Malware

Kc Udonsi

Malware

Action

Cryptominer

Rabbit

Spyware

Adware

Spamware

Ransomware

Backdoor

Infection

Virus

Worm

Trojan Horse

Rootkit

Logic Bomb

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

Basic 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

Prevalent Types

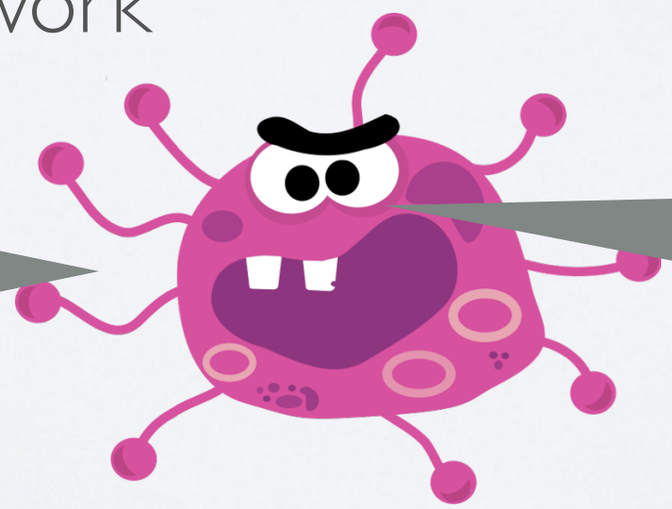
Viruses

➡ Anatomy of a virus

A **virus** can be

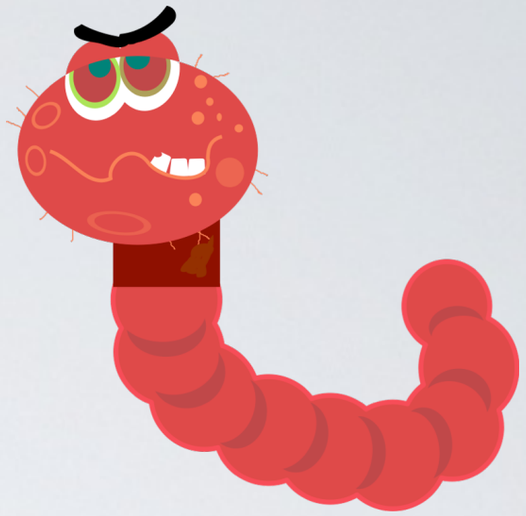
- a malicious code embedded in an existing program and replicates itself by infecting other programs through the filesystem or the network
- a program that exists by itself and replicates through the filesystem or network

Infection vector
how the virus penetrate the system



The payload
what the virus does

Worms



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)

Remote Administration Tool/ Trojan (RAT)

Basically a **remote administration tool** with

- stealth features
- and specific functionalities such as :
  - camera controller
  - hardware destroyer
  - password / credit card loggers
  - … and so on

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)

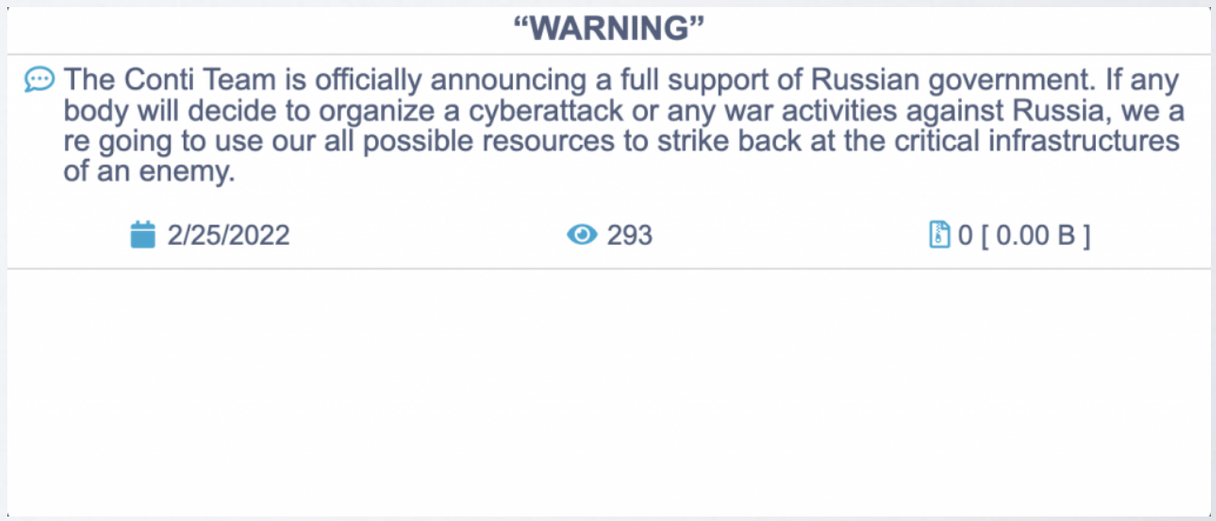
- Use a vulnerability found in the NSA hacking toolkit leak
- Researcher have found a "kill switch"
- Paralyzed hospitals in UK and trains in Germany

