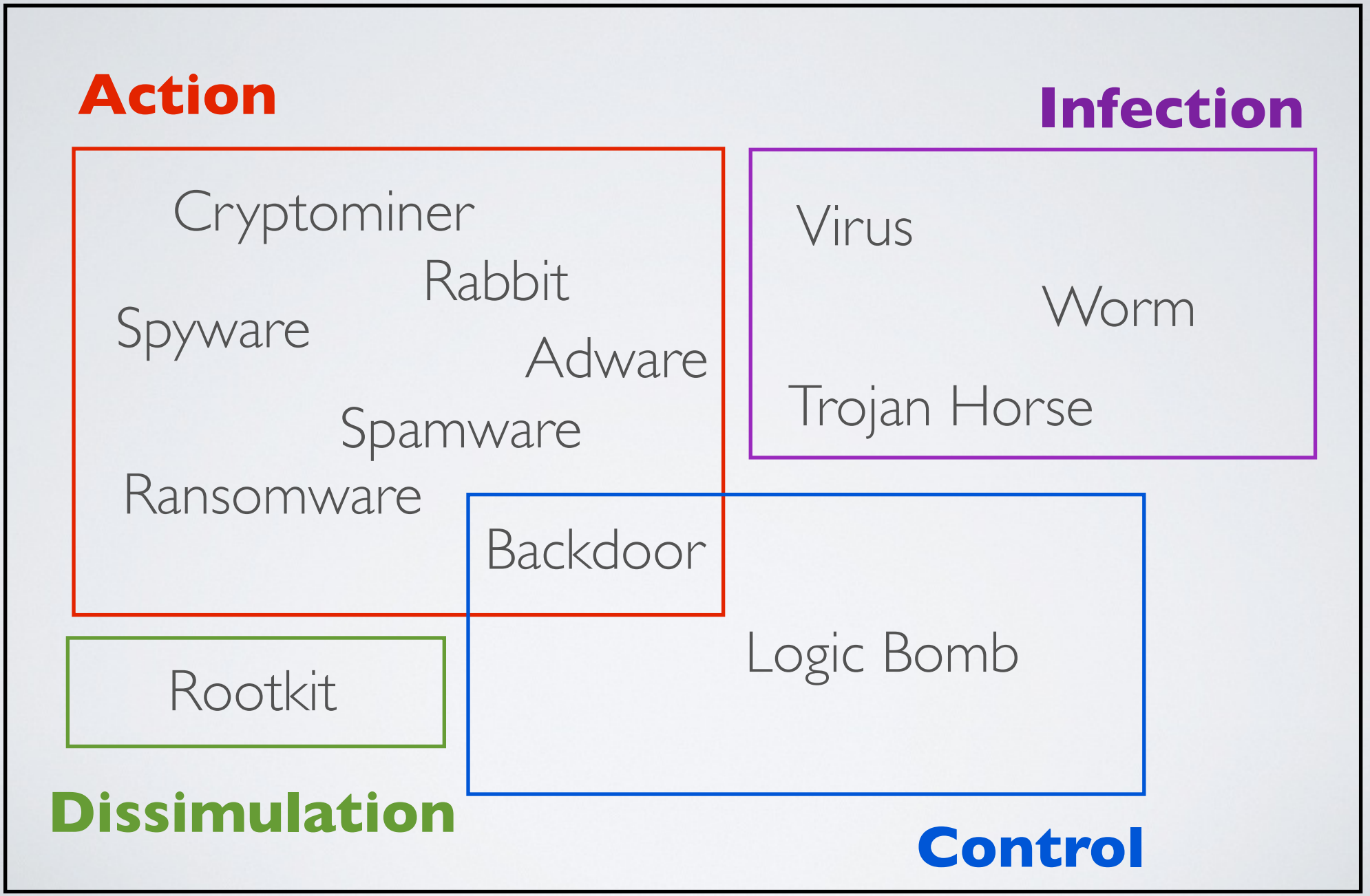
Malicious Code

Thierry Sans

Malware


Action
Infection
Cryptominer
Rabbit
Spyware
Adware
Spamware
Ransomware
Virus
Worm
Trojan Horse
Backdoor
Logic Bomb
Rootkit
Dissimulation
Control

Action

- performs unsolicited operations on the system

- **Rabbit** exhausts the hardware resources of a system until failure
- **Backdoor** allows an attacker to take control of the system bypassing authorization mechanisms
- **Spyware** collects information
- **Spamware** uses the system to send spam
- **Ransomware** restricts access to system's data and resources and demands for a ransom
- **Adware** renders unsolicited advertisement

