Targeting availability

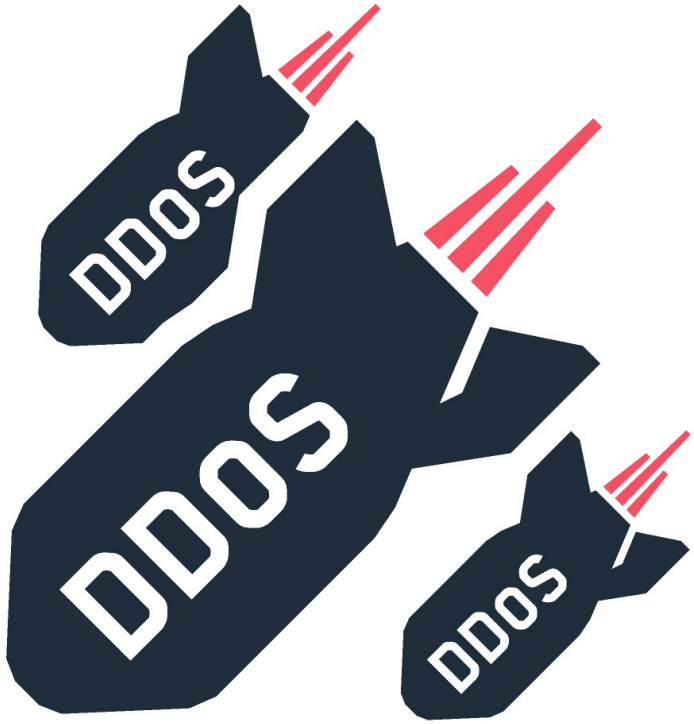
Malware dissemination

Ransomware


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

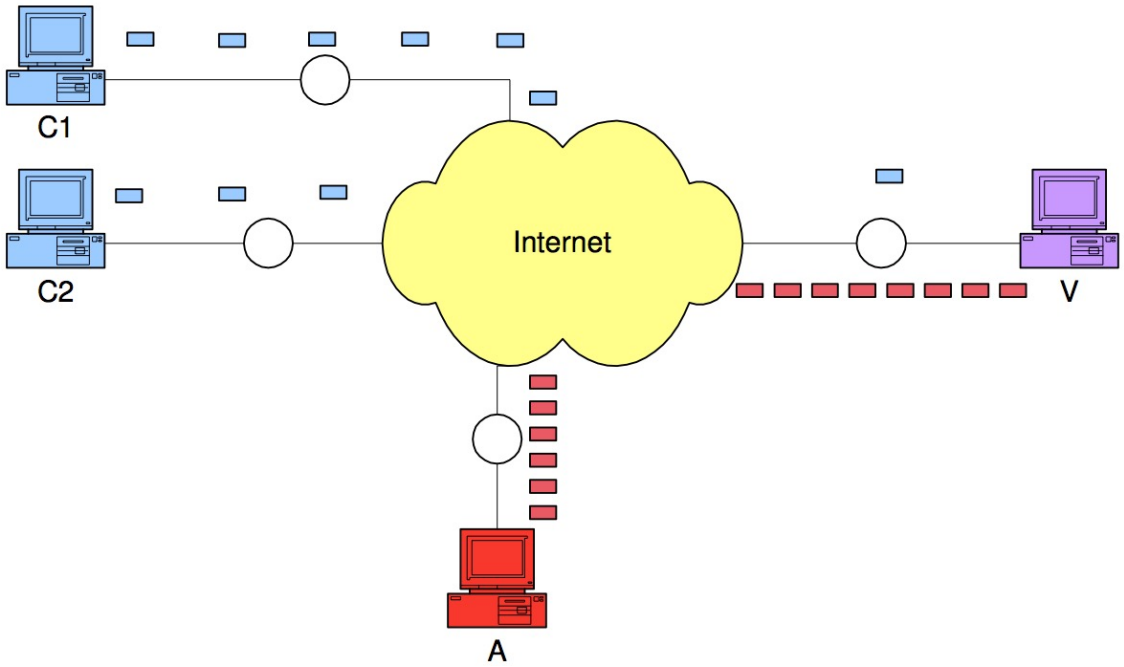
Tools

Distributed Denial of Service



Denial of Service

- Denial of Service (DoS) is an attack where a victim receives a stream of malicious packets that exhausts a key resource. This exhaustion is translated by the denial of this service (the resource) to the legitimate clients of the victim [*Mirkovic 2003*]



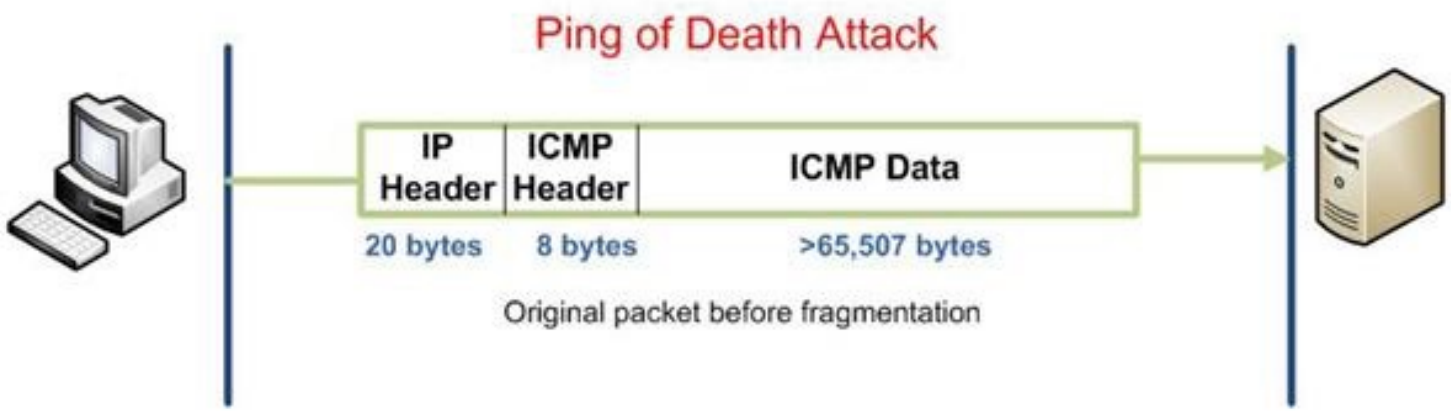
Denial of Service

- Two methods to achieve a Dos :
  - by exploiting certain vulnerabilities in the protocols or software used by the victim (vulnerability attacks)
    - Ping of Death,
    - Land attack
  - Sending a volume of traffic higher than what the victim's resources can handle ➔ Flooding

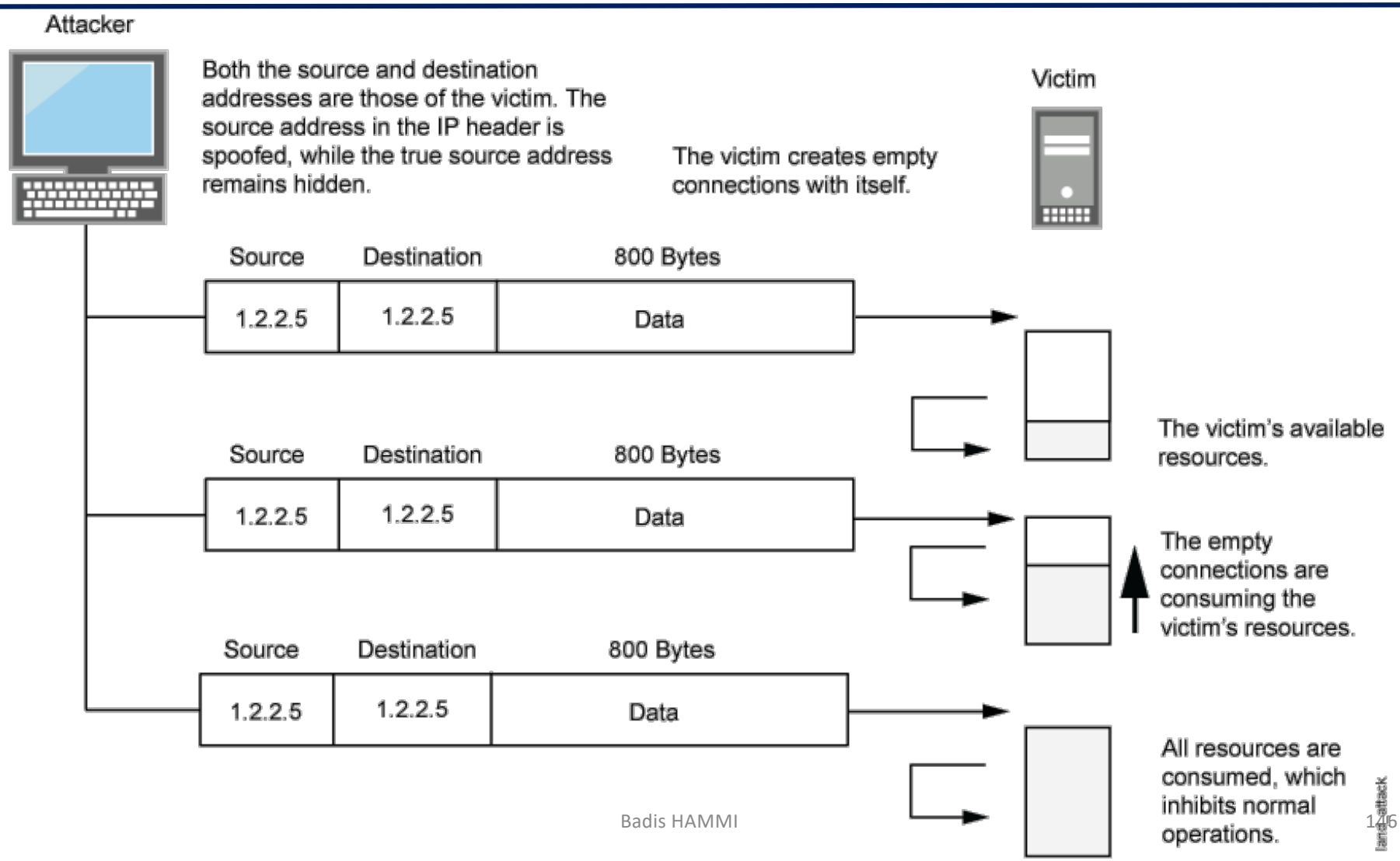
DoS

- Ping of Death
- Land Attack
- Teardrop (fragmentation)

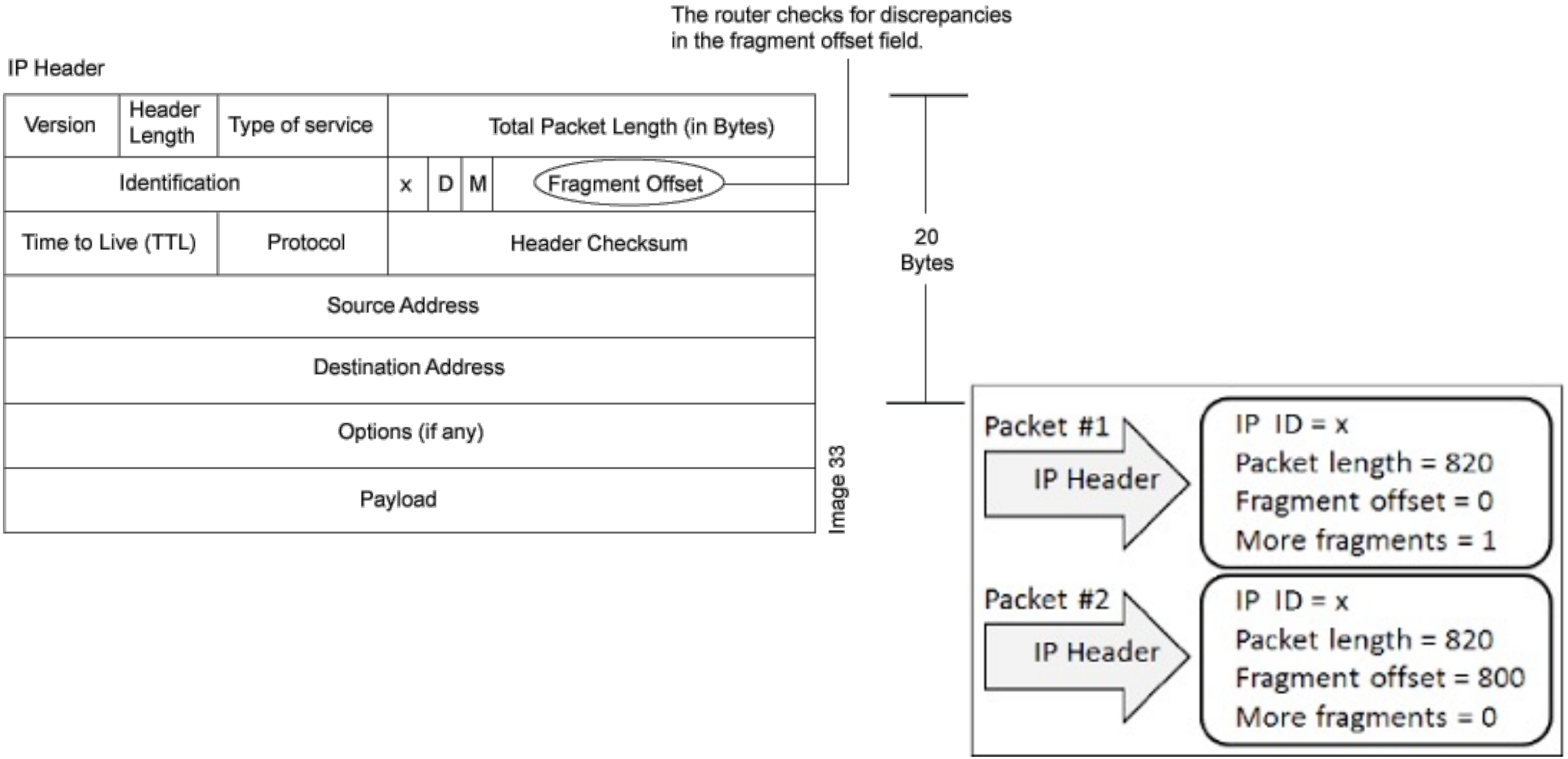
DoS: Ping of Death



DoS: Land attack

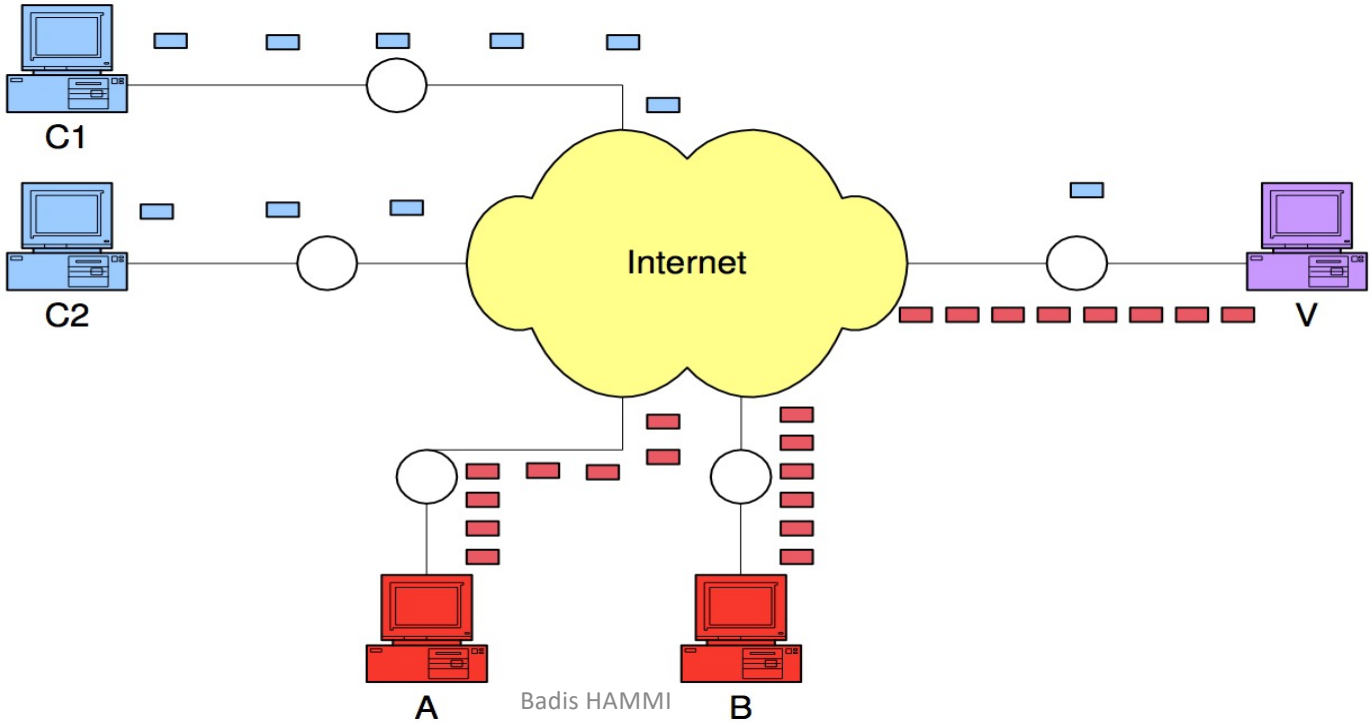


DoS: Teardrop (fragmentation)

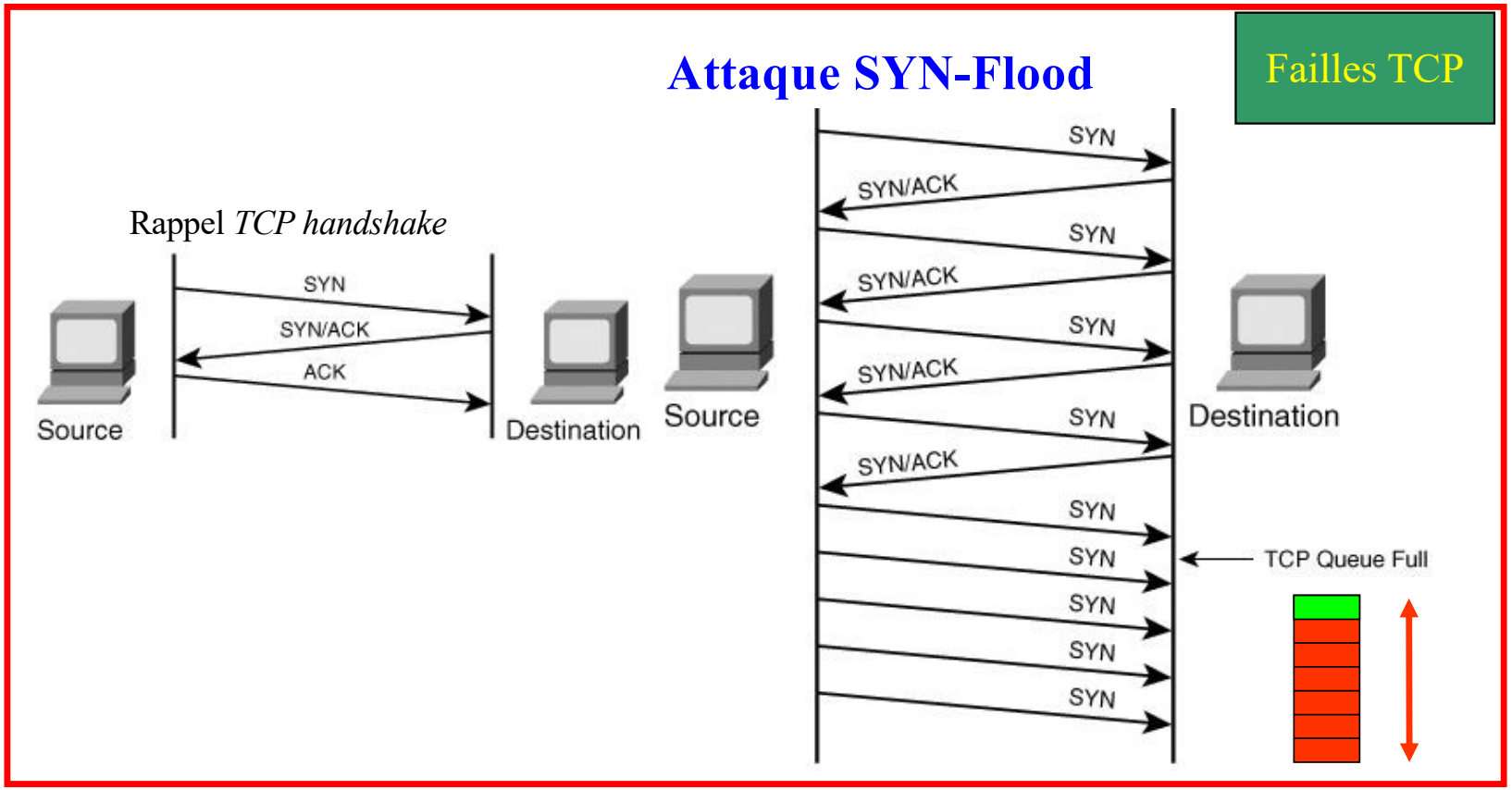


Distributed Denial of Service

"An overwhelming quantity of packets being sent from multiple attack sites to a victim site. These packets arrive in such a high quantity that some key resource at the victim (bandwidth, buffers, CPU time to compute responses) is quickly exhausted." [*Mirkovic 2003*]