Ransomware as a Service (RaaS)

- Zeppelin (2019 - 2022); exploiting RDP & Firewall vulnerabilities
- Lockbit (2019 -)

Gangs

- e.g Conti



Components of Malware

Yep, it's modularized too …

- ➡ Downloaders and Launchers
- ➡ Stagers
- ➡ Persistence Mechanisms
- ➡ Command and Control or other payload

Techniques of Malware

Malicious Behaviour

- ➡ Hooking (IAT, Inline)
- ➡ Process Injection, Hollowing, Replacement
- ➡ Packing
- ➡ Memory Patching
- ➡ Obfuscation and Encryption

Cyber-warfare

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

Cyber threat activity related to the Russian invasion of Ukraine (cyber.gc.ca 2022)

Russian and Russia-linked cyber activity within Ukraine

We assess that Russian cyber operations have almost certainly sought to degrade, disrupt, destroy, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public's access to information. [3] Russian state-sponsored cyber threat actors will almost certainly continue to perform actions in support of the Russian military's strategic and tactical objectives in Ukraine.

Since the 2014 Russian annexation of Crimea, Ukraine has significantly improved its cyber security posture, including with recent assistance from European Union (EU) and Five Eyes (Australia, Canada, New Zealand, United Kingdom, and US or FVEY) governments and technology companies. [4]

Following Russia's invasion of Ukraine on February 24, 2022, likely Russian threat actors conducted several disruptive and destructive computer network attacks against Ukrainian targets, including Distributed Denial of Service (DDoS) attacks and the deployment of wiper malware against various sectors, including government, financial, and energy. Cyber operations have often coincided with conventional military operations.

To date, there are eight tracked malware families that Russia-linked cyber threat actors have used for destructive activity against Ukraine: WhisperGate/Whisperkill, FoxBlade (HermeticWiper), SonicVote (HermeticRansom), CaddyWiper, DesertBlade, Industroyer2, Lasainraw (IsaacWiper) and FiberLake (DoubleZero). [5]

In mid-April, Russian state-sponsored cyber threat actors launched four different variants of a new malware at various Ukrainian targets. Cyber security firms have attributed these attacks to a group known as Armageddon (aka Gamaredon/Shuckworm), which has been linked to Russia's Federal Security Service (FSB). [6]

Economics of Malware

Darkweb Commercialization

- "Kits" can be bought often with cryptocurrency and often includes support!
- Components can be bought commercial-off-the-shelf and integrated

Buy a RAT as a COTS*

BLACKSHADES NET (VPN INCLUDED!)

Blackshades NET has for several years been considered as simply the best RAT (Remote Administration Tool) on the market.
Its main purpose is to allow users to easily control clients from around the world.

BLACKSHADES STEALTH

The first RAT client to be coded in Java while the bin is C.
Blackshades Stealth is extremely fast & secure. All of your traffic data is encrypted with AES.
You can pull up the server's screen, webcam and audio on the fly.

Some RAT Builders

- **Zeus** (2007) initially $700, now open source
- **DarkComet** (2008), open source
- **BlackShades** (2010) can now be purchased from an official company $49 - $56

* Commercial Off-The-Shelf

Buy a Crypter as a COTS

Some available Crypters

- **Byte Crypter** $35 for 3 months, $60 for lifetime
- **Datascrambler** $20 for 3 months, $40 for a year
- **BlackShades Crypter** from an official company $60 for 3 months, $100 for a year

Exploits bundle and other services

1. **Exploit bundle** : $25/day, $400/month, up to $3,000
   ➡ program to embed into a webpage

2. **Bulletproof host** : $15–250 per month
   ➡ hosting service to bypass any kind of IP filtering
   anti-spam, anti-virus, anti-malware, law enforcement,
   search engine anti-malware service and so on

3. **Traffic** : $4–10 per 1,000 unique hits
   ➡ attract people to visit the infected webpage

   Installs $12 – $550 per 1000 infections
   ➡ use a spreading service also called Pay-Per-Install (PPI)

Conclusion

Creating a malware, making it undetectable and spreading it would normally be difficult and require a good deal of expertise

However, the cyber underground market makes this process accessible to the mass given a small amount of money

Malware Analysis

What do smart good folks do …

- Analysis for IoC extraction, trend reports, detection engineering
- Static analysis
- Dynamic analysis
- Often a hybrid approach
- Operational Security (OPSEC) to protect analysis infrastructure
- Online repositories: VT, Anyrun, VXIntel etc

Malware Anti-analysis

Gotta protect malicious intellectual property

- Code obfuscation and confusion
- Cryptography
- Runtime environment detection
- Defense evasion technology
- Stagers
- Tamperproof