Dissimulation

- avoid detection by anti-malware programs

Rootkit hides the existence of malicious activities

Infection

- penetrate a system and spread to others

Replication

- copy itself to spread

- **Virus** contaminates existing executable programs
- **Worm** exploits a service's vulnerability

Subterfuge

- based on user's credulity

- **Trojan Horse** tricks the user to execute the malicious code

Control

- activate the malicious code

- **Backdoor** communicates with command & control servers allowing an attacker to control the virus
- **Logic Bomb** activates the malicious code when certain conditions are met on the system

The history of malicious code

Chronology

- 70's - The era of the first self-replicating programs
- 80's - The era of maturity and first pandemics
- 90's - The era of self-modifying virus and macro viruses
- 00's - The era of Trojan horses and internet worms
- 10's - The era of cyber-warfare viruses

70's - The era of the first self-replicating programs

The era of the first self-replicating programs (70's)

ANIMAL (a popular game)

- Replication through the filesystem
- No effect

Simple Joke

Creeper (and **Reaper**) on Tenex OS (Arpanet)

- Replication through a modem and copied itself to the remote system
- Displays the message
  `I'M THE CREEPER : CATCH ME IF YOU CAN`

Disruptive

The **Rabbit** program

- Replication through the filesystem
- Reduces system performance till crashing

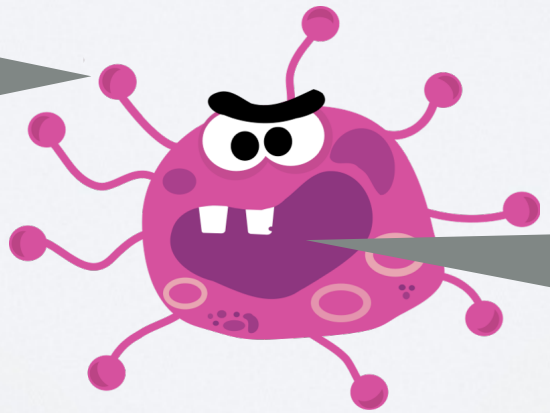
Destructive

Anatomy of a Virus

A **virus** can be

- a malicious code embedded in an existing program and replicates itself by infecting other programs through the filesystem or the network
- a program that exists by itself and replicates through the filesystem or network

Infection vector
how the virus penetrate the system



The payload
what the virus does

80's - The era of maturity and first pandemics

1987 - the beginning of pandemics

Jerusalem (MS-DOS)

- Destroys all executable files on infected machines upon every occurrence of Friday the 13th

SCA (Amiga)

- Displays a text every 15th boot
- 40% of the Amiga owners were infected

Christmas Tree EXEC (IBM/PC)

- Displays a snow flow animation
- Paralyzed several international computer networks in December 1987

The first anti-virus softwares (end of 80's)

Virus scanner (detection)

- Signature based -
  Using a signature database of existing viruses
- Behavior based
  Looking for suspicious code patterns that can be used by viruses

Virus removal tools (sanitation)

- Cleaning the memory and the filesystem

Avoiding detection

Cascade (1987)

- The virus encrypts itself with a cryptographic key and changes this key when replicating itself

✓ Each instance of the virus does not look the same

➡ This is the emergence of polymorphic viruses

90's - The era of self-modifying virus and macros viruses

The era of self-modifying virus (90's)

The **Chameleon** family (1990)

Ply (1996)

- DOS 16-bit based complicated polymorphic virus with built-in permutation engine

Anatomy of a "polymorphic" virus

A **polymorphic virus** mutates when replicating (but keeps the original algorithm intact)

- By using cryptography
- By injecting garbage code
- By doing permutations within certain instructions or block of instructions
- By using code obfuscation technique

How to detect it?

➡ By detecting code patterns used for the self-modification

Macro Viruses

A **macro virus** is written in scripting languages used by some office applications (can be cross-platform)

- Written in VBS, embedded in a MS-office document, activated when the document is open (autoload function)

Concept (1995)

Melissa (1999)

- March 26 1999, Melissa shut down e-mail systems that got clogged with infected e-mails

00's - The era of Trojan horses and internet worms

Anatomy of a Trojan horse

A **Trojan horse** is a program that disguise itself as a legitimate program or file

➡ In most cases, Trojan horses replicate themselves through emails

The big stars among trojan horses

VBS/Loveletter ILOVEYOU (2000)