DDoS: TCP SYN

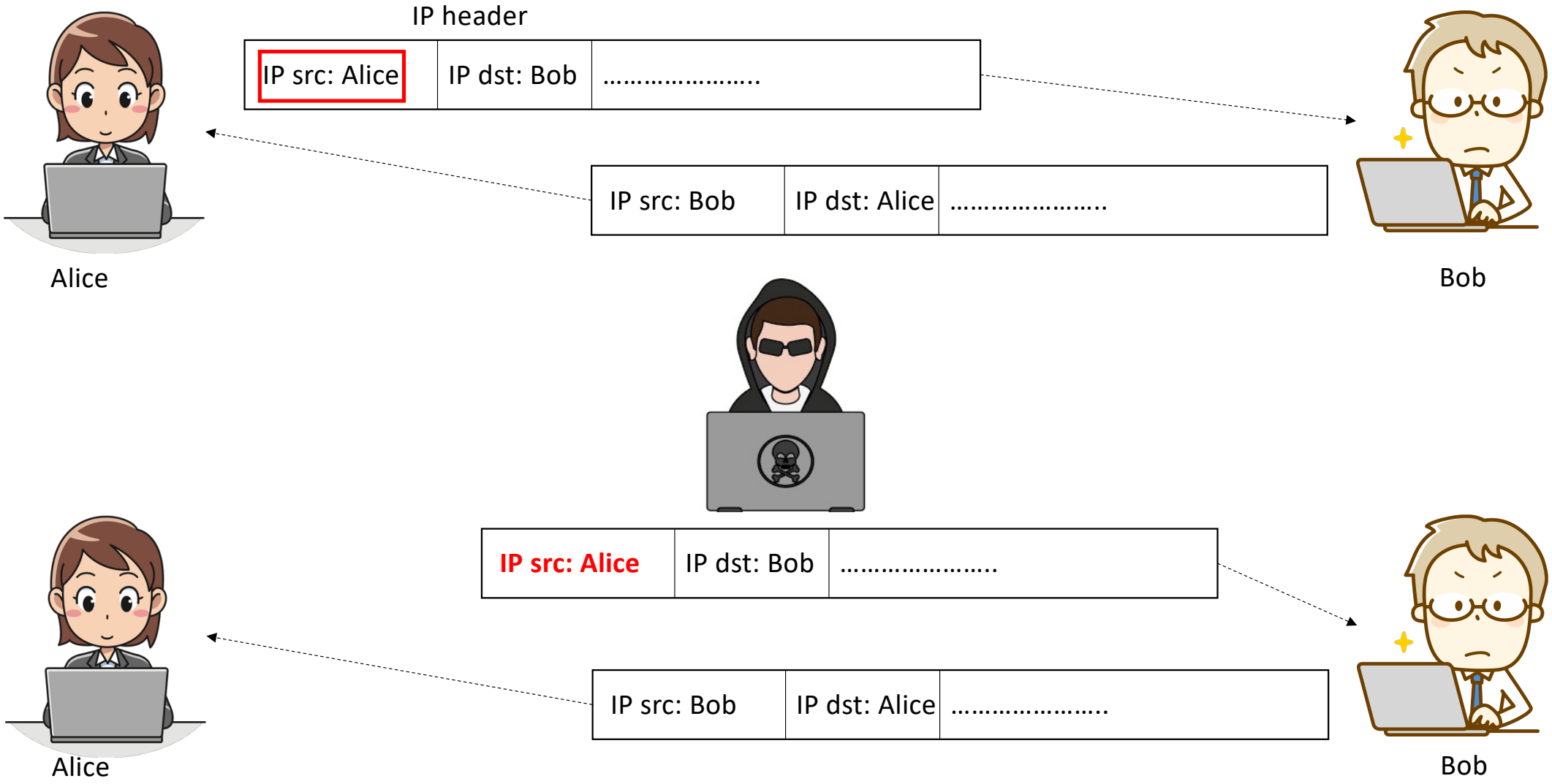

Attaque SYN-Flood
Failles TCP
Rappel *TCP handshake*
SYN
SYN/ACK
ACK
Source
Destination
Source
Destination
SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN
SYN
SYN
SYN
TCP Queue Full

DDoS: Flooding attacks

DDoS attack: Features

- Number of attacking machines
- Similarity between attack traffic and legitimate traffic
- IP address Spoofing

DDoS attack: Features: IP spoofing



DDoS and Botnets

"DDoS attacks are attempts to make a computer resource (i.e. website, e-mail, VoIP, or a whole network) unavailable to its intended users. Overwhelmed with massive amounts of unsolicited data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled zombie or botnet (robot network) computers." [Prolexic 2015]

Botnet

“A botnet is a collection of compromised machines (bots) receiving and responding to commands from a server (the C&C server) that serves as a rendezvous mechanism for commands from a human controller (the botmaster)”. [Khattak et al. 2013].

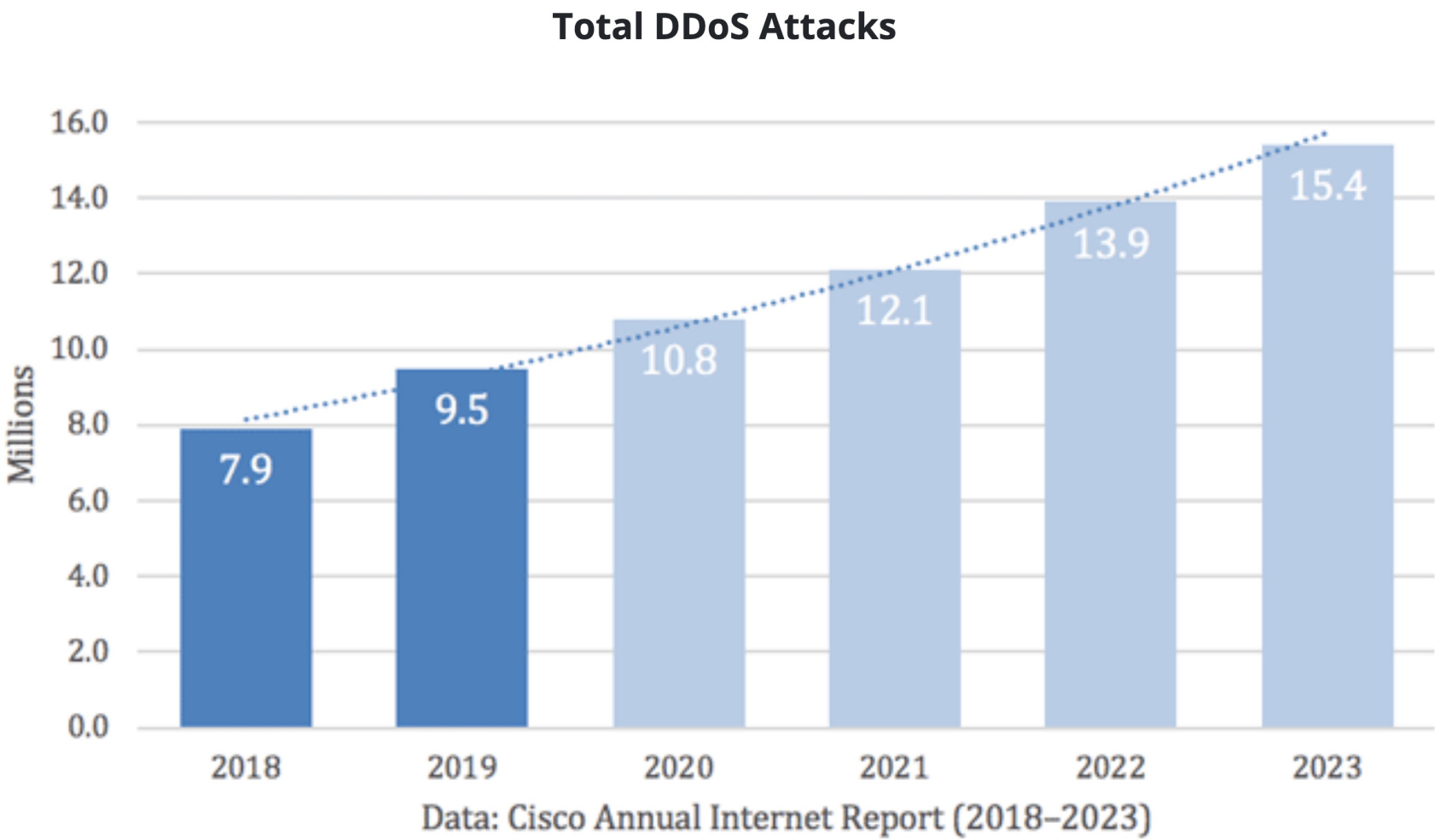
“Botnets are networks formed by “enslaving” host computers, called bots (derived from the word robot), that are controlled by one or more attackers, called bot-masters, with the intention of performing malicious activities”. [Silva et al. 2013]

Types of malware

Botnets: a danger

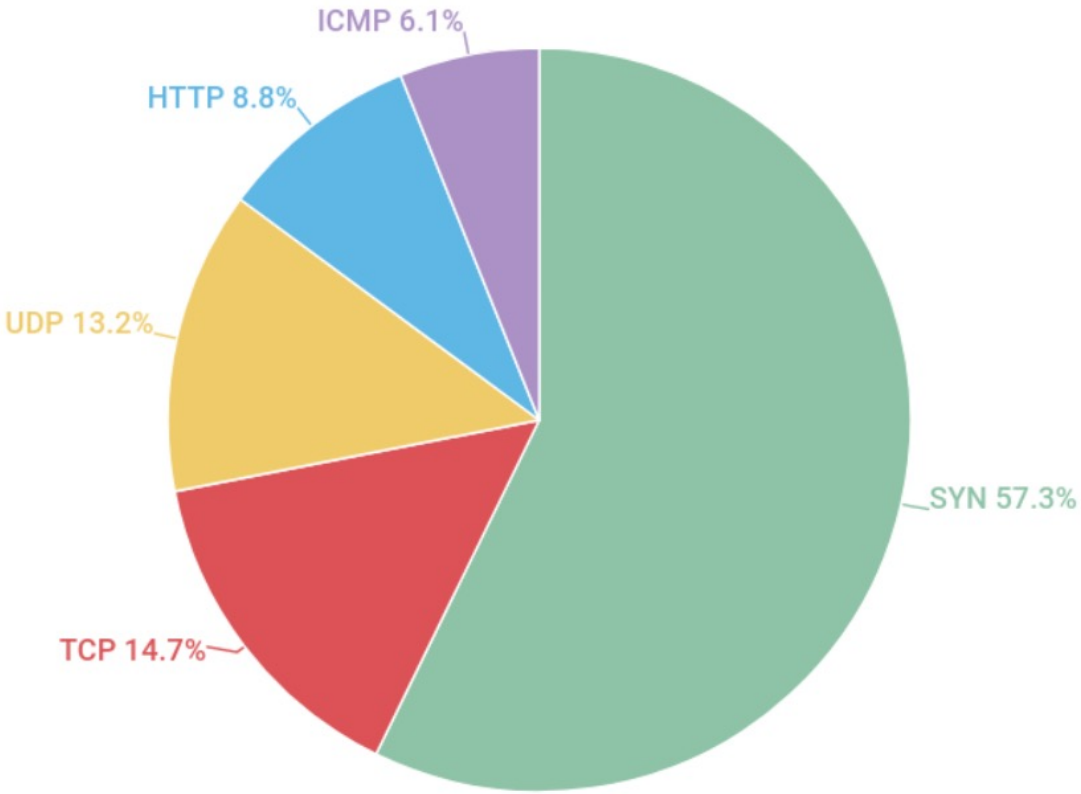
- DDoS
- Spam
- Data theft
- BlockChains hosting (cryptojacking)
- Click Fraud

Botnets: a danger

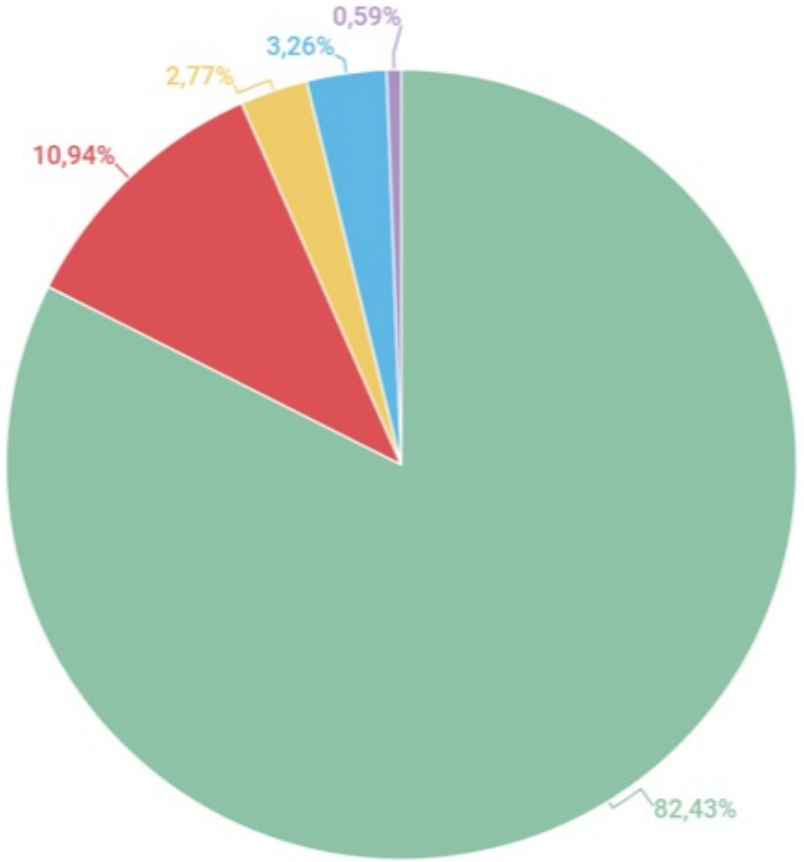


Netscout Arbor Map

Distribution of DDoS attacks by type

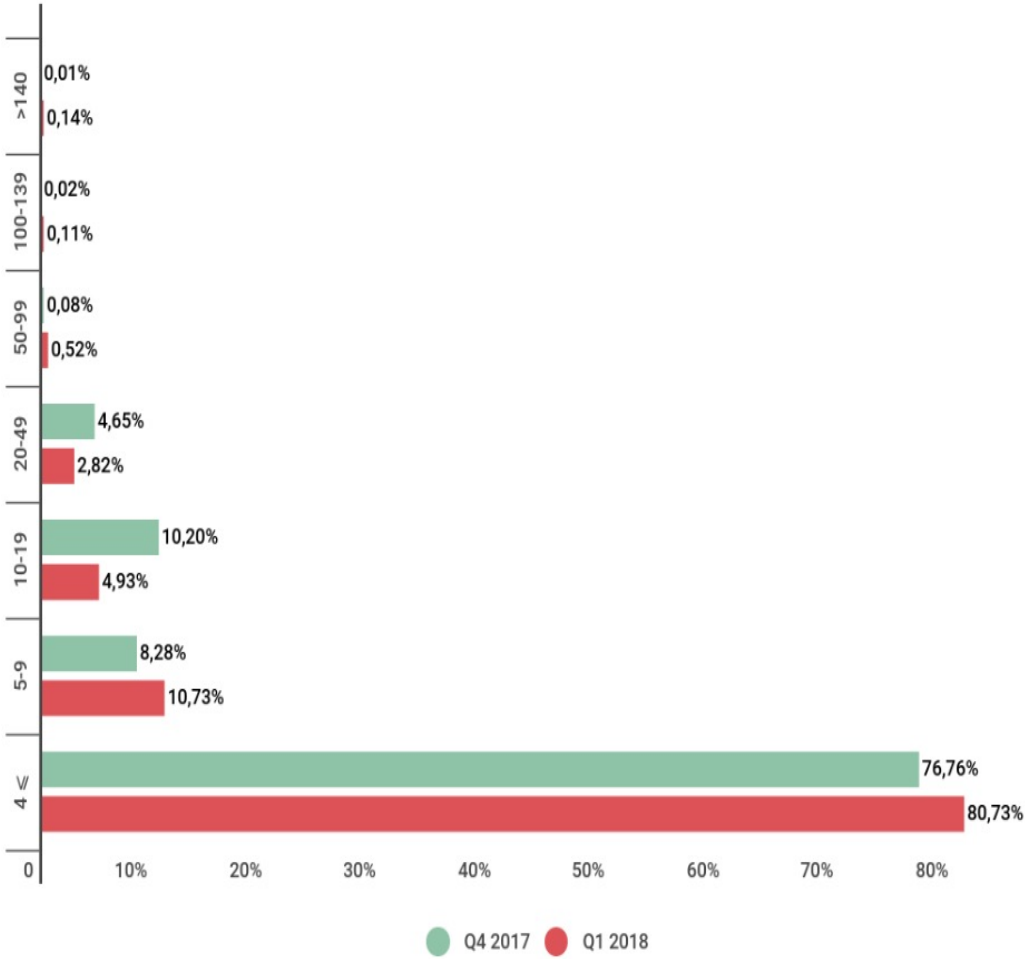


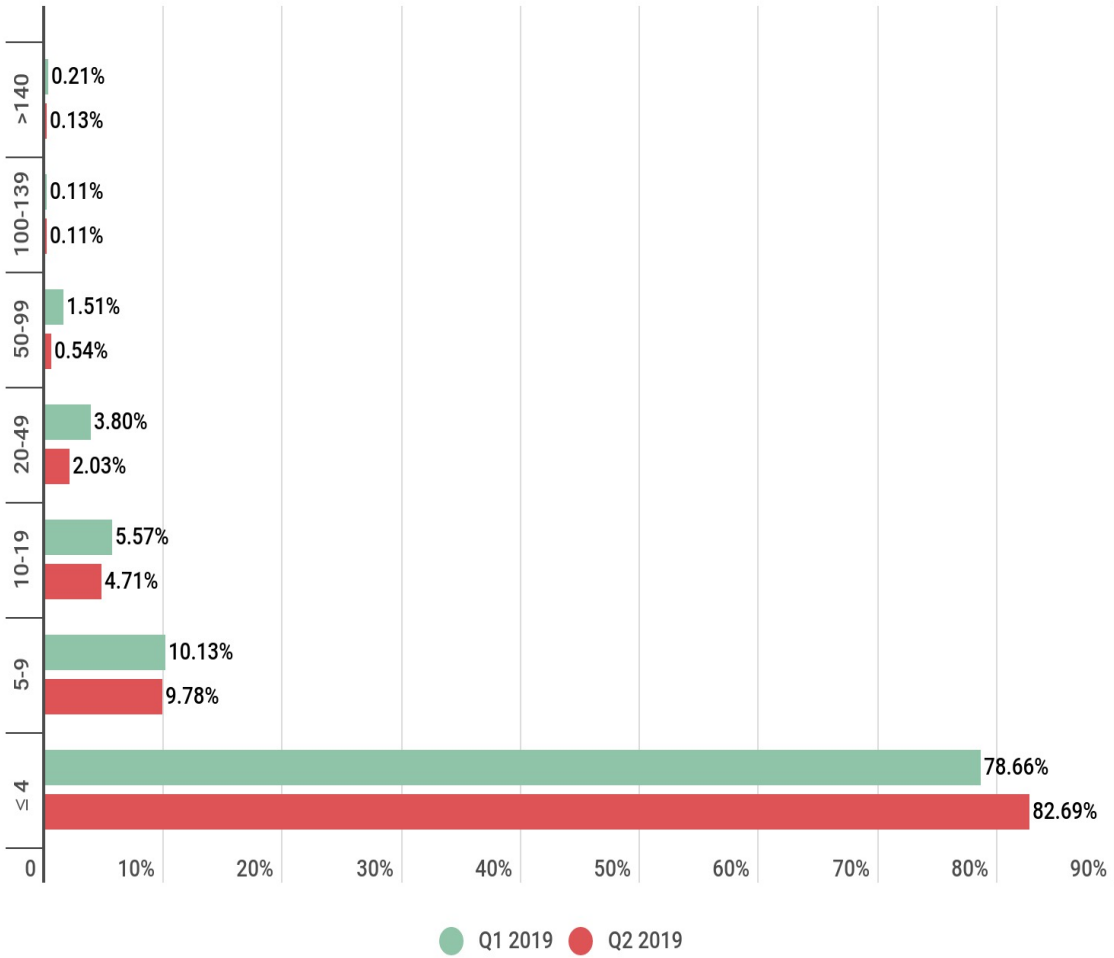
Q1 2018



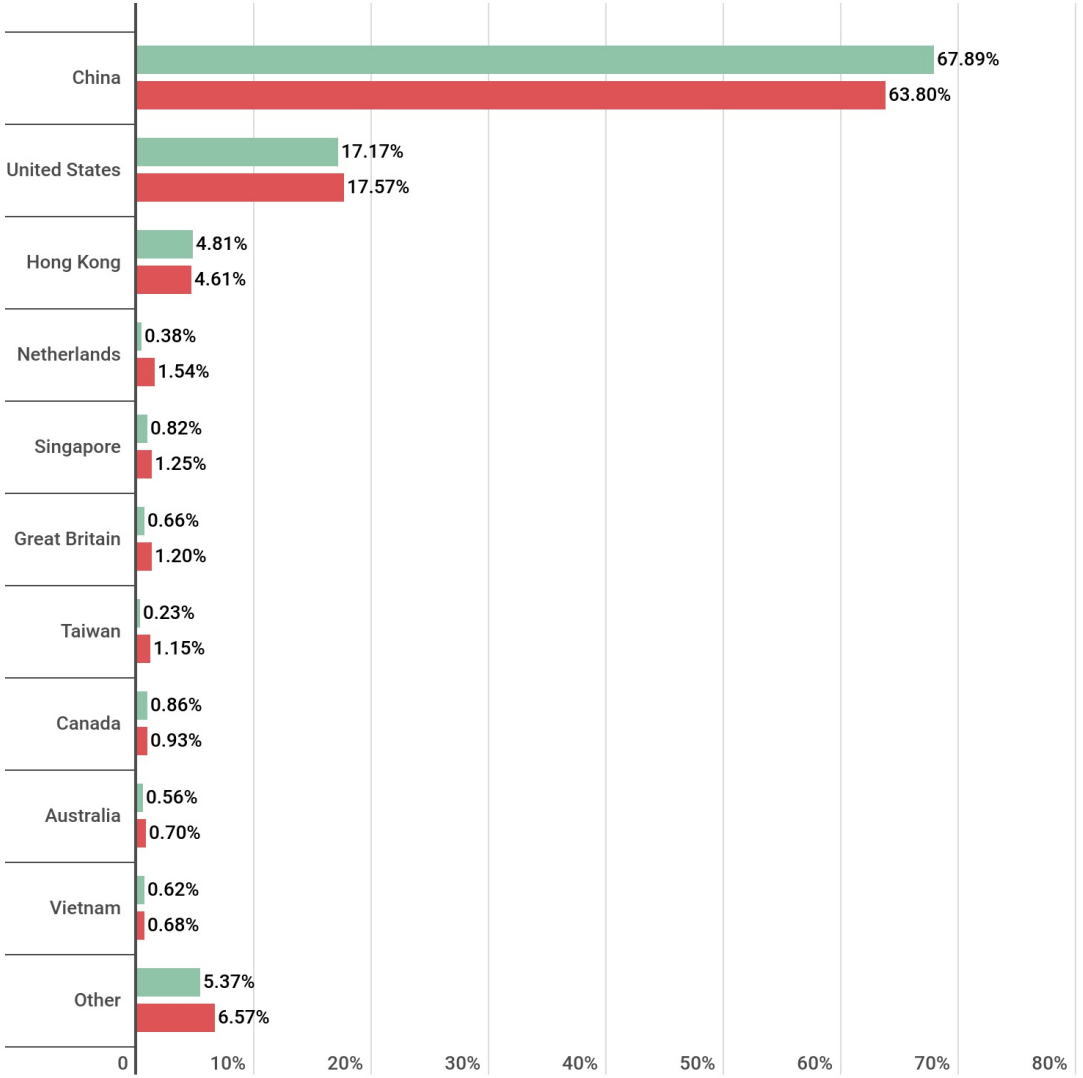
Q2 2019

Distribution of DDoS attacks by duration (hours)





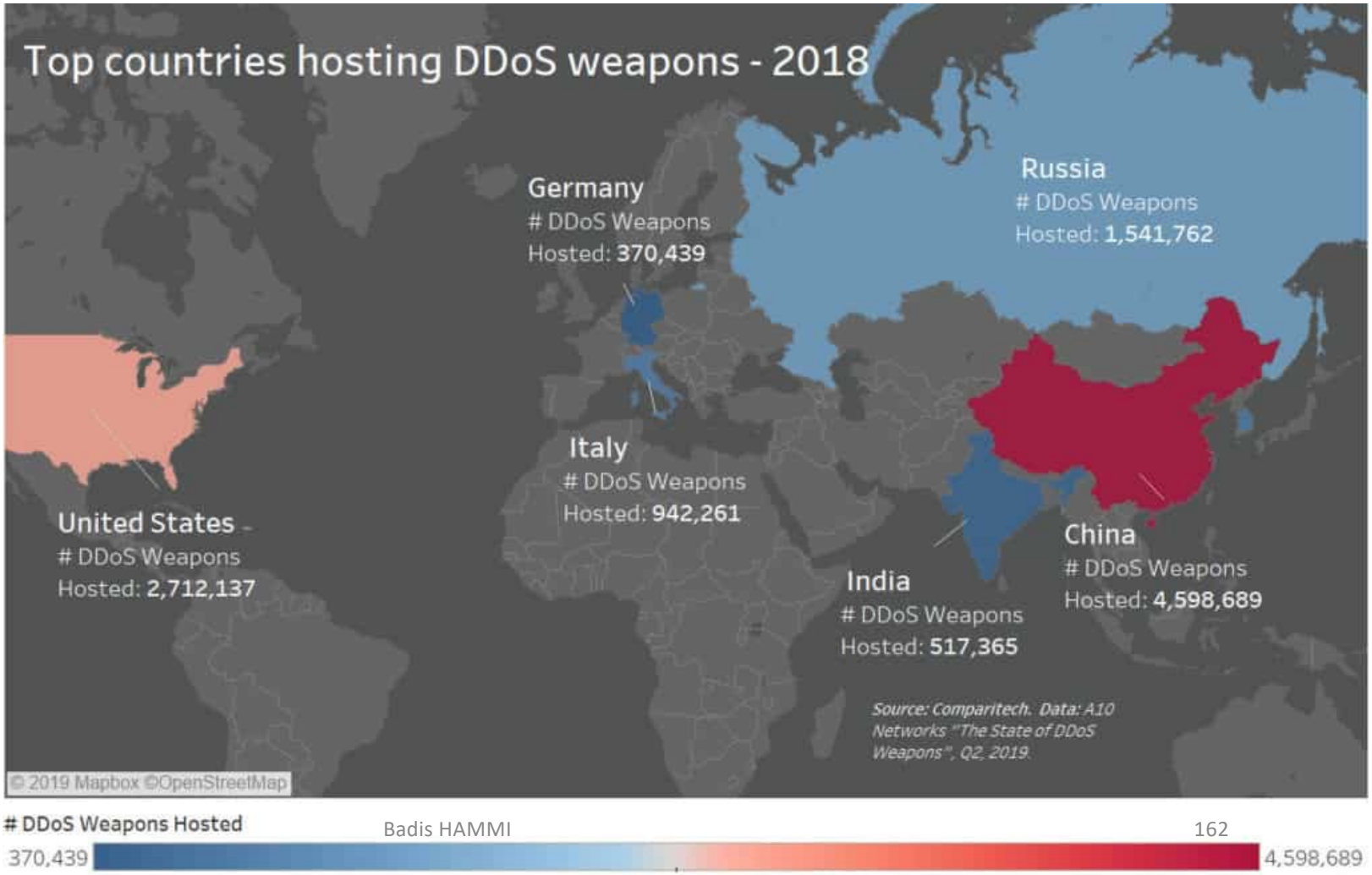
Most targeted countries



Top DDoS sources

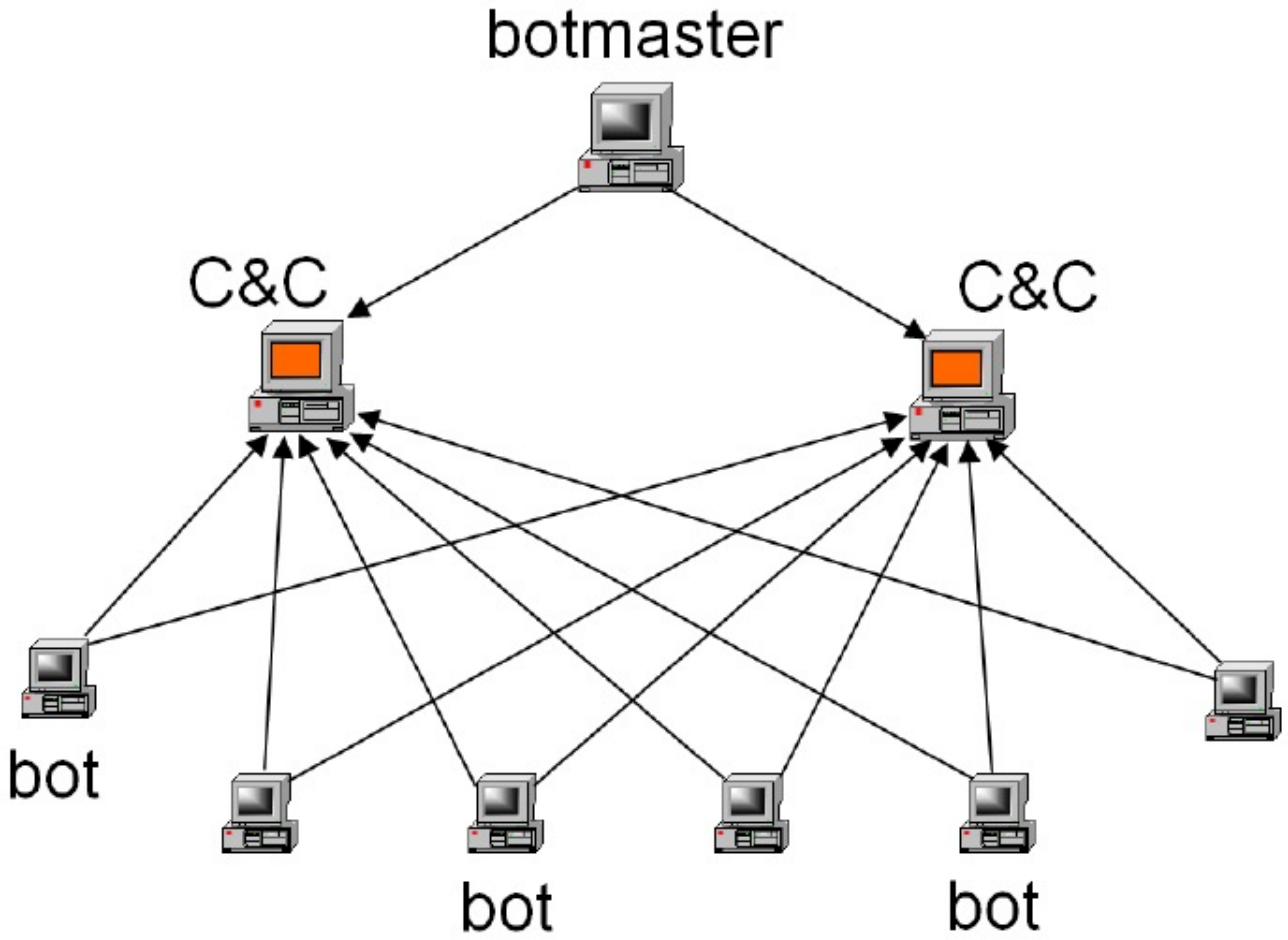
The majority of DDoS attacks are launched from:

- China (over 4.5 million in 2018)
- USA (2.7 million)
- Russia (1.5 million)
- Italy (940,000)
- South Korea (840,000)
- India (500,000)
- Germany (370,000)



Botnets: Architectures

Centralized



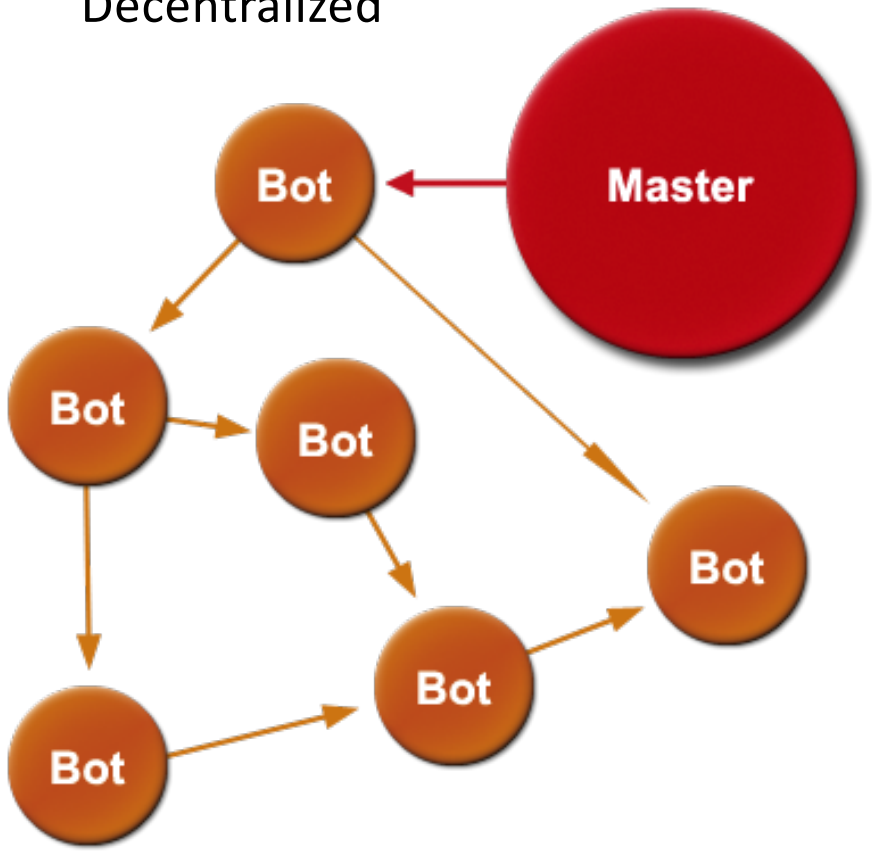
Botnets: Architectures

Decentralized botnets are typically based on a variety of peer-to-peer (P2P) protocols and function as an overlay network.

Structured peer-to-peer overlay: Often uses Distributed Hash Tables (DHT), such as those based on the CAN, Chord, Pastry, and Tapestry protocols. This type of architecture allows targeted and optimal communication between the different nodes of the network.

Unstructured peer-to-peer overlay: This type of network refers to random topologies with different degrees of distribution. Thus, they offer no possibility of routing.

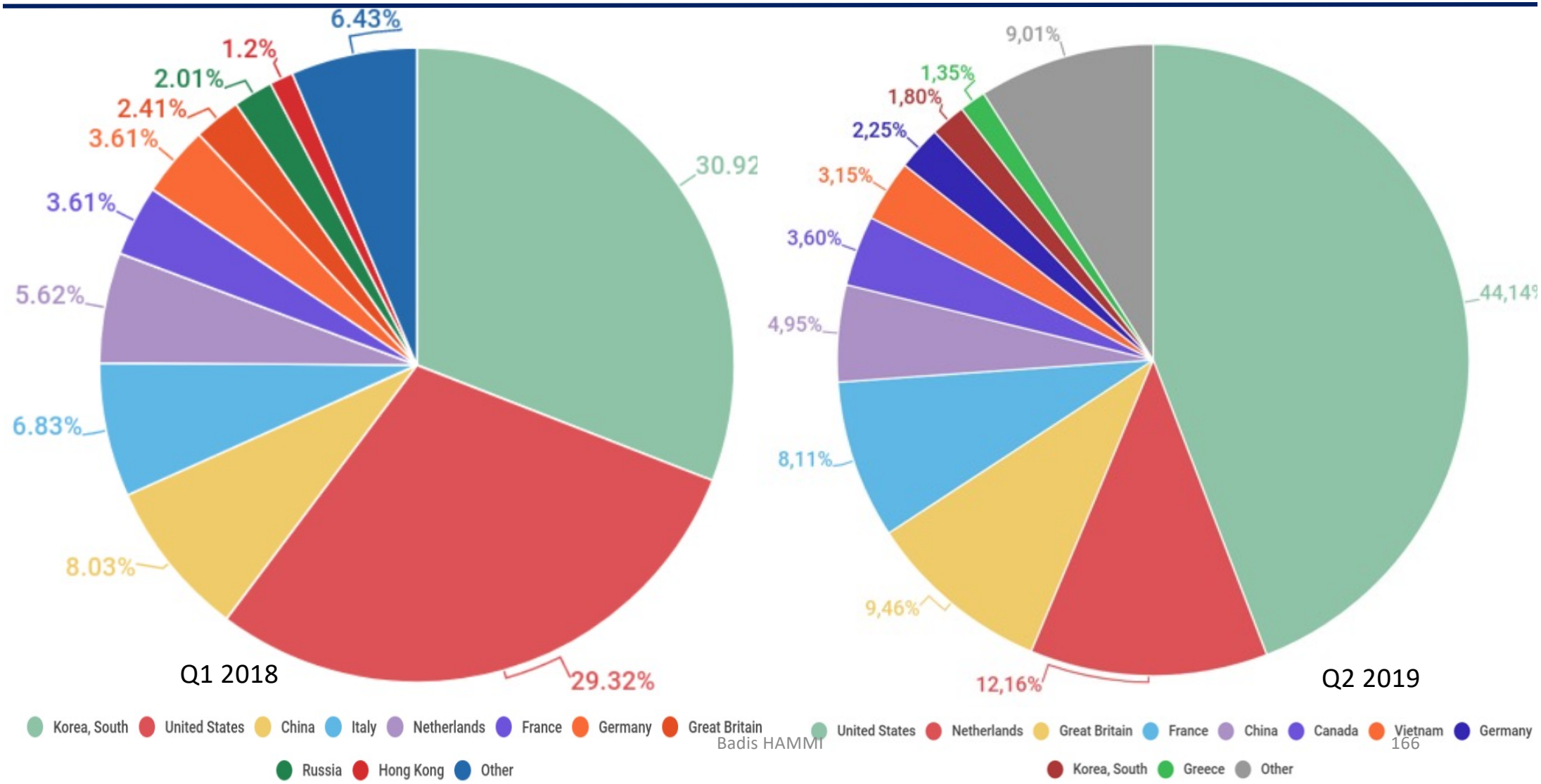
Decentralized



Botnets: Architectures

Hybride: the bots of a hybrid botnet can be classified into two groups: servant bots and client bots. Serving bots behave like waiters and like customers. They are configured with static and routable IP addresses. Client bots are configured with dynamically and non-routable IP addresses and do not accept any incoming connections

Distribution of botnet C&C servers by country



Botnets: communication protocols

- ***Internet Relay Chat* (IRC) :** The botmaster creates IRC channels on the C&C servers on which the bots will connect and wait for the commands. IRC allows communication through multicast groups called "communication channels" or through private unicast communications between two members. This feature allows the botmaster to have flexible control over his botnet.
  Exemples: Kaiten , Agobot, Rxbot, Sdbot et EggDrop

- ***HyperText Transfer Protocol* (HTTP) :** in order to remedy the disadvantages of the IRC protocol, the HTTP protocol has been proposed to ensure C&C communications. In comparison, its main advantage lies in the permissiveness of HTTP traffic which is allowed in most networks and which allows to conceal the communications within the botnet.
  Exemple: Zeus, Hybrid_V1.0, Festi, Bobax, Asprox, Srizbi

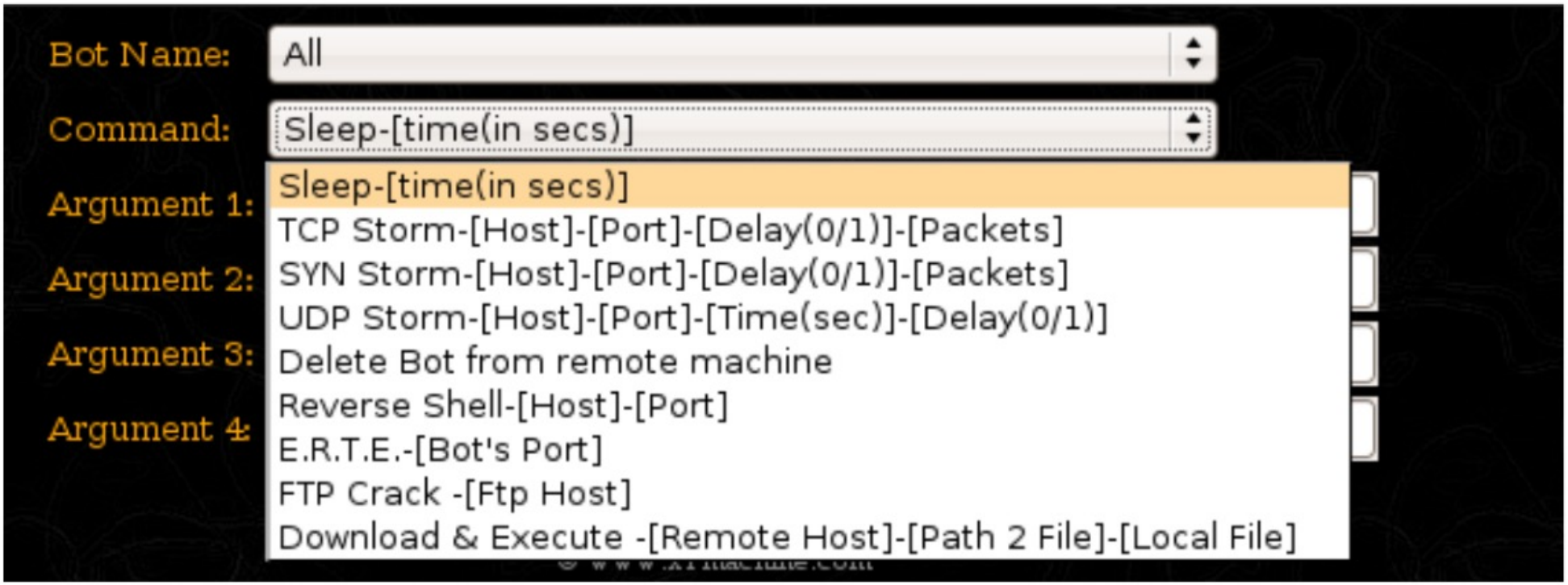
Botnets: a use case study

- Botmaster composition :
  - Data base
  - HTTP server
  - HMI

Botnets: a use case study

» Bot IP «	» Country «	» Current Command «	» Bot Name «	» Bot Message «	» Check «	» Action «
47.89.187.196	Canada		/opt/Hybrid_root_Ouef1	Unknown Command		Delete
173.255.113.41			/opt/Hybrid_pedouard78450_Xi7VW	Unknown Command		Delete
47.89.190.168	Canada		/opt/Hybrid_root_MChG6	Unknown Command		Delete
47.89.178.242	Canada		/opt/Hybrid_root_HjqaU	Unknown Command		Delete
146.148.39.54	United States		/opt/Hybrid_pedouard78450_cJZlu	Unknown Command		Delete
104.197.49.121			/opt/Hybrid_pedouard78450_BysbF	Unknown Command		Delete
104.197.233.90			/opt/Hybrid_pedouard78450_odEvQ	Unknown Command		Delete
104.197.191.35			/opt/Hybrid_pedouard78450_Fxjyv	Unknown Command		Delete
159.8.96.86	Switzerland		/opt/Hybrid_root_8h2Ni	Unknown Command		Delete
159.8.126.35	Switzerland		/opt/Hybrid_root_ROM1j	Unknown Command		Delete
82.223.67.106	Spain		/opt/Hybrid_root_DgHGM	Unknown Command		Delete
35.167.15.4	United States		/opt/Hybrid_ubuntu_UrfcX	Unknown Command		Delete
35.164.178.68	United States		/opt/Hybrid_ubuntu_QOtoK	Unknown Command		Delete
104.199.5.139			/opt/Hybrid_christophe_ozkur_icBhM	Unknown Command		Delete
104.199.91.145			/opt/Hybrid_christophe_ozkur_rDziw	Unknown Command		Delete
130.211.48.242	United States		/opt/Hybrid_mhaocn1990_0x000BTC	Unknown Command		Delete
104.199.81.220			/opt/Hybrid_mhaocn1990_T21Uz	Unknown Command		Delete
104.199.72.140			/opt/Hybrid_mhaocn1990_z004N	Unknown Command		Delete

Botnets: use case study



Botnets: use case study

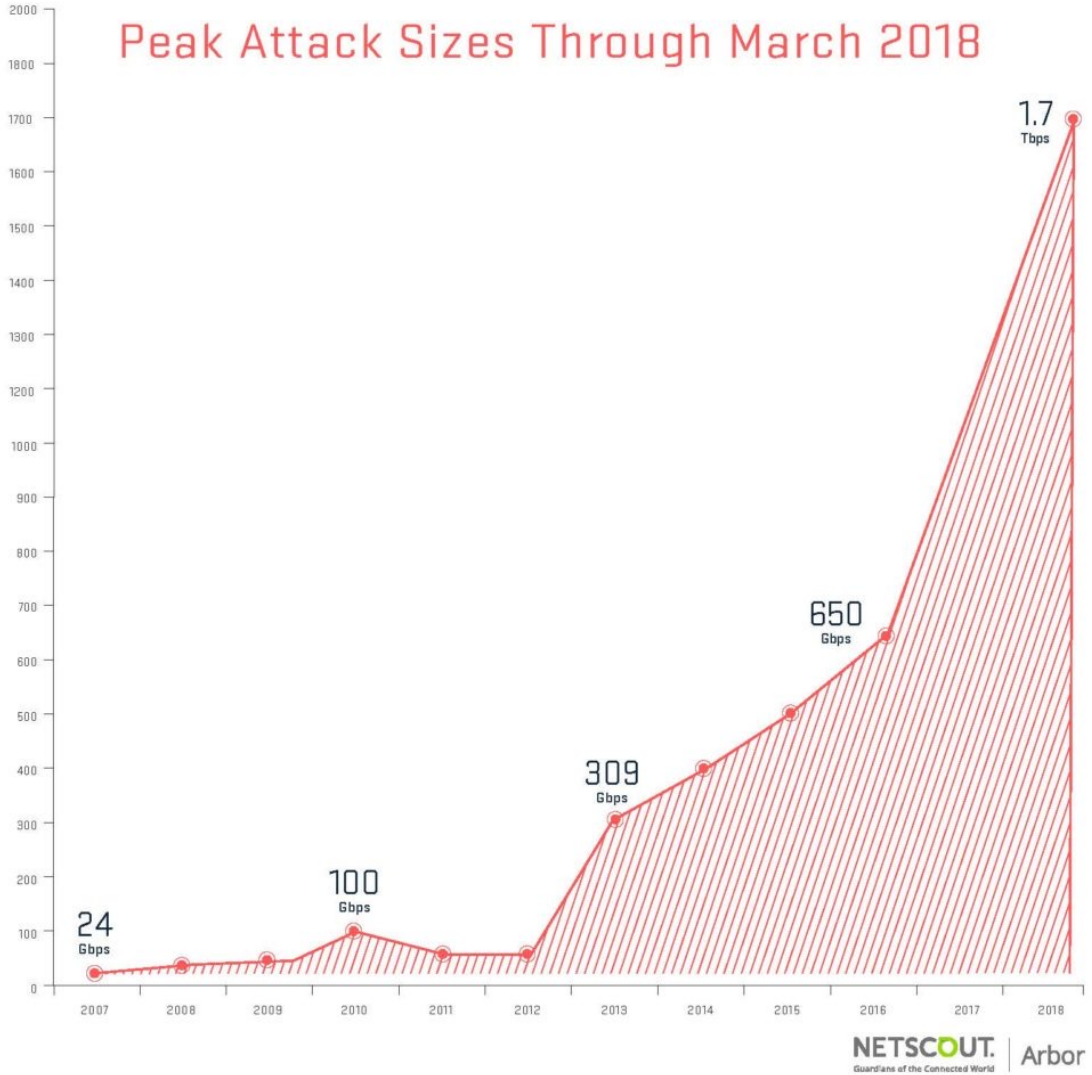
Voir code source Bot

Research problem

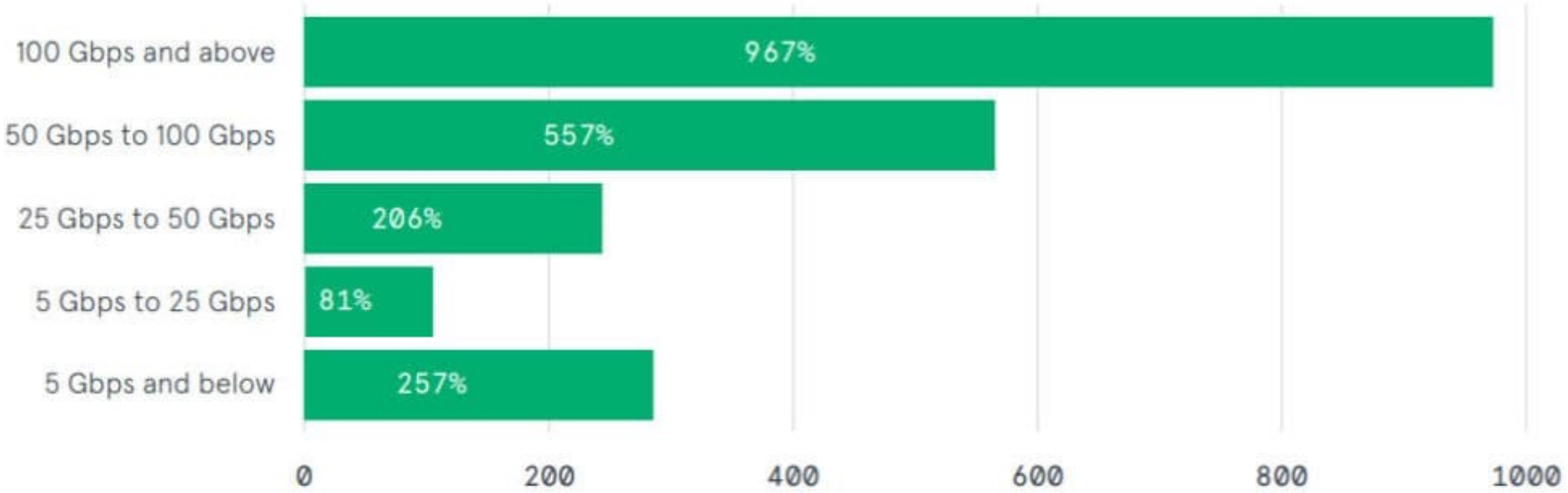
- DDoS attacks are easy to detect however they represent a persistent challenge for academia and industry

- **Because they are in constant evolution**

Botnets/DDoS: a danger



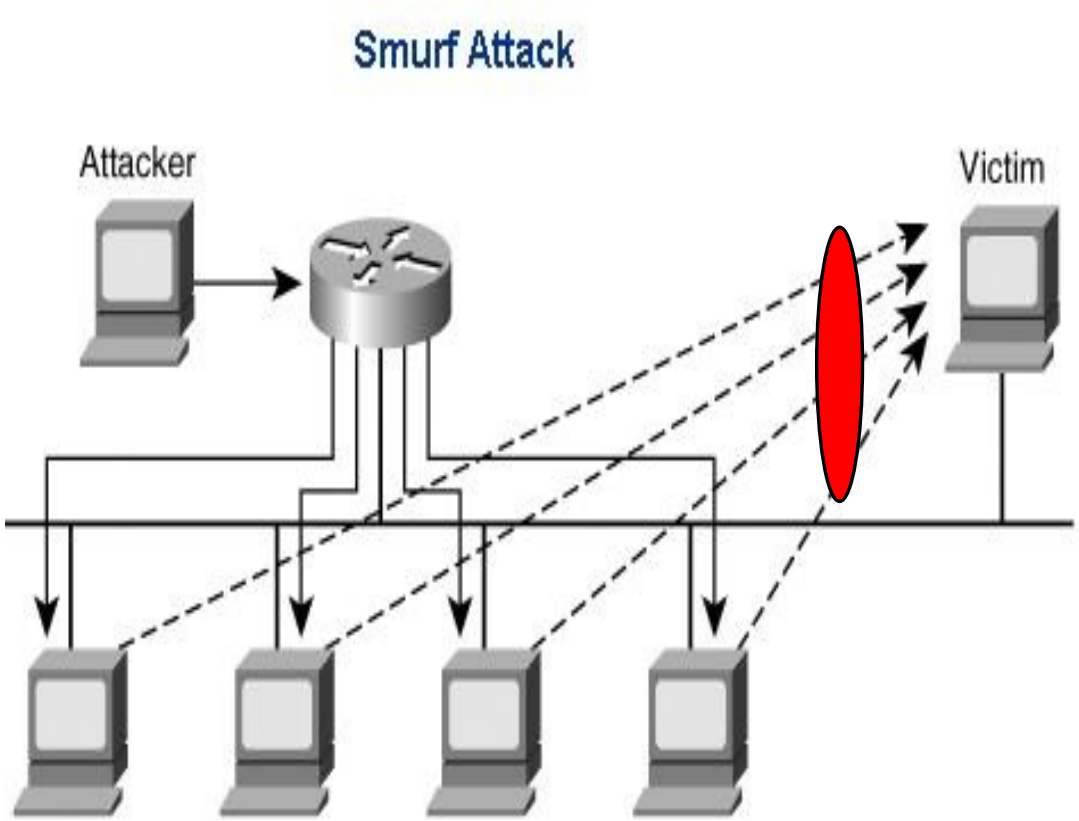
Botnets/DDoS: a danger



DDoS increasing (percent) between 2018 and 2019

© comparitech.com

DDoS: reflective attacks



DDoS: DNS reflection/amplification attack

DNS Reflection : During a DNS reflection / amplification attack, the attacker sends a stream of DNS queries to a set of open DNS resolvers, while replacing the source IP address of the requests with that of the victim. A DNS query usually requires a large set of records, which leads to an increase in attack traffic.

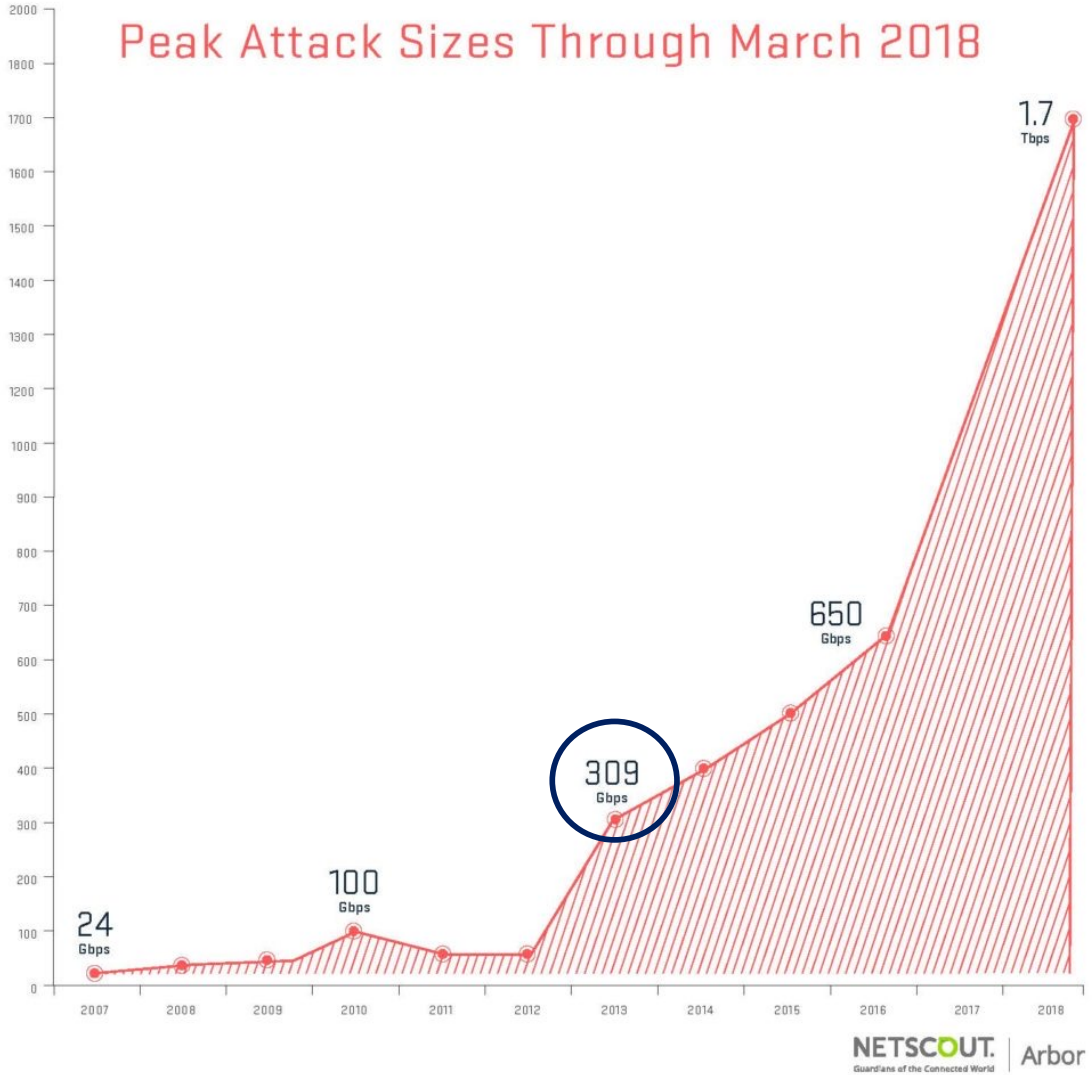
By using multiple machines (bots) to send requests to multiple DNS servers, an attacker can cause very large volumes of attack traffic from widely distributed sources. The other power factor of these attacks lies in the large number of DNS servers. Indeed, currently, it is estimated that there are more than 32 million DNS servers on the Internet, including 28 million that represent a potential threat

DDoS: NTP reflection/amplification attack

NTP Reflection/Amplification: Like DNS, NTP is an ideal tool for generating DDoS attacks. The NTP protocol uses a command called monlist that can be sent to an NTP server for monitoring purposes. The latter returns the addresses of the last 600 machines with which the NTP server interacted, thus generating a large response. It is the latter that is used to amplify attacks. Thus, an attacker, armed with a list of NTP servers on the Internet, can easily perform a powerful DDoS attack, especially when he uses a large number of bots

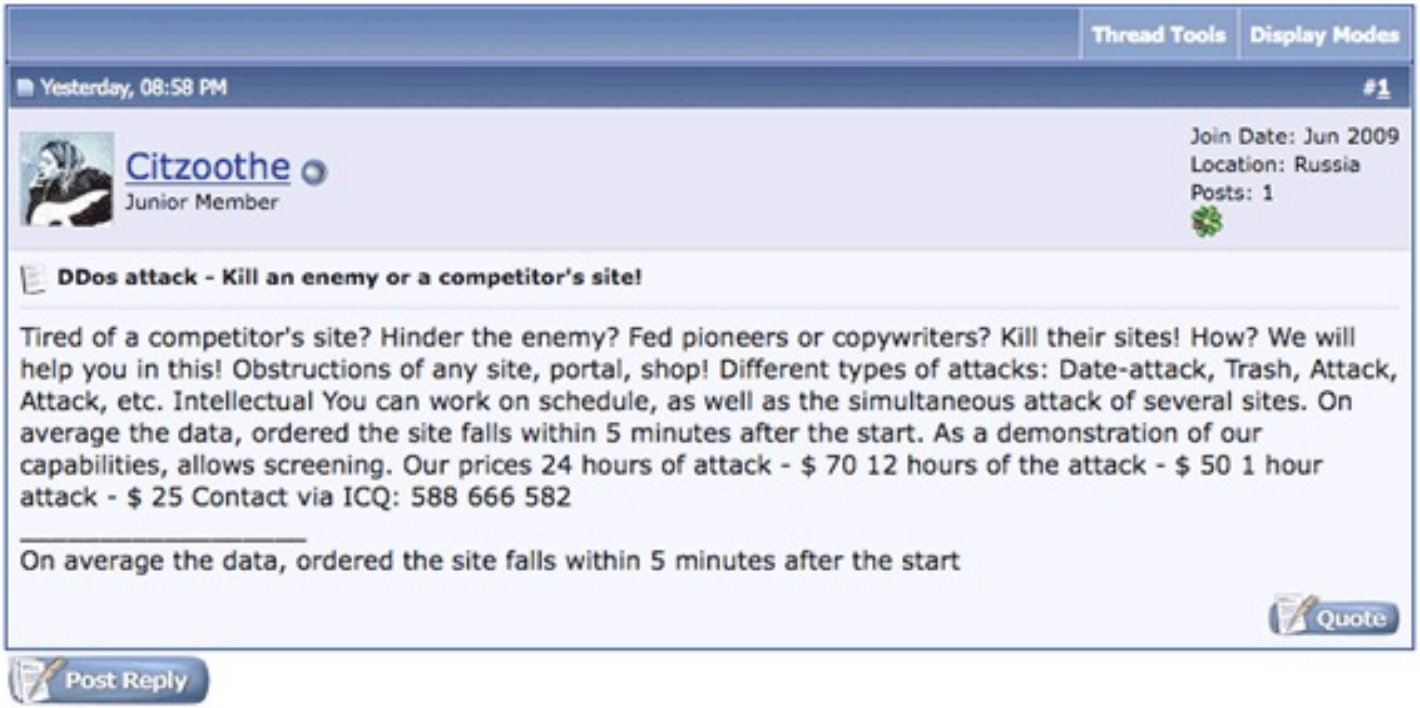
NTP servers are not difficult to solicit. Indeed, common tools like Metasploit and NMAP have modules that can easily identify the NTP servers that support the monlist command

Botnets/DDoS: a danger



- Botnet + DDoS, it is dangerous but how far ???

DDoS attacks evolution



Average price between $ 9 per hour and $ 67 per 24 hours (in 2014)

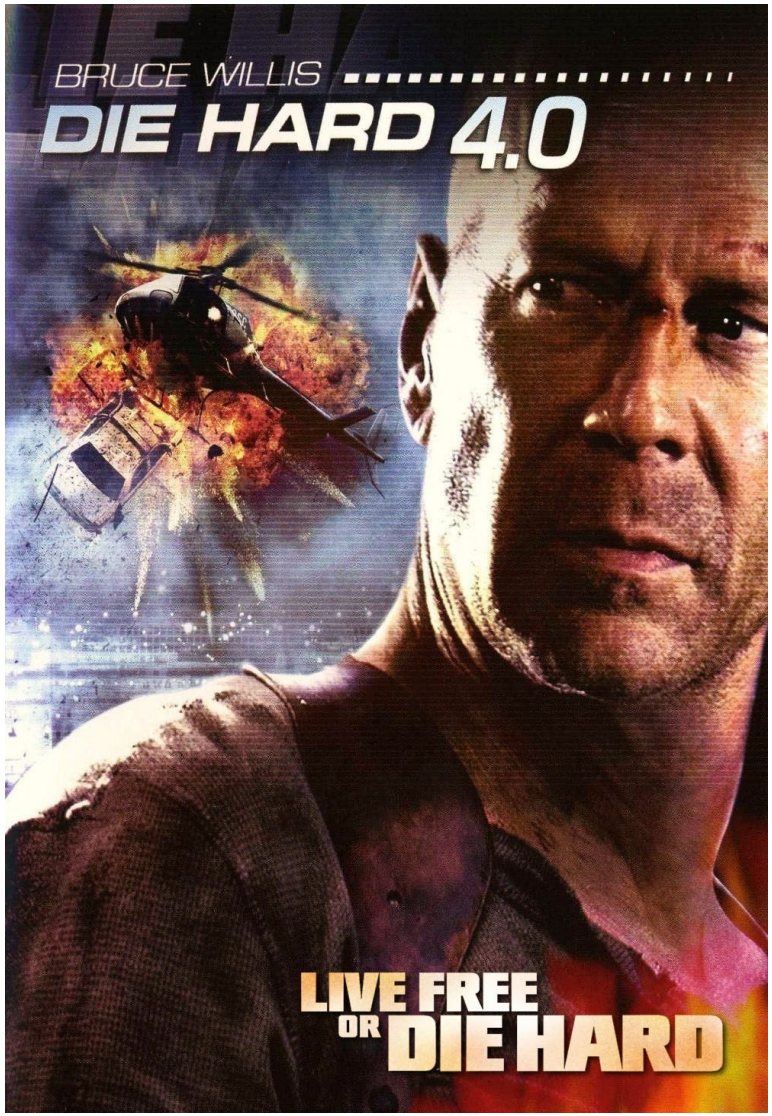
A bit of history about DDoS attacks

- Morris worm
  - 2nd november 1988 : first electronic bomb
  - Proof of concept put 6,000 Internet systems out of order (15%)
  - Features
    - Created to spread by exploiting vulnerabilities and configuration errors
    - No possibility to detect its presence on a system
    - Reproduce on remote systems, but also locally
  - Result
    - Thousands of small processes were running on the target system and causing the first massive DoS in history

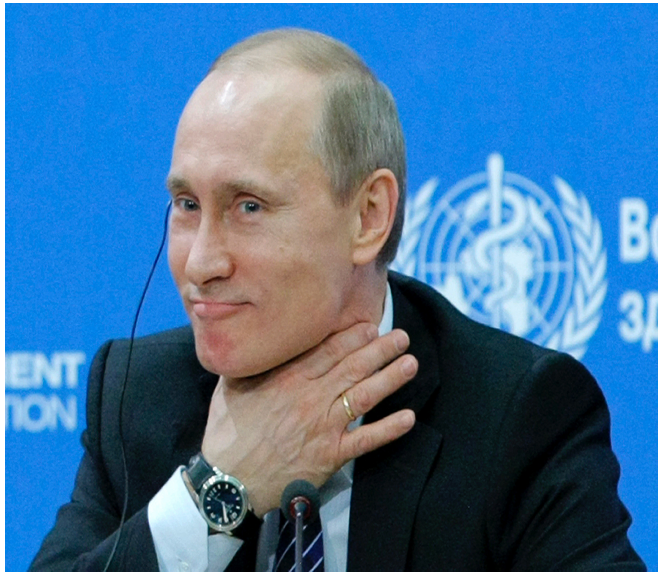
A bit of history about DDoS attacks

- 2000 :
  - DoS contre un certain nombre de grands sites américains Yahoo (inaccessible pour 3 heures, 500,000 $ de perte), Buy(disponible que 10%), Stamps, eBay, CNN, Amazon(inaccessible 10 heures et 600,000$ de perte), MSN et ZDNet
  - Perte de 1.7 milliards $
  - Combinaison des outils : Trinoo, TFN, TFN2K, Stacheldraht
- 2002 :
  - DDoS contre 7 des 13 serveurs DNS
  - Paralyser le réseau mondial par l'impossibilité d'accéder au web.
  - Attaque par des paquets ICMP, TCP-SYN et UDP.
  - Débit variant entre 50 Mbps et 100 Mbps / serveur
- 2007 :
  - Attaque massive et coordonnée contre l'Estonie
  - 128 attaques en deux semaines
  - 115 en ICMP *floods*, 4 en TCP SYN *floods*, et 9 flux générique
- 2008 :
  - CNN était victime d'une attaque DDoS par un débit de 14 Mo/s
  - Ralentissements sur le site auraient été ressentis par les internautes asiatiques
  - Les contre-mesures qui étaient mises en place n'ont pas protégé le serveur
- 2009 :
  - *Cyber milice* russe met le Kirghizistan hors ligne
  - 3 FAI sont tombés

CyberWar: Estonia 2008



CyberWar: Estonia 2008



CyberWar: Estonia 2008

Paralysis of the computer system:

- Banks
- Information channels
- Government websites

CyberWar: Estonia 2008

CyberWar: Estonia 2008

Result : The *North Atlantic Treaty Organization (NATO)* integrates the concept of Cyberwar

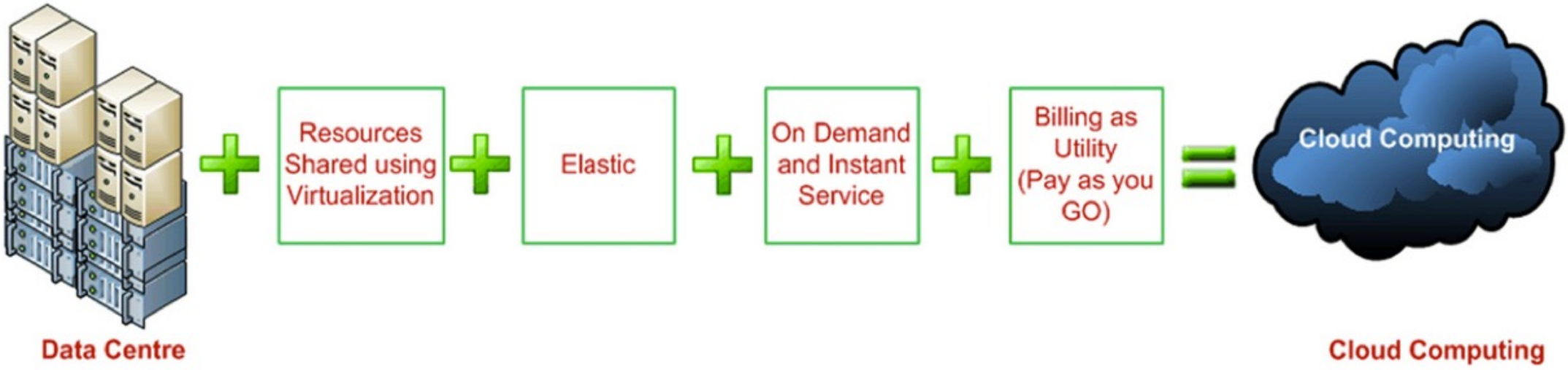
CyberWar

- Iran 2010
  - Electronic war against Iran
  - Several thousands of computers out of service
  - Against the energy distribution infrastructure
  - Malware considered as a weapon intended to undermine the security of the Iranian territory
  - Cyberspace has become a theater of geopolitical conflict
  - Rethinking the notion of territory
- Cyberdefense
  - Set of physical and virtual means set up by a country in the context of the computer warfare conducted in cyberspace
- Cyberespace
  - A mental representation, a virtual territory, outside the physical world in which exchanges and interactions take place

CyberWar: public opinion manipulation

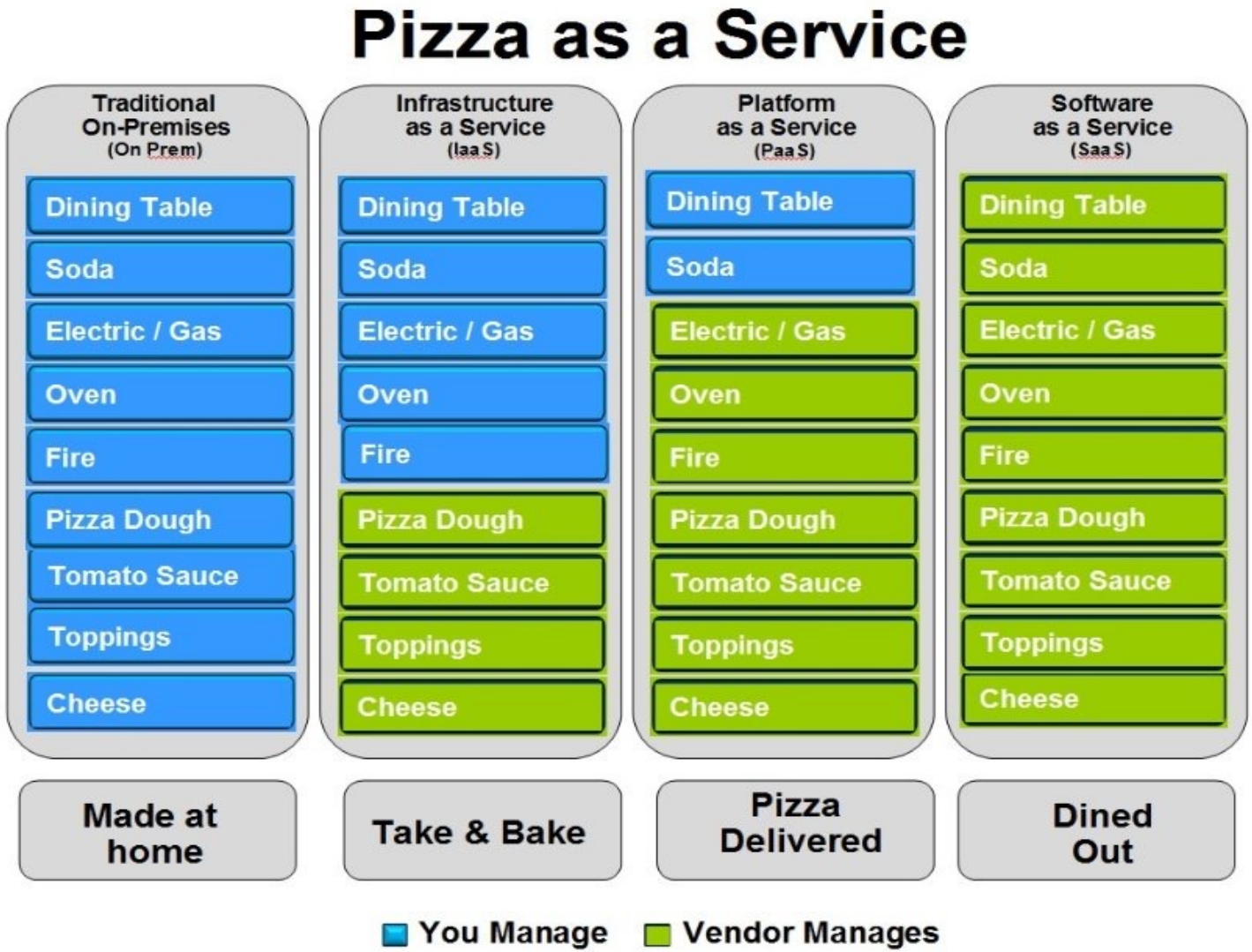
Evolution of DDoS

Botnet/DDoS evolution: Towards the cloud computing

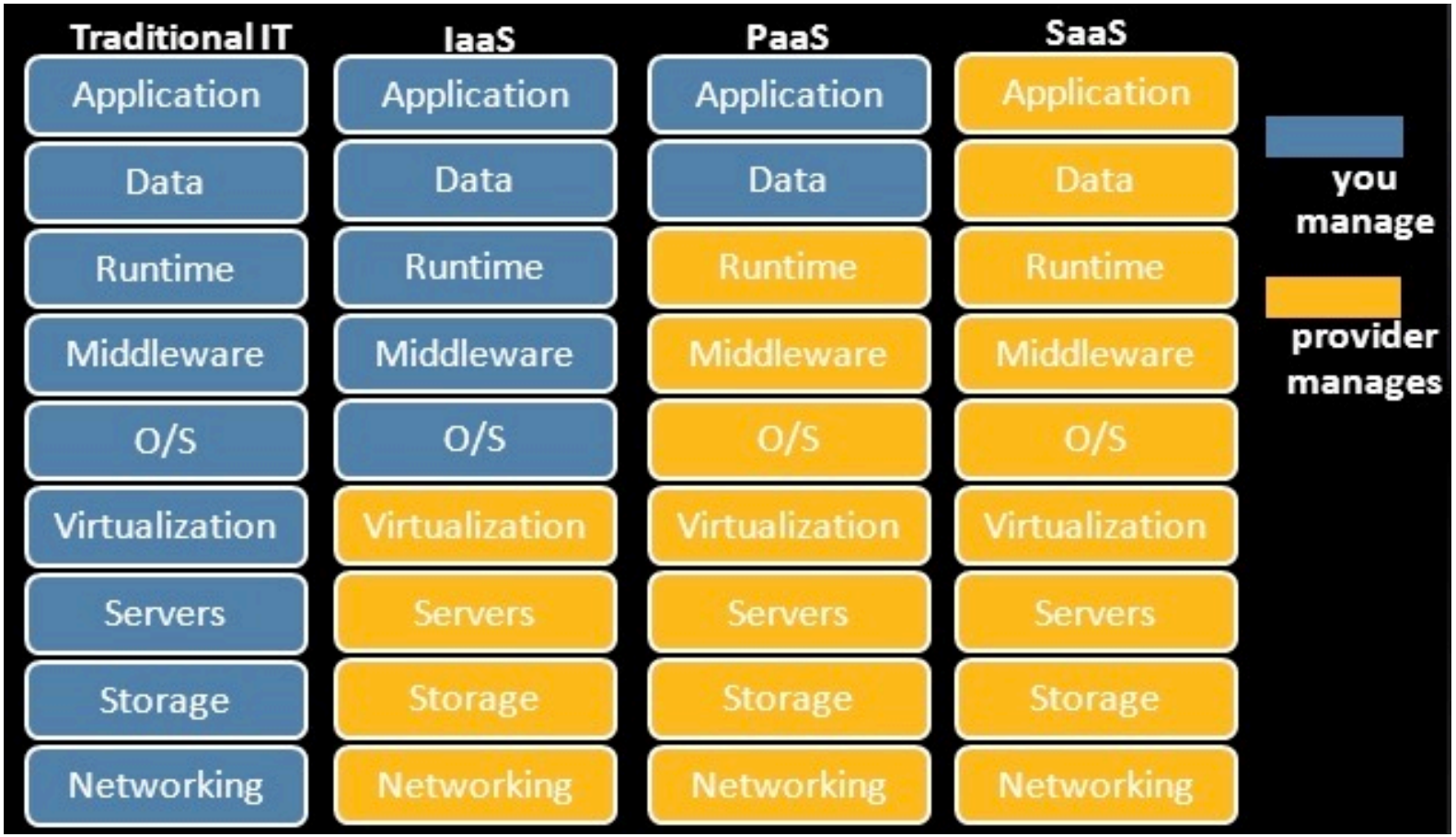


Source : Tanzim *et al.* 2012

- Cloud advantages
  - Rapid deployment
  - Cost reduction
  - Massive scalability
  - Pay-per-use


Pizza as a Service
Traditional On-Premises (On Prem)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Dining Table
Soda
Electric / Gas
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Made at home
Take & Bake
Pizza Delivered
Dined Out
You Manage
Vendor Manages

Cloud Computing



Cloud computing: Avantages

- Cloud use
  - Rapid deployment
  - Cost reduction
  - Massive scalability
  - Pay-per-use

- Example

The New York Times Archives + Amazon Web Services = The New York Times TimesMachine

  - 150 years of archives to export
  - 14 years of local treatment
  - 36 hours on Amazon for 240 dollars

Botnet + Cloud = Botcloud

Botclouds: Avantages

- Setup on demand, on a very large scale
- Completely legal process
- Record time with minimal effort
- Does not require a dissemination phase
- Attack as a Service

- Very dynamic and widely distributed attacks
- The anonymity of the attacker is often guaranteed

Botclouds: Examples

[Kassidy et al. 2011] **:**

- Setting up a botcloud on Amazon EC2
- DDoS (Flooding and click fraud) attacks

[Hayati et al. 2012] **:**

- Implementation of Botclouds within 5 known CSPs
- Carrying out many types of attacks (DDoS, shellcode, malformed traffic, etc.)
- 21-day period (48 hours non-stop for DDoS attacks)

Thomas Roth :

- Setting up a botcloud on Amazon EC2
- Break WPA keys in 6 mins for around $ 2 (Brute Force)

[Hammi et al. 2014, Hammi et al. 2015] **:**

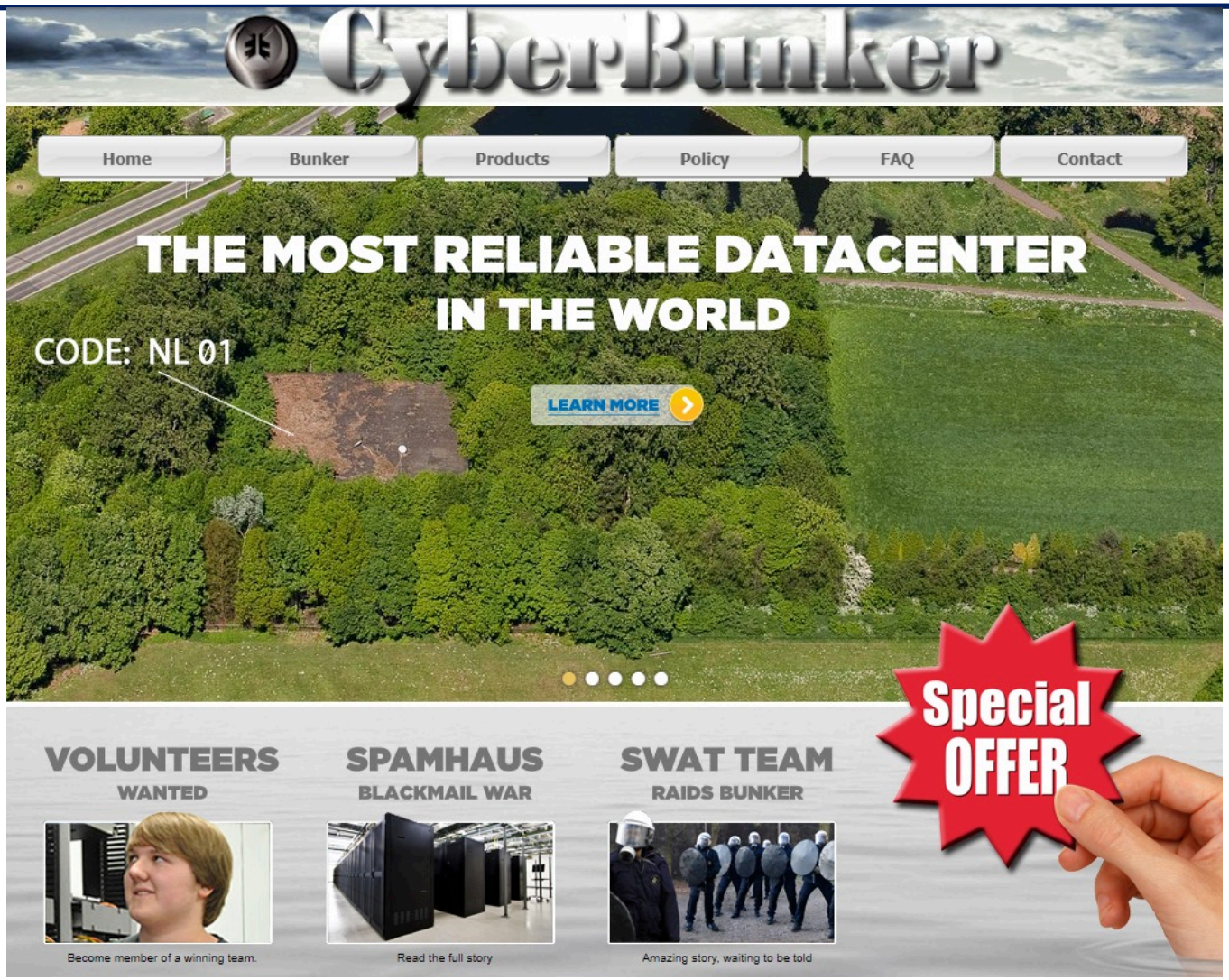
- Implementation of a Botcloud
- Around 50 VMs
- Realization of TCP and UDP flood attacks

Botclouds: Examples

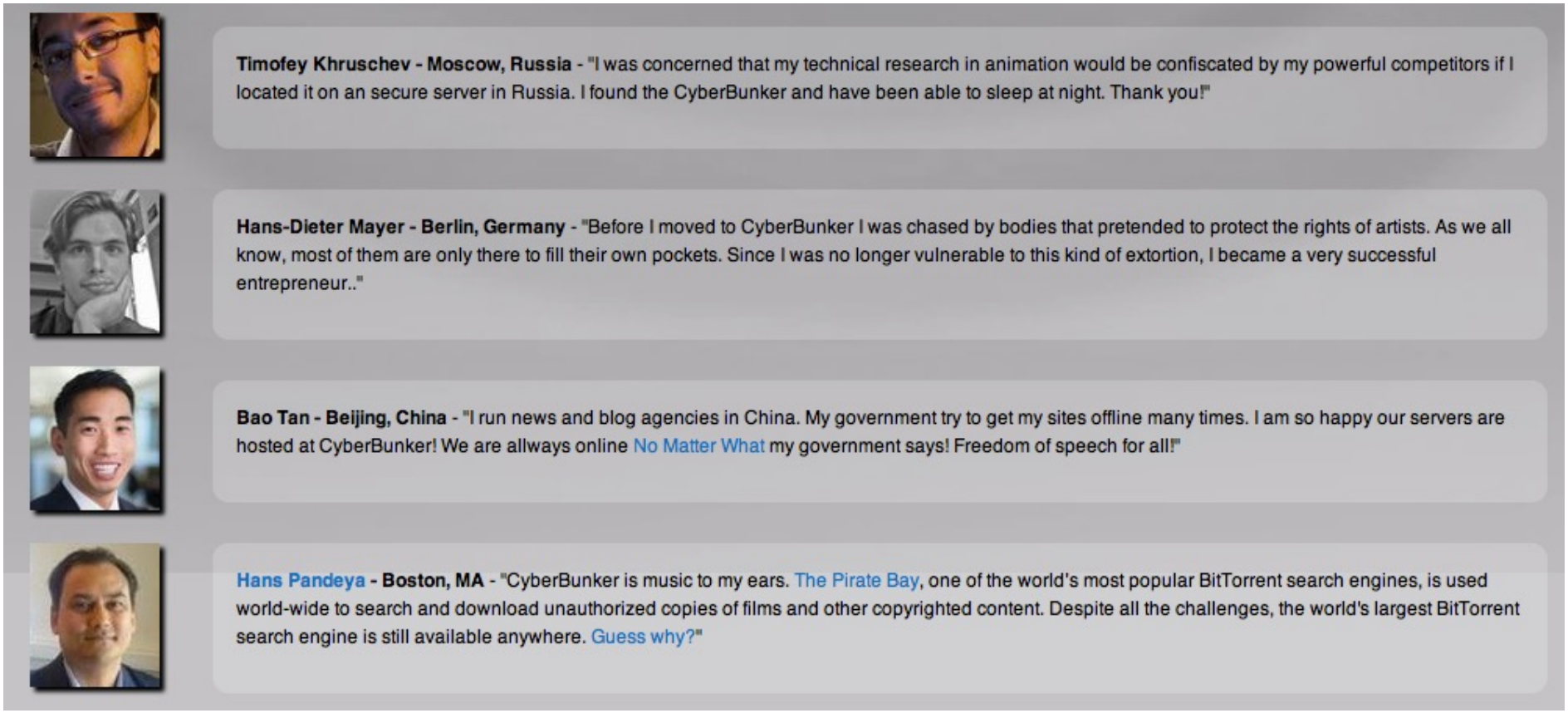
Attack on PlayStation Network and Qriocity :

- By Anonymous to defend George Hotz (GeoHot)
- Out of service for several months
- Personal and bank data theft of over 25 million (100 million) users
  - 2.2 million cards were sold
- Losses during decommissioning
- Losses for compensation
- Legal proceedings against SONY (Announcement after 6 days)

New dimension for DDoS



New dimension for DDoS



Timofey Khruschev - Moscow, Russia - "I was concerned that my technical research in animation would be confiscated by my powerful competitors if I located it on an secure server in Russia. I found the CyberBunker and have been able to sleep at night. Thank you!"

Hans-Dieter Mayer - Berlin, Germany - "Before I moved to CyberBunker I was chased by bodies that pretended to protect the rights of artists. As we all know, most of them are only there to fill their own pockets. Since I was no longer vulnerable to this kind of extortion, I became a very successful entrepreneur.."

Bao Tan - Beijing, China - "I run news and blog agencies in China. My government try to get my sites offline many times. I am so happy our servers are hosted at CyberBunker! We are allways online No Matter What my government says! Freedom of speech for all!"

Hans Pandeya - **Boston, MA** - "CyberBunker is music to my ears. The Pirate Bay, one of the world's most popular BitTorrent search engines, is used world-wide to search and download unauthorized copies of films and other copyrighted content. Despite all the challenges, the world's largest BitTorrent search engine is still available anywhere. Guess why?"

Mind Your Own Business

CyberBunker does not poke around on your servers. Customers are allowed to host any content they like except child porn and anything related to terrorism. Everything else is fine. CyberBunker has adopted a policy not to mind our clients business. Our famous "Mind Your Own Business" policy.

New dimension for DDoS

CyberBunker was an Internet service provider that, according to its website, hosts "services to any Web site 'except child pornography and anything related to terrorism'". It served as a host for The Pirate Bay and as one of the many WikiLeaks mirrors.[1][2] CyberBunker has also been accused of being a host for spammers, botnet command-and-control servers, malware and online scams.[3] The company has also been involved in Border Gateway Protocol hijacks of IP addresses used by Spamhaus and the United States Department of Defense.[4] The Spamhaus hijack was part of an exceptionally large distributed denial of service attack launched against them in March 2013. Because of the size of this attack it received considerable mainstream media attention. [wikipedia]

New dimension for DDoS

- Attaque sur Spamhaus > 100 GBps 2013 ➔ cyberBunker

Security

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus

Plucky mail scrubbers battle internet carpet bombers

By John Leyden 27 Mar 2013 at 17:03 124 SHARE ▼

The Biggest Cyber Attack In History Is Taking Place Right Now

Dylan Love 27 Mar 2013, 14:14

New dimension for DDoS

Security

600 armed German cops storm Cyberbunker hosting biz on illegal darknet market claims

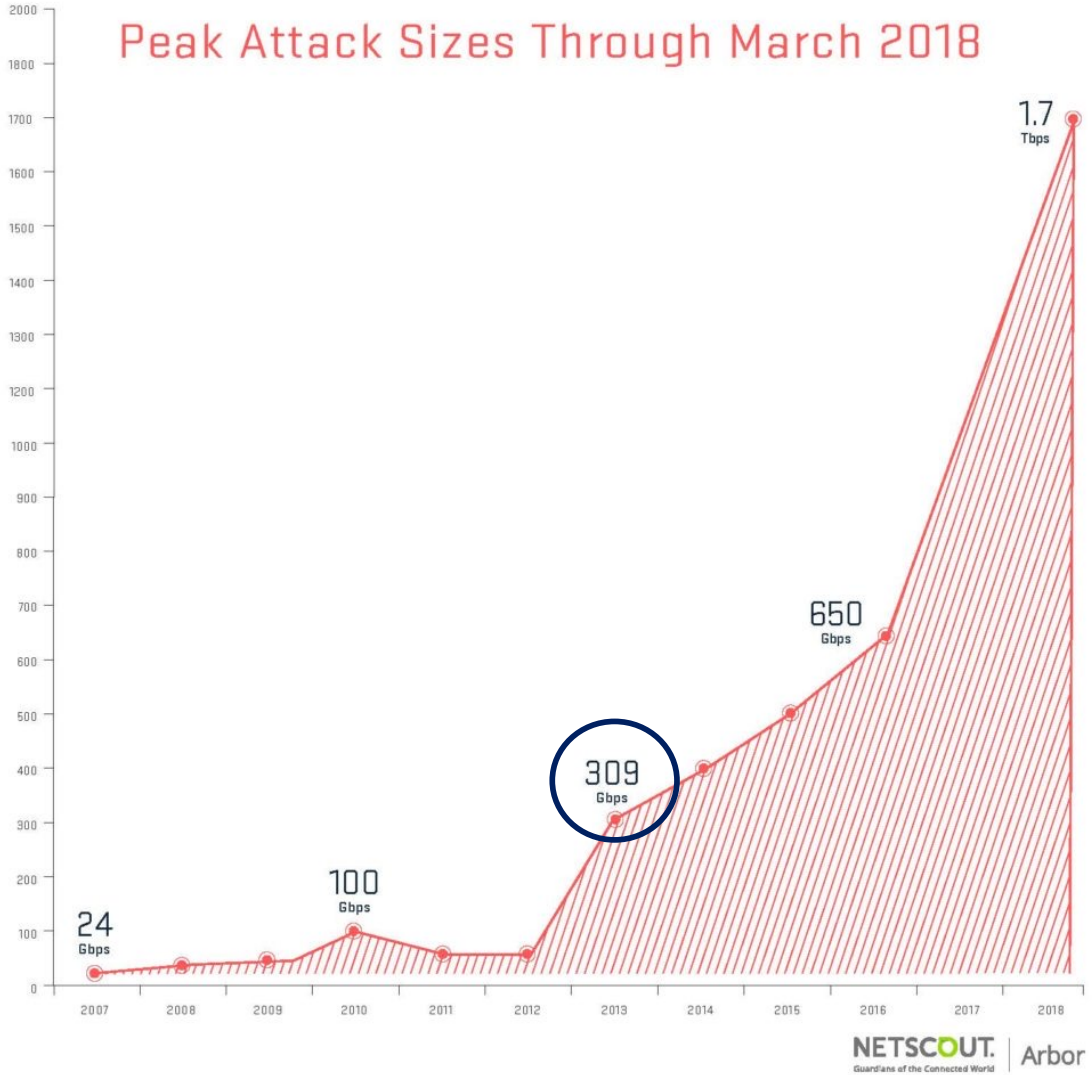
Look, it's CB3ROB – remember them?

By Gareth Corfield 30 Sep 2019 at 14:54 85 SHARE ▼

The bunker is around 96km (60 miles) west of Frankfurt.

CB3ROB has a reasonably long history of providing hosting services to what the rest of the world might regard as the murkier ends of the internet. If German police and prosecutors are to be believed, at the time of the raid CB3ROB was hosting several darknet souks, including ones themed around the sale of "drugs, weapons, counterfeit documents and stolen data" as well as allegedly hosting "sites distributing child [sex abuse material]".

Botnets/DDoS: a danger



New dimension for DDoS: Booters

What is an IP stresser?

An IP stresser is a tool designed to test a network or server for robustness. The administrator may run a stress test in order to determine whether the existing resources (bandwidth, CPU, etc.) are sufficient to handle additional load.

Testing one's own network or server is a legitimate use of a stresser. Running it against someone else's network or server, resulting in denial-of-service to their legitimate users, is illegal in most countries.

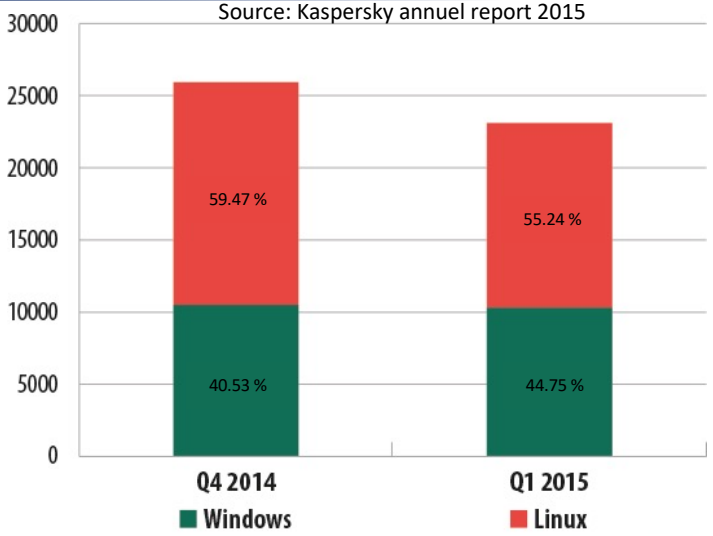
Research problem

- DDoS attacks are easy to detect however they represent a persistent challenge for academia and industry

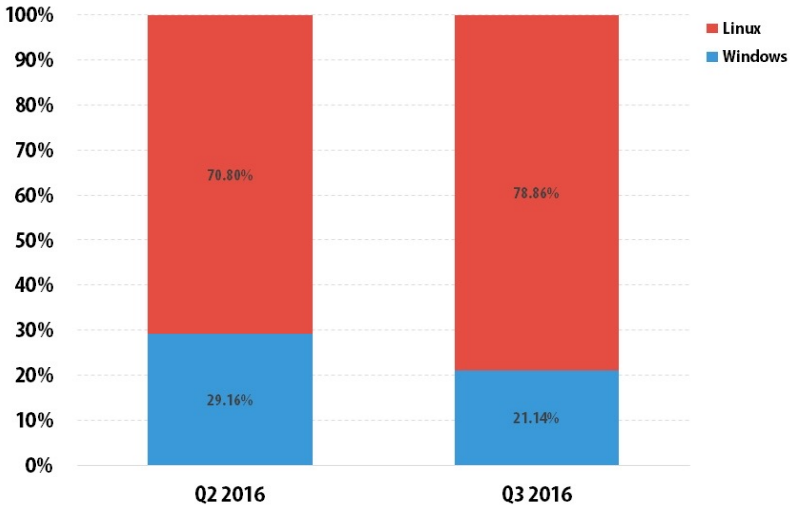
- **Because they are in constant evolution**

Botnets: Correlation between Linux vs Windows based botnets

Source: Kaspersky annuel report 2015



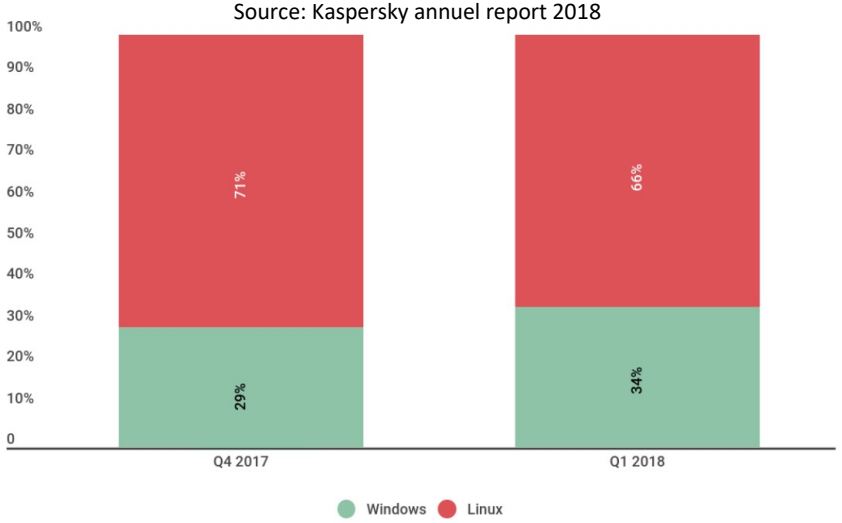
Source: Kaspersky annuel report 2016 © Kaspersky Lab



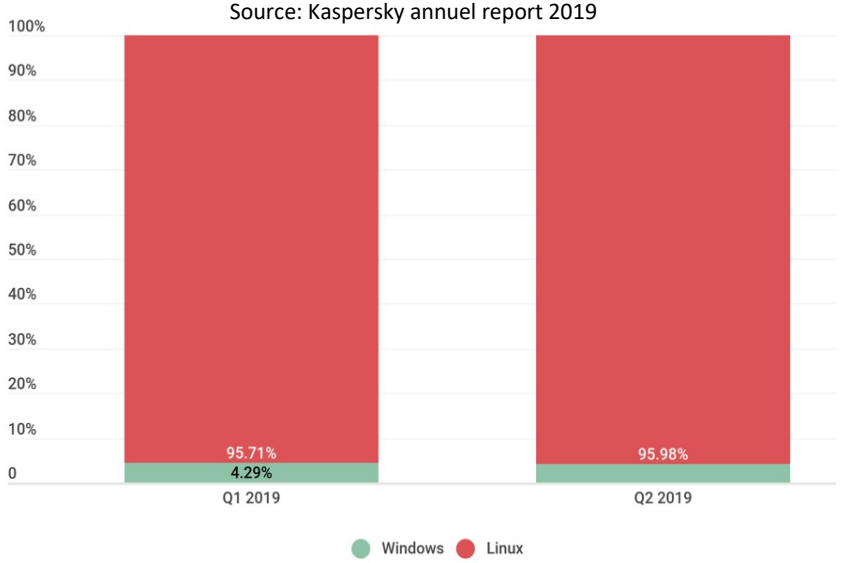
© 2016 AO Kaspersky Lab. All Rights Reserved.

Badis HAMMI

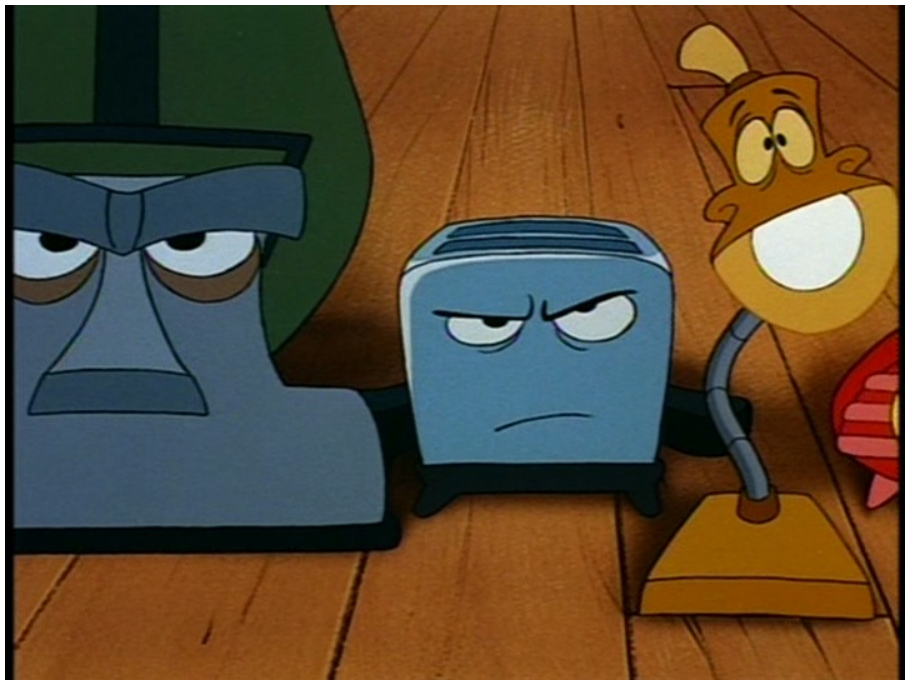
Source: Kaspersky annuel report 2018

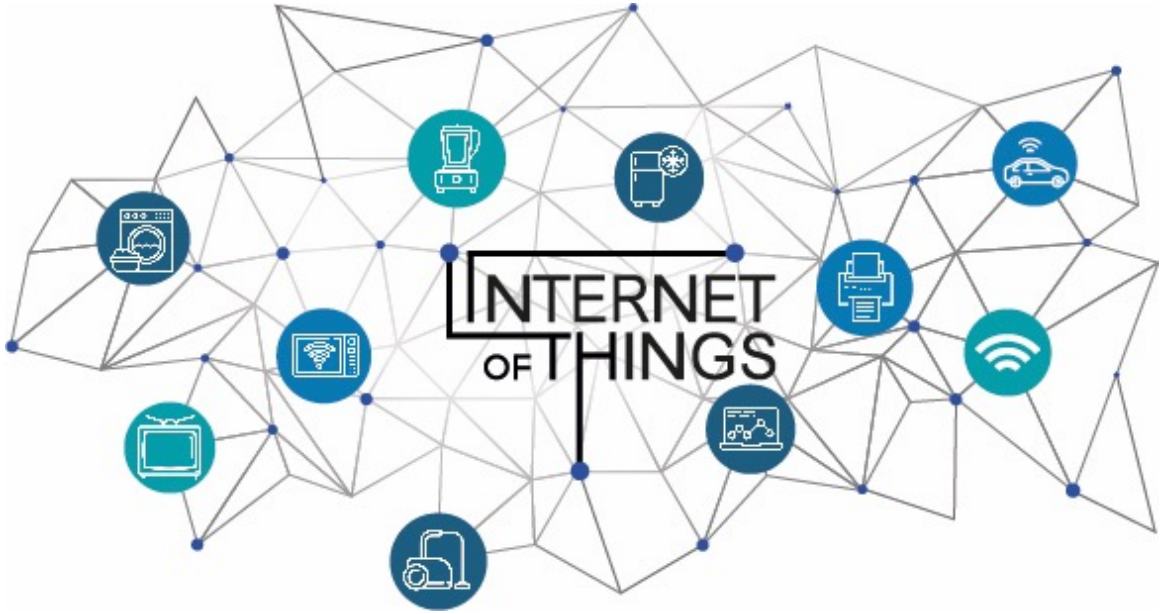


Source: Kaspersky annuel report 2019



New dimension for DDoS: Internet of Things





New dimension for DDoS: Internet of Things

- In the last few years, malware developers' have shown increasing interests in IoT devices
  - Ex: *Mirai*, *Bashlite* and *Silex*
- Exploite vulnerable IoT devices that used weak or default credentials to attempt brute force attacks and further add these devices to the botnet army

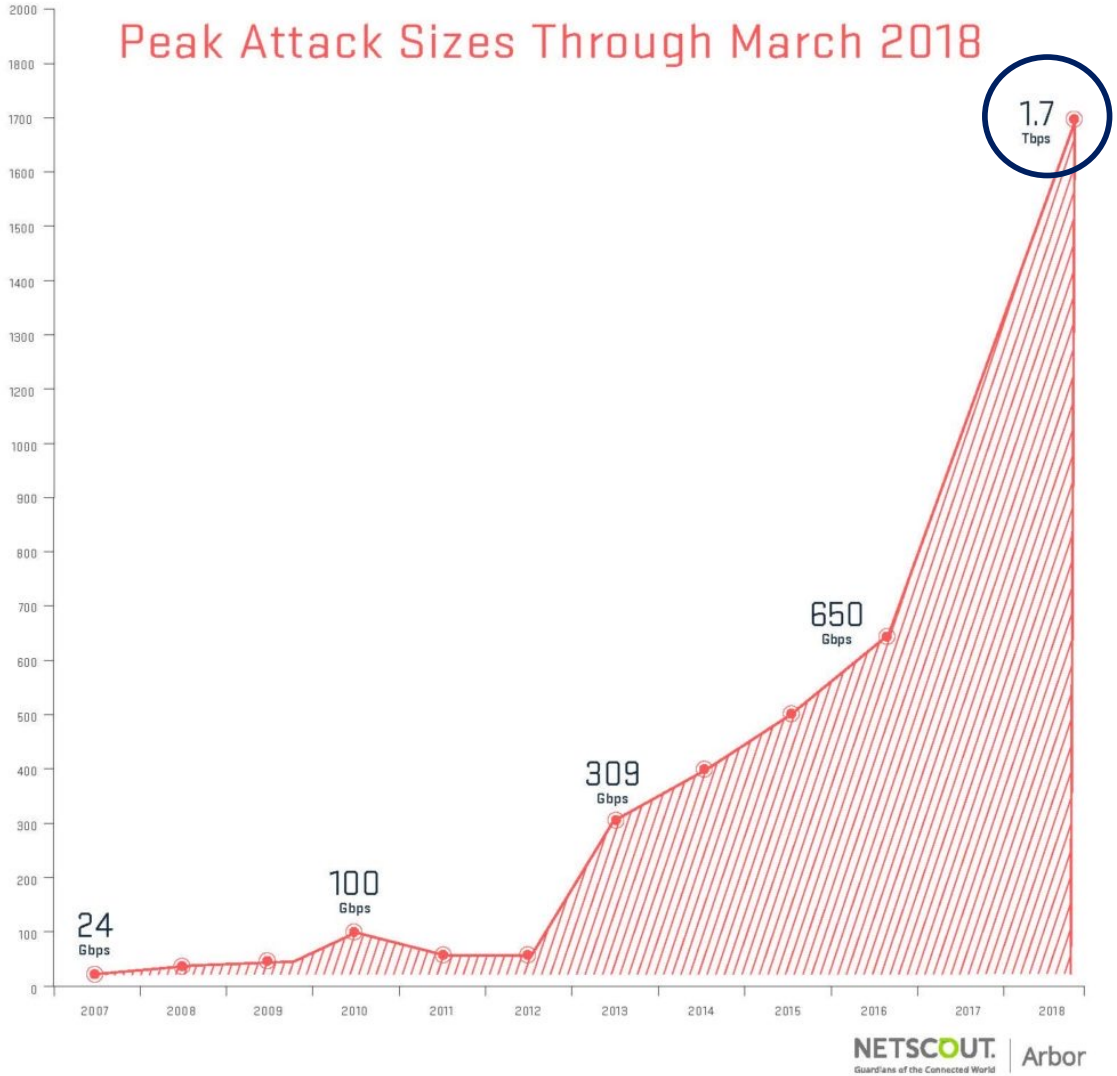
- The password management company *Splash-Data* evaluated more than five million passwords leaked on the Internet during the previous years and compiled the top 100 worst passwords
- Surprisingly, for the fifth straight year, the top spots (#1 and #2) in the annual worst-of-the-worst list remain unchanged**: "123456" and "password"**

Mirai

- Every bot that *Mirai* obtained, would scan for nearby vulnerable devices and report back to the Command and Control server
- It executes a brute force attack on the scanned devices relying on a small dictionary of **62 possible username/password** pairs that are common to IoT devices

New dimension for DDoS: Internet of Things

- A massive denial of service (DDoS) attack of **more than one Terabyte/s per second** targeting the Dyn Managed DNS service
- Many sites that use this service (different from DynDNS), such as **Twitter, Ebay, Netflix, GitHub, PayPal**, are **inaccessible for ten hours** (from 7 a.m. UTC to around 5 p.m. UTC)
- The attackers used pirated connected objects (such as surveillance cameras) infected with malware **Mirai** to relay the massive packet flow.
- According to the computer security company FlashPoint, this attack could well be the work of amateur hackers.



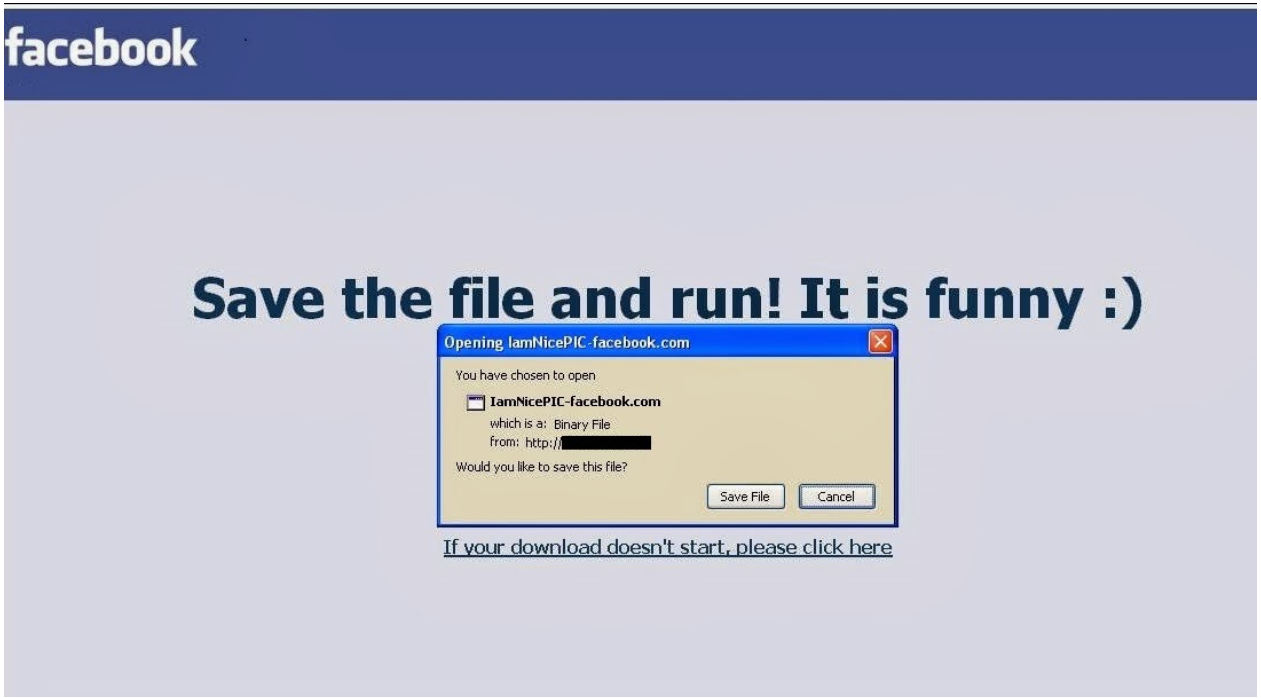
Types of malware

Common Vulnerabilities and Exposures

- CVE is a list of entries -each containing an identification number, a description, and at least one public reference- for publicly known cybersecurity vulnerabilities.
- CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).
- https://cve.mitre.org/index.html

Malwares

Malware is a general term that describes several types of malicious programs such as viruses, worms, rootkits, trojan horses, backdoors, botnets, spyware, adware, ransomware, etc. Every type of malware is classified based on certain unique characteristics like propagation methods, infection types, etc



Malwares: Virus

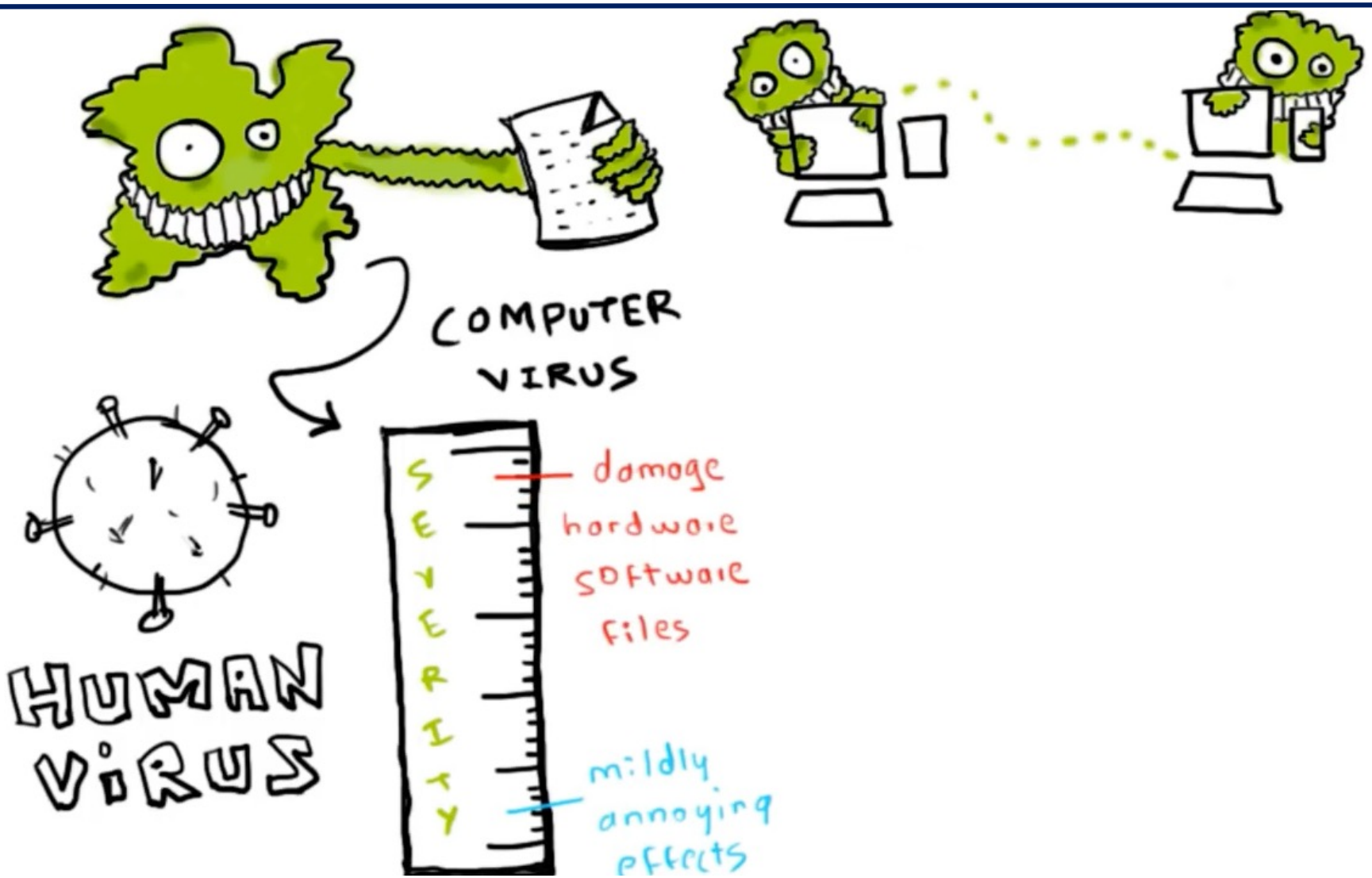
A virus is an unwelcome computer program that can infect legitimate host programs by attaching to a useful application or making copies of itself, causing damage to the host and the integrity of information. Viruses typically spread in one of the three ways (i) removable media; (ii) internet downloads; and (iii) e-mail attachments. When the infected code is executed, it might produce harmless activities like ***periodical illegitimate message alerts, slow startup, and performance, or more serious threats like degrading computer performance, formatting disks, damaging files or even crashing systems***

ceotodaymagazine.com

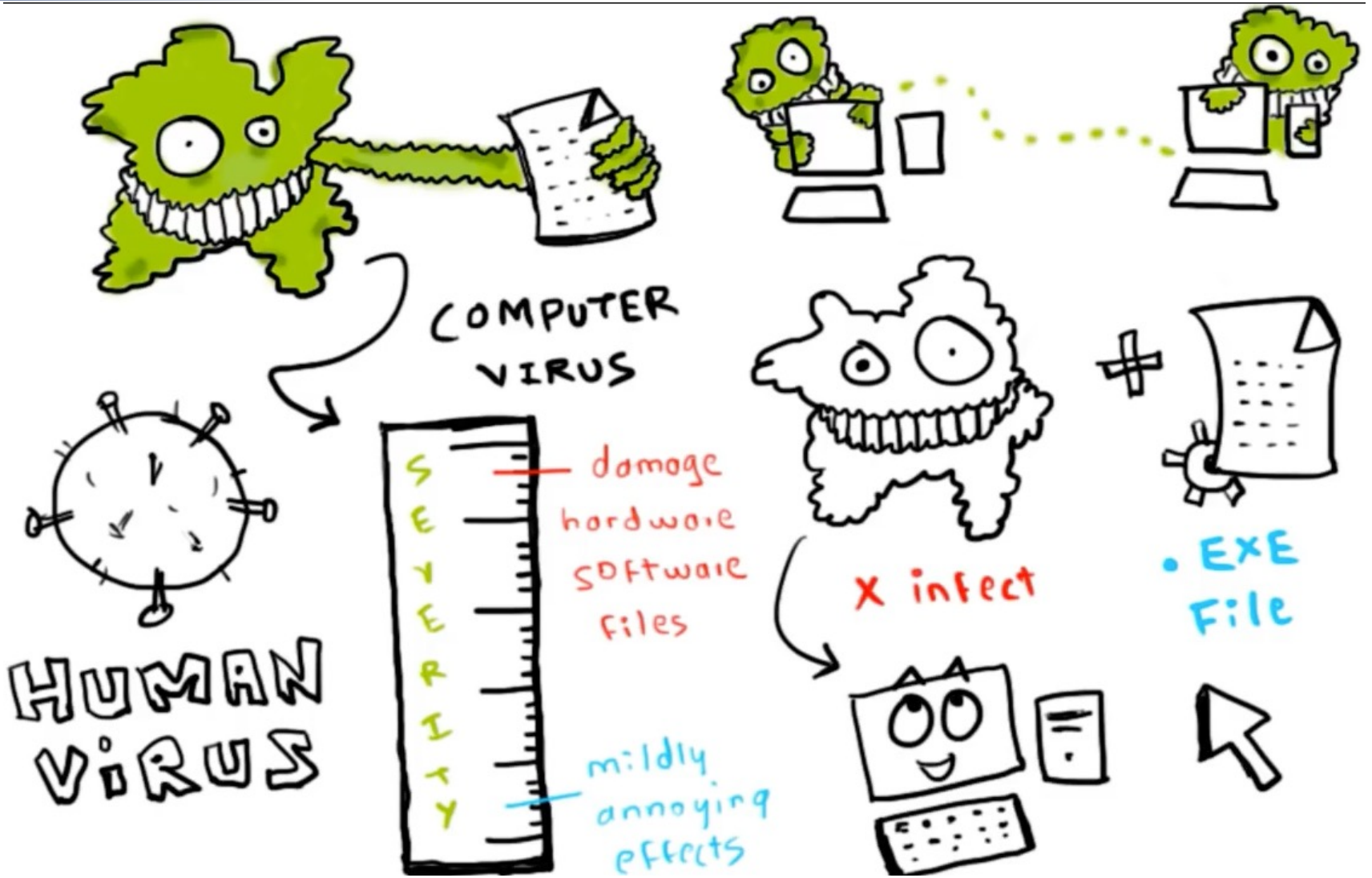
Malwares: Virus

Malwares: Virus

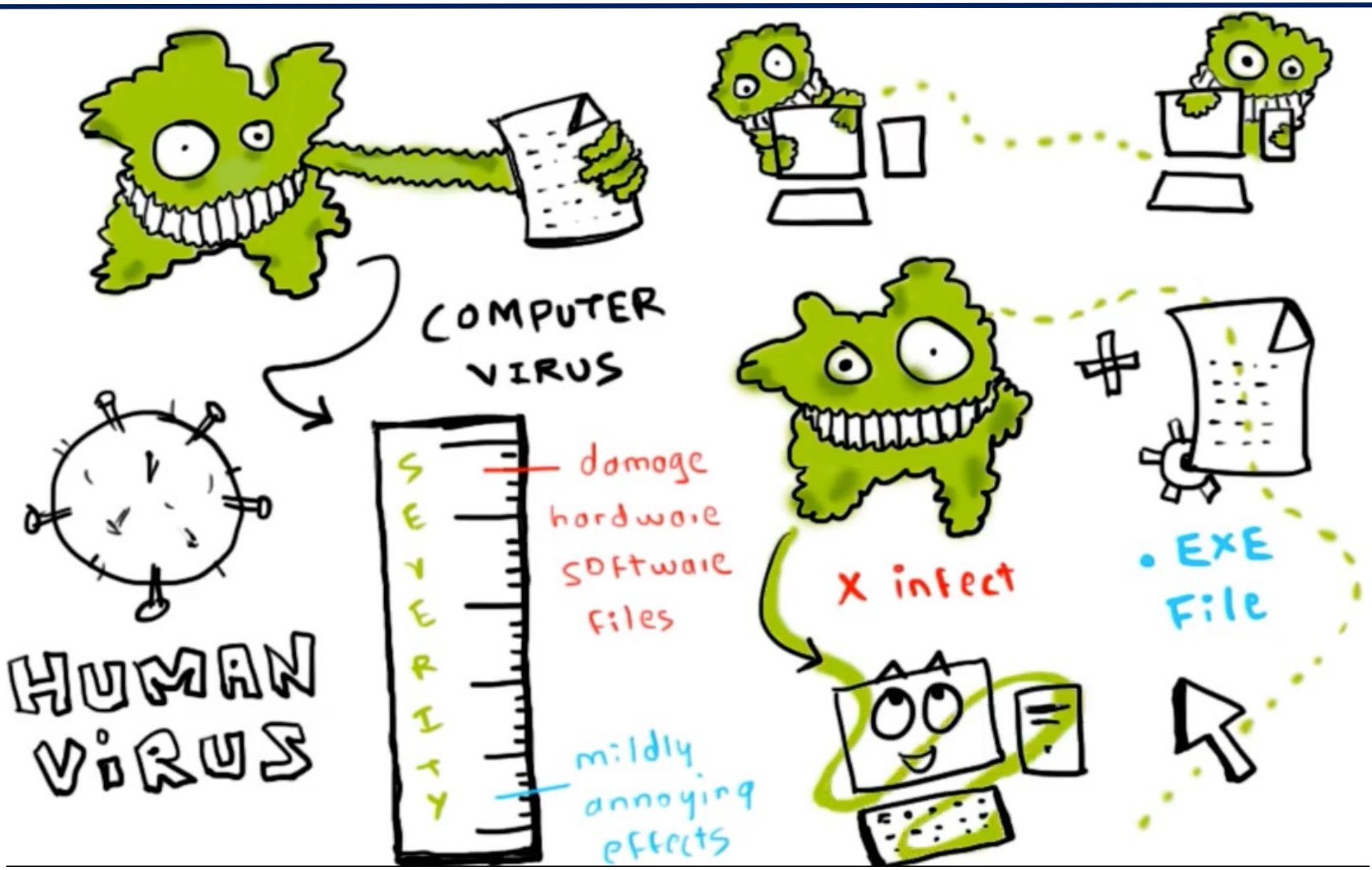
Malwares: Virus



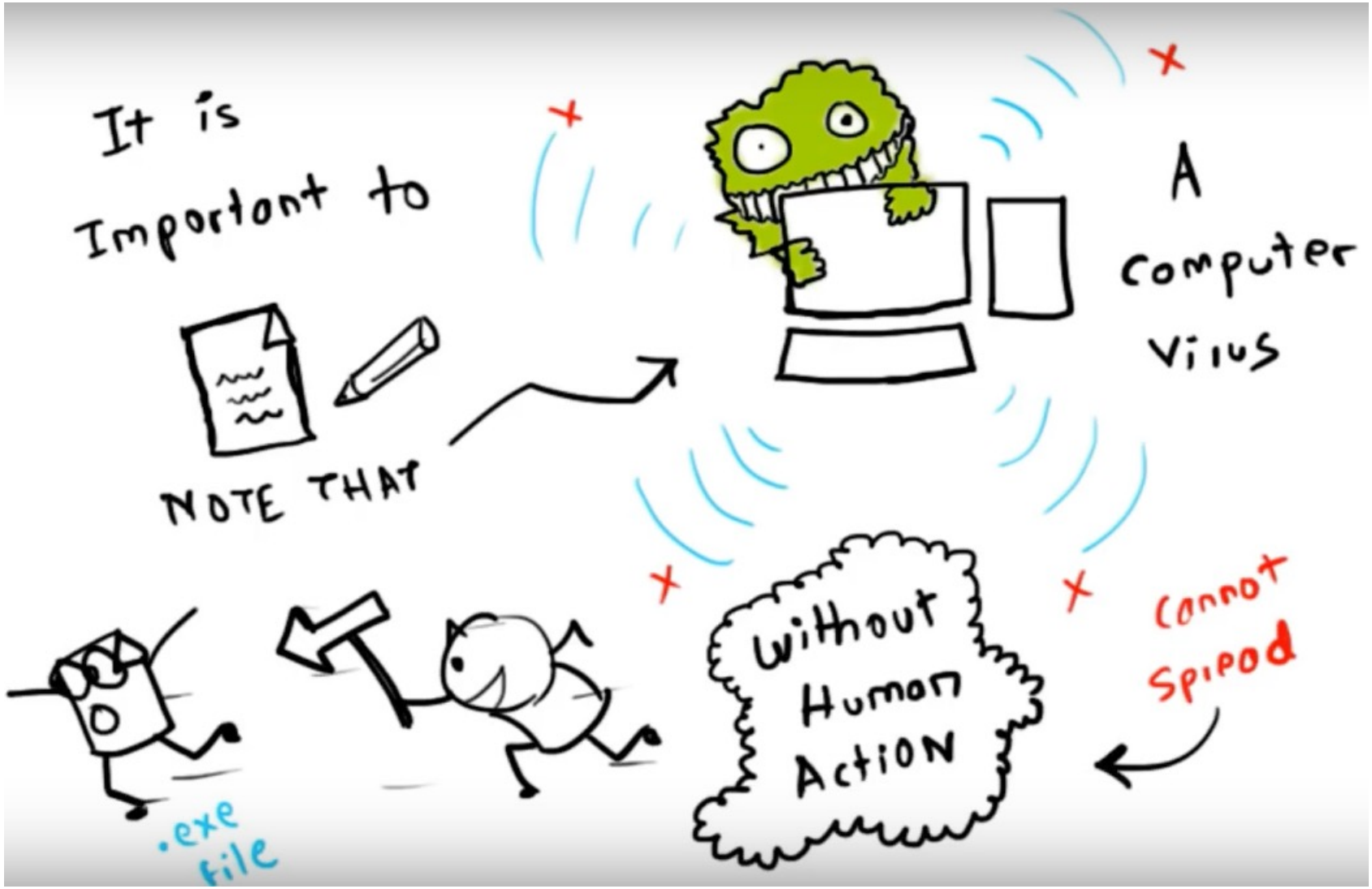
Malwares: Virus



Malwares: Virus



Malwares: Virus

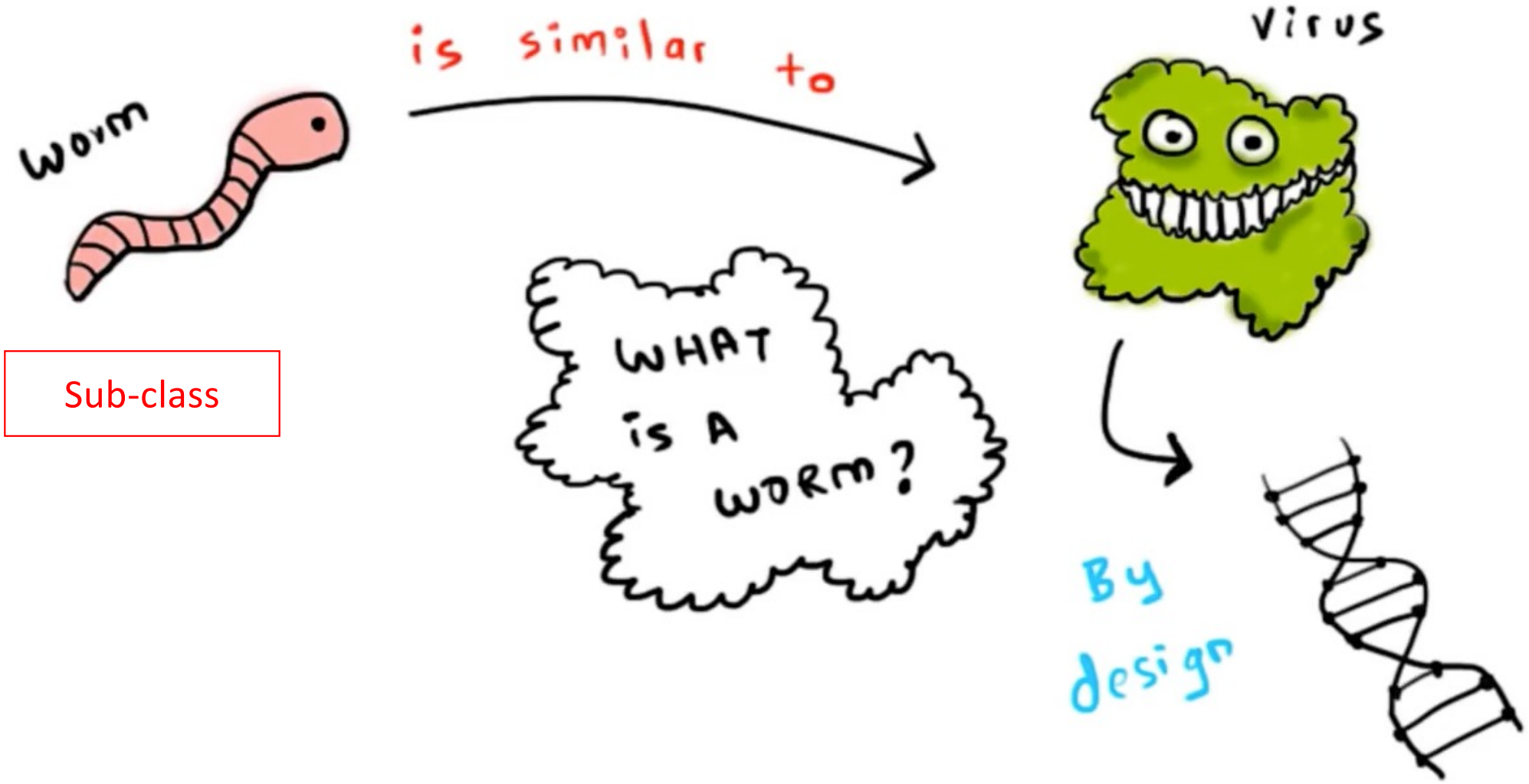


Malwares: Worm

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. More advanced worms leverage encryption, wipers, and ransomware technologies to harm their targets. (tools.cisco.com)

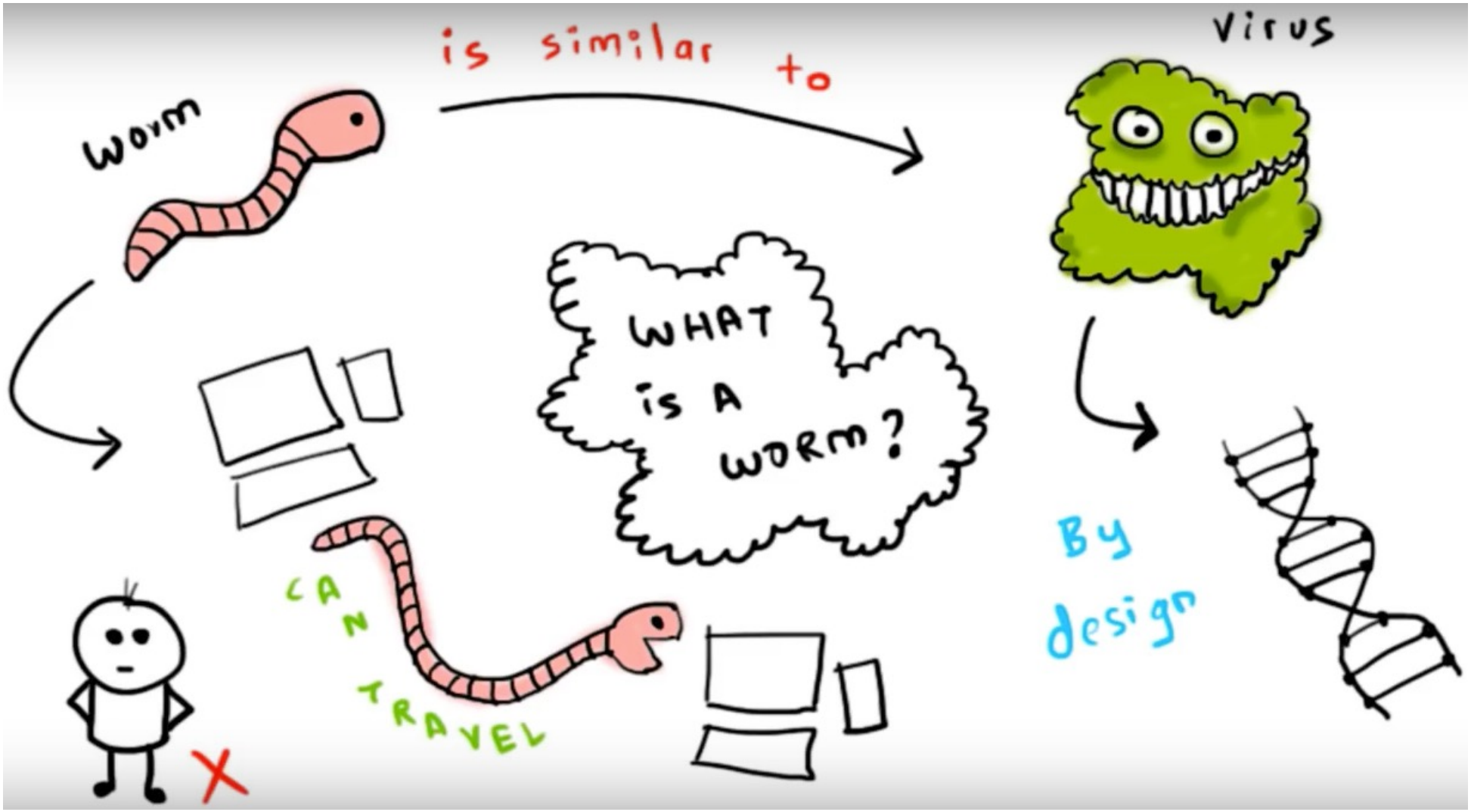
Avast.com

Malwares: Worm

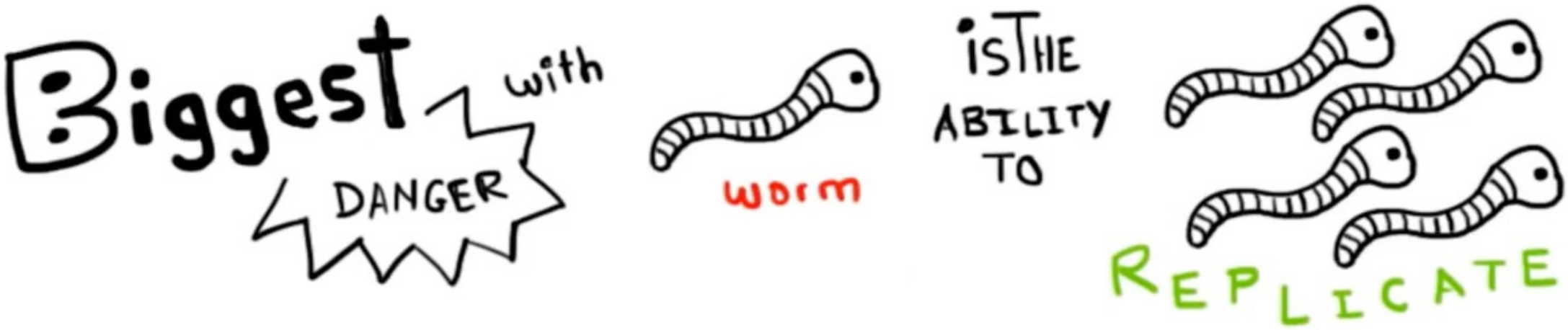


Sub-class

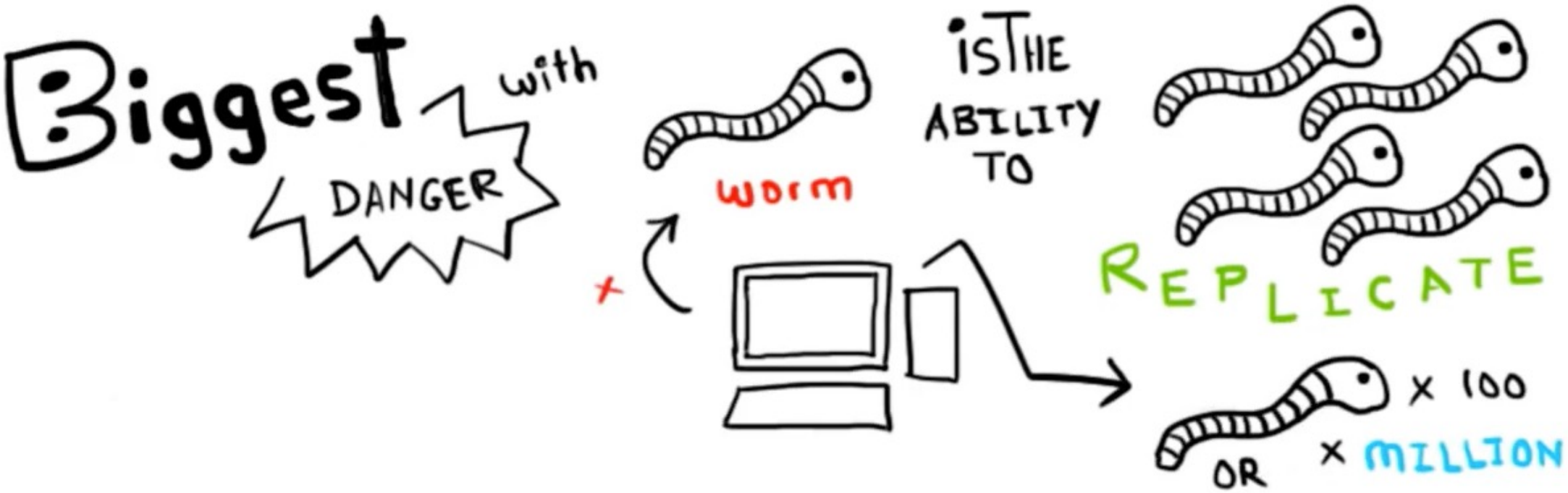
Malwares: Worm



Malwares: Worm



Malwares: Worm

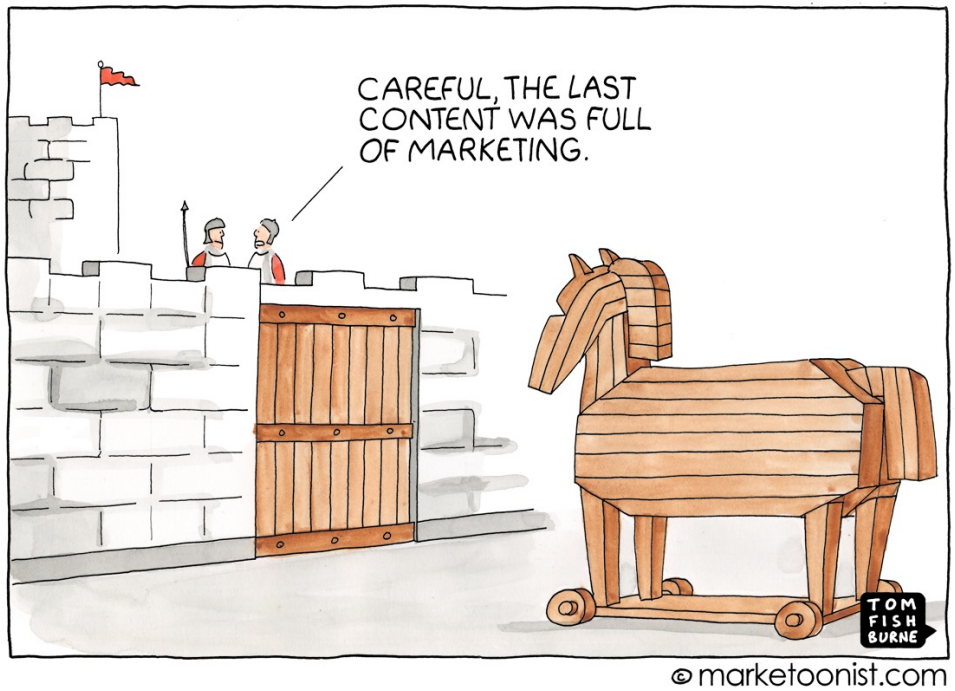


Malwares: Worm

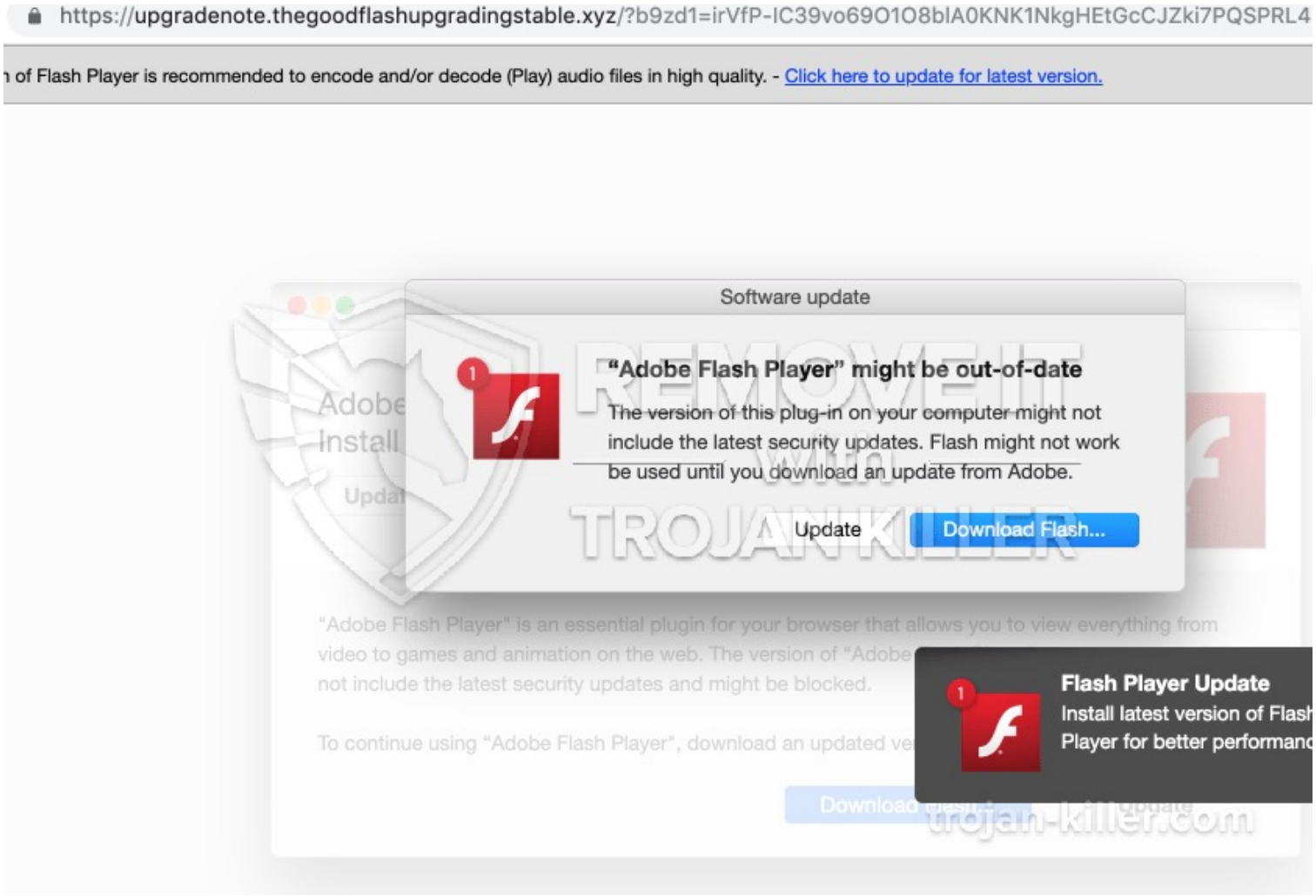
Malwares: Worm

Malwares: Trojans

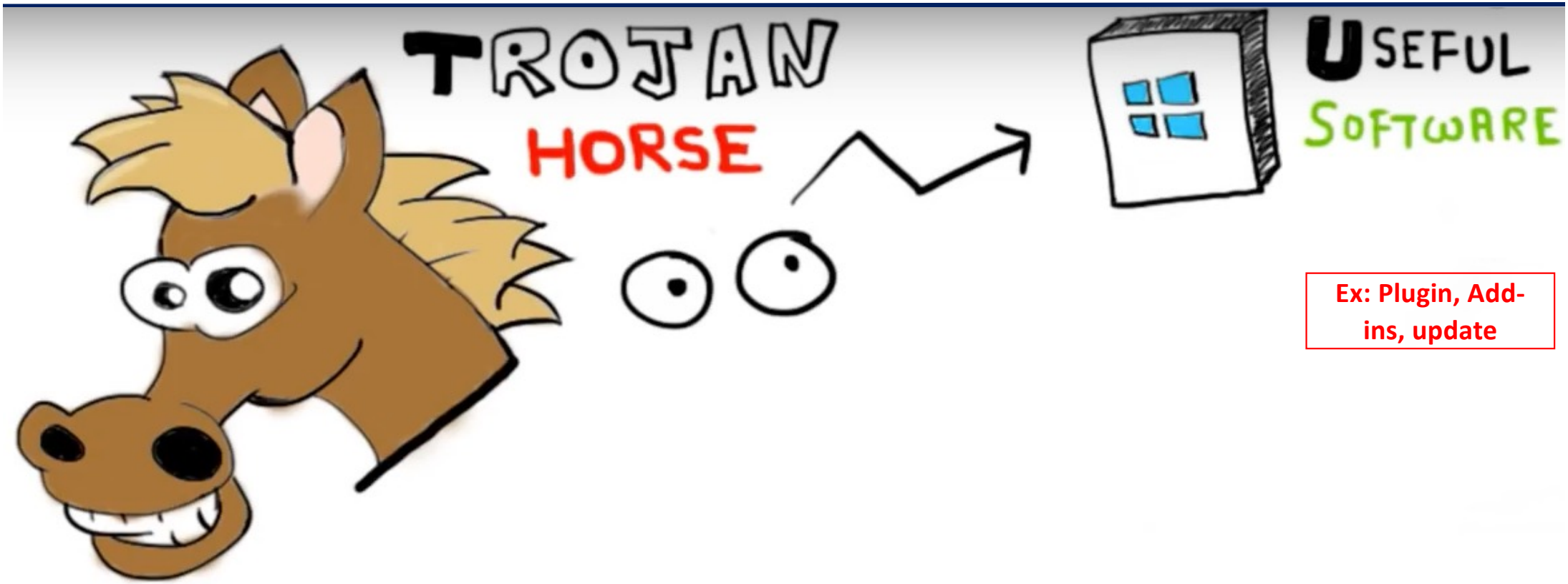
A Trojan is another type of malware named after the wooden horse that the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create backdoors to give malicious users access to the system. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet.



Malwares: Trojans

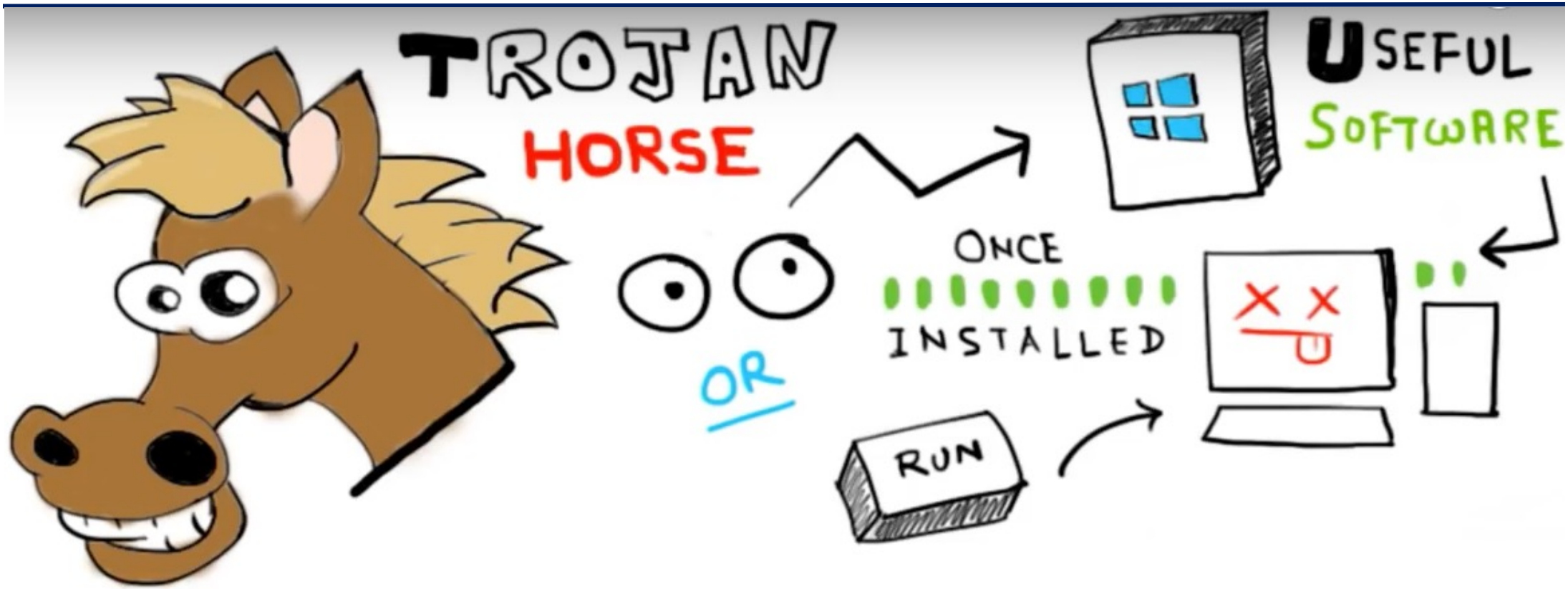


Malwares: Trojans

