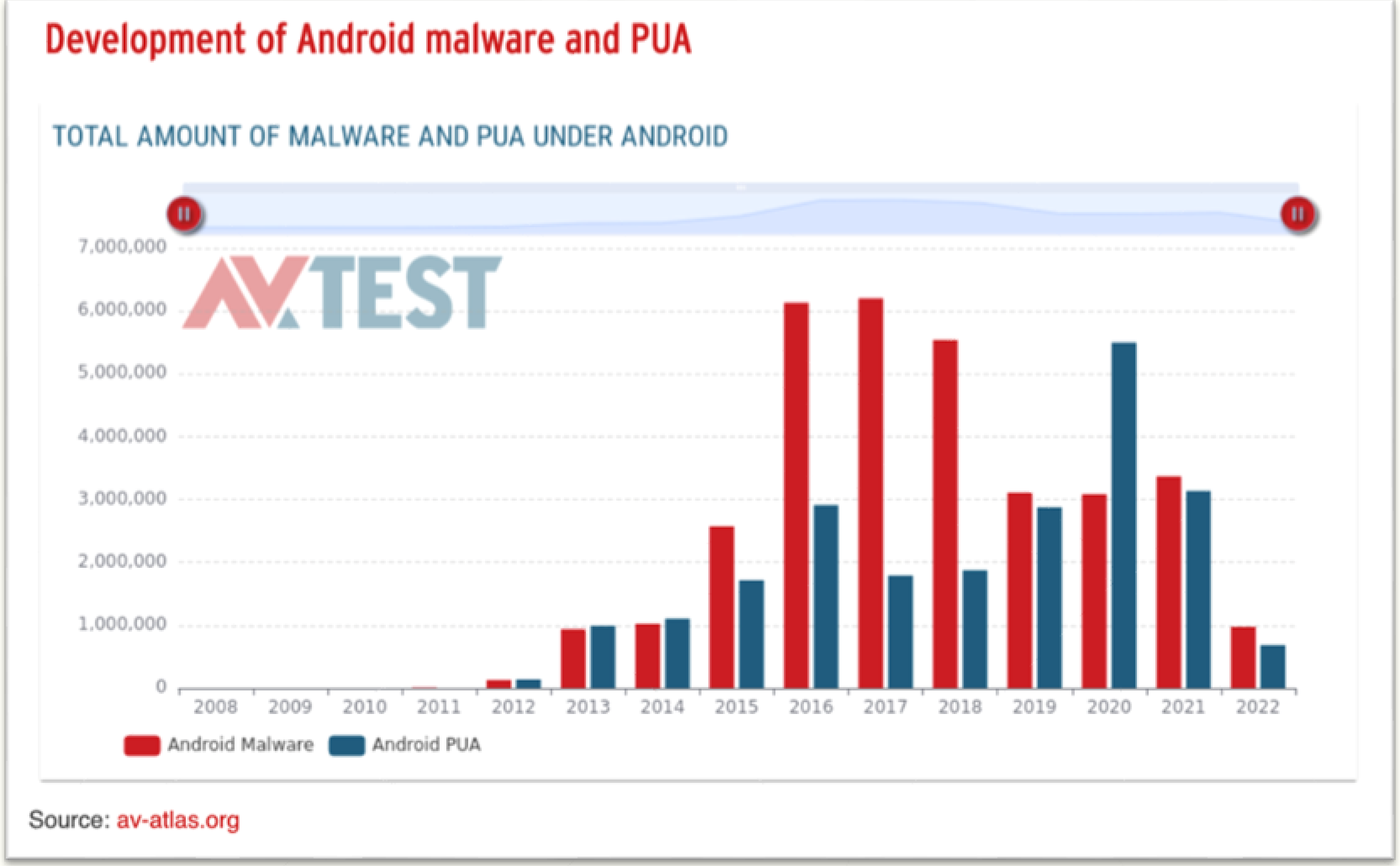
DGA: Domain Generation Algorithm

DOH: DNS over HTTPS

Flubot's infection chain

https://blog.f-secure.com/flubot_doh_tunneling/

Development of Android Malware



Development of Android malware and PUA

TOTAL AMOUNT OF MALWARE AND PUA UNDER ANDROID

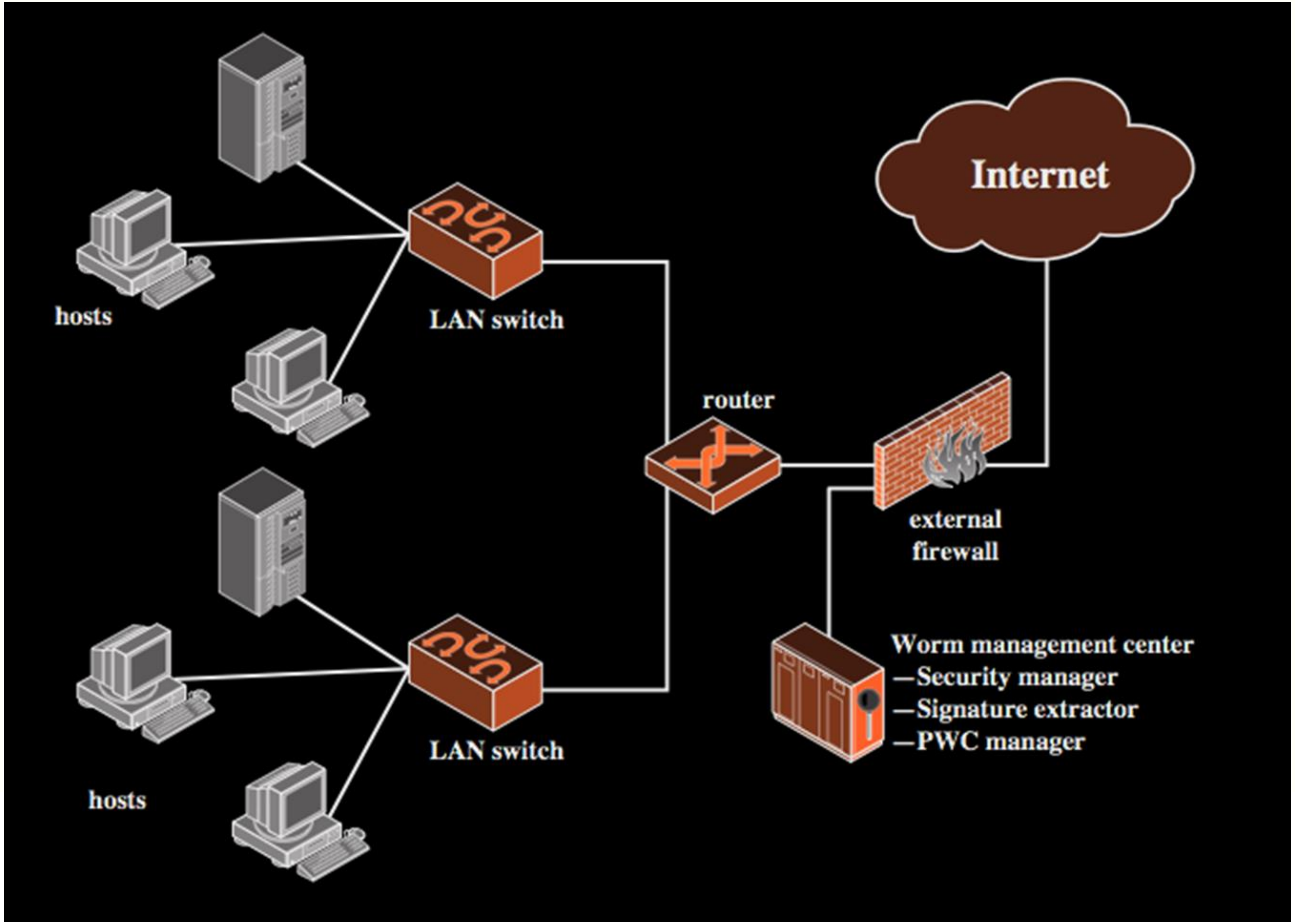
Source: av-atlas.org

https://www.av-test.org/en/statistics/malware/

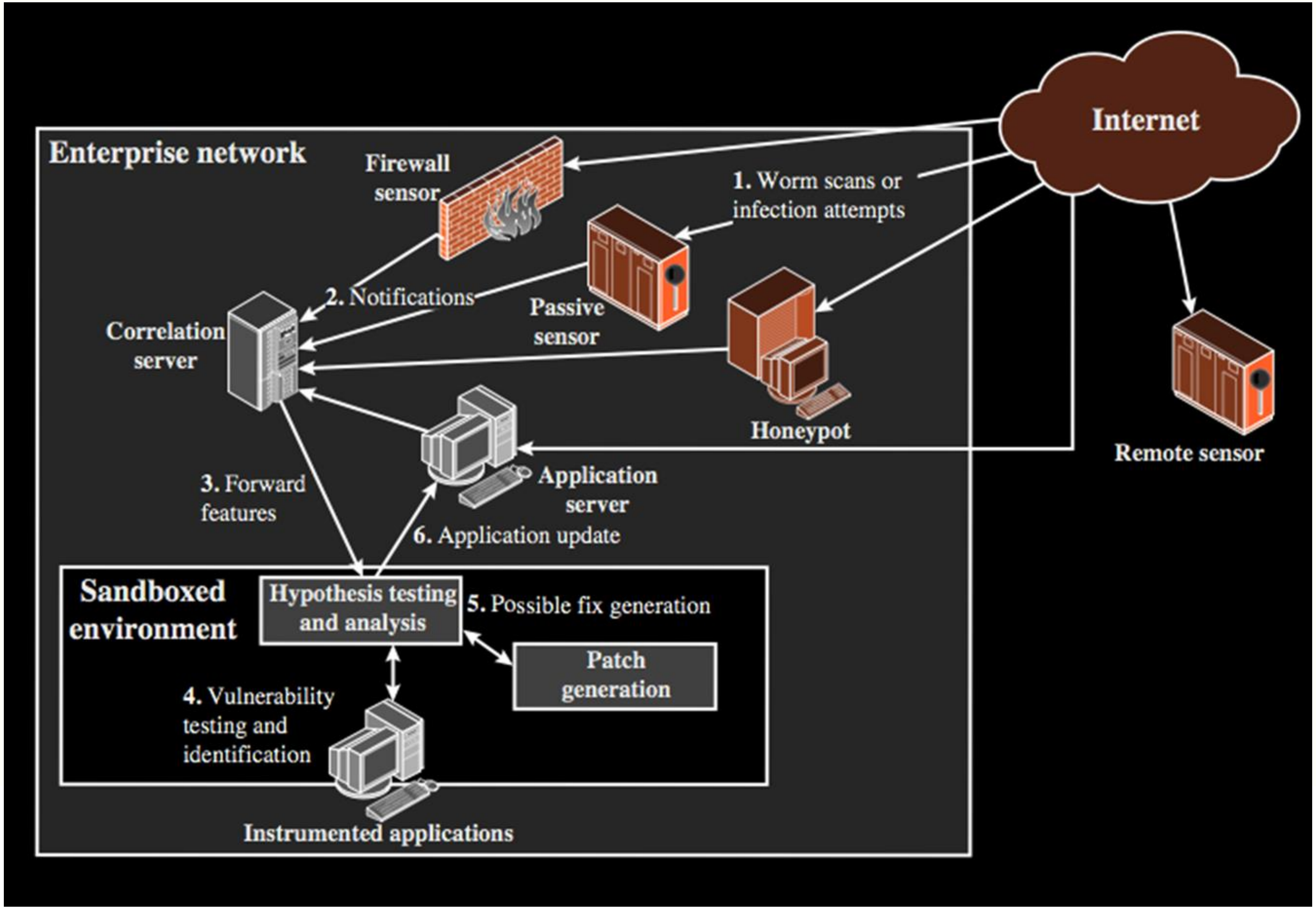
Worm Countermeasures

- Overlaps with anti-virus techniques
- Once worm on system A/V can detect
- Worms also cause significant net activity
- Worm defense approaches include:
  - signature-based worm scan filtering
  - filter-based worm containment (what does the code do?)
  - payload-classification-based worm containment (anomaly)
  - threshold random walk scan detection (is it a random scan?)
  - rate limiting and rate halting

Proactive Worm Containment



Network Based Worm Defense



Summary

- have discussed:
  - various malign programs
  - backdoor, logic bomb, trojan horse, zombie
  - viruses
  - worms
  - distributed denial of service attacks