- Caused 5.5 to 10 billion dollars in damage

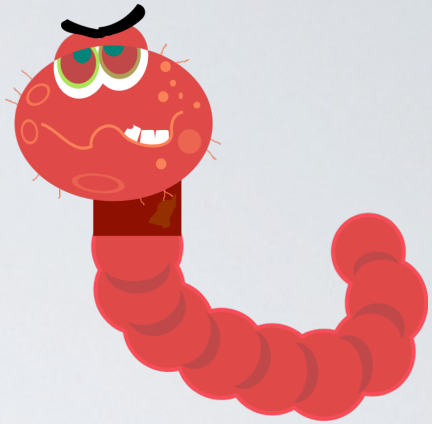
Sobig (2002)

- Sobig.F set a record in sheer volume of e-mails

MyDoom (2002)

- Broke the record set by Sobig.F

Anatomy of a worm



A **worm** exploits a security flaw (often of a network service) to infect the machine and replicates itself through the network

- ➡ Very fast infection (does not need the user to be activated)
- ➡ Has a payload as well (more or less harmful)

Factors

- The wide adoption of internet
- The global network is a good medium for virus pandemics
- The multiplication of internet applications and services
- Fast publication of program vulnerabilities
- Slow release of corrective patches
- Slower adoption of these patches (not automatic)

Code-Red (2001)

- Exploits a security flaw (buffer overflow) of Microsoft IIS web server (MS01-033) patched one month earlier
- In few days, 359 000 machines infected

Nimda (2001)

- Exploits another security flaw of MS-IIS
- The Internet's most widespread worm so far (the most part of the infection was done in 22min)

Klez (2001)

- Exploits a security flaw of Microsoft Internet Explorer layout engine used by Outlook and IE
- Infection through email attachment however the user does not have to open this attachment to get infected

SQL-Slammer (also called **Sapphire**) (2002)

- Exploits a security flaw in MS-SQL servers for which a patch had been released six months earlier (MS02-039)
- Infected 75,000 machines in 10 minutes causing caused a massive denial of service and dramatically slowed down global Internet traffic

Sasser (2002)

- Exploiting a buffer overflow of Microsoft LSASS on Windows 2000 and XP systems
- Many companies had to shut down their services

Blaster (also known as **Lovesan**) (2003)

- Exploits a security flaw in DCOM-RPC services on Windows 2000 and XP
- Was supposed to do SYN flood on August 15, 2003 against port 80 of windowsupdate.com

Welchia (also known as **Nachia**) (2003)

- Exploits the same security flaw than Blaster
- Corrects the security flaw by patching the system

Conficker (2008)

- Exploits a security flaw in NetBIOS
- Disables auto-update
- Embeds a dictionary password cracker and a backdoor to turn the machine into a "bot"
- Believed to be originated from Ukraine and/or Russia

The first web-worm

Santy (2004)

- Exploited a vulnerability in phpBB and used Google in order to find new targets
- It infected around 40 000 sites before Google filtered the search query used by the worm, preventing it from spreading

The emergence of XSS worms

An **XSS worm** exploits a cross site scripting (XSS) within a website (see lecture on *web security*)

Samy (2005)

- Targeting MySpace (social network)

JTV.worm (2008)

- Targeting Justin.tv (video casting)

Twitter.worm (2010)

- Targeting Twitter (micro-blogging)

10's - The era of cyber-warfare malware & Ransomware & IoT malware

The first cyber-warfare virus

W32.Dozor (July 2009)

- A virus that created a botnet dedicated to perform a DDoS attack South Korea and US government website on July 4th
- Believed to be originated from China and/or North Korea

Stuxnet (Sept 2010)

- A very sophisticated virus that targets SCADA systems (supervisory control and data acquisition)
- Believed that it took down 4000 nuclear centrifuges in Iran
- Believed to be originated from the USA and Israel

Flame also called **Skywiper** (May 2012)

- An *espionage* virus that embeds sophisticated spywares
- Believed to be originated from the USA (*Olympic Games* defense program)

Another trend - Ransomware

Reveton (2012)

- Displays a message from the law enforcement agency saying that you have pirated software and child pornography on your machine
- Ask you to pay a fine using a prepaid cash service

CryptoLocker (2013)

- Encrypt specific files on your machine with a 2048 RSA key
- Ask you to pay a ransom with Bitcoins

"Ransomware attacks grew by 500% in 2013 and turned vicious"

source : *Symantec Internet Security Threat Report 2014*

... and it turned vicious

WannaCry and **Petya** (2017)

- Use a vulnerability found in the NSA hacking toolkit leak
- Researcher have found a "kill switch"
- Paralyzed hospitals in UK and trains in Germany

Late 10's - the emergence of IoT malware and Cryptominers

Mirai (2016)

- Infects IoT devices
- Most powerful DDoS attacks to date

Coinhive (2018)

- Javascript embedded in website (either legitimately or not) and popular malware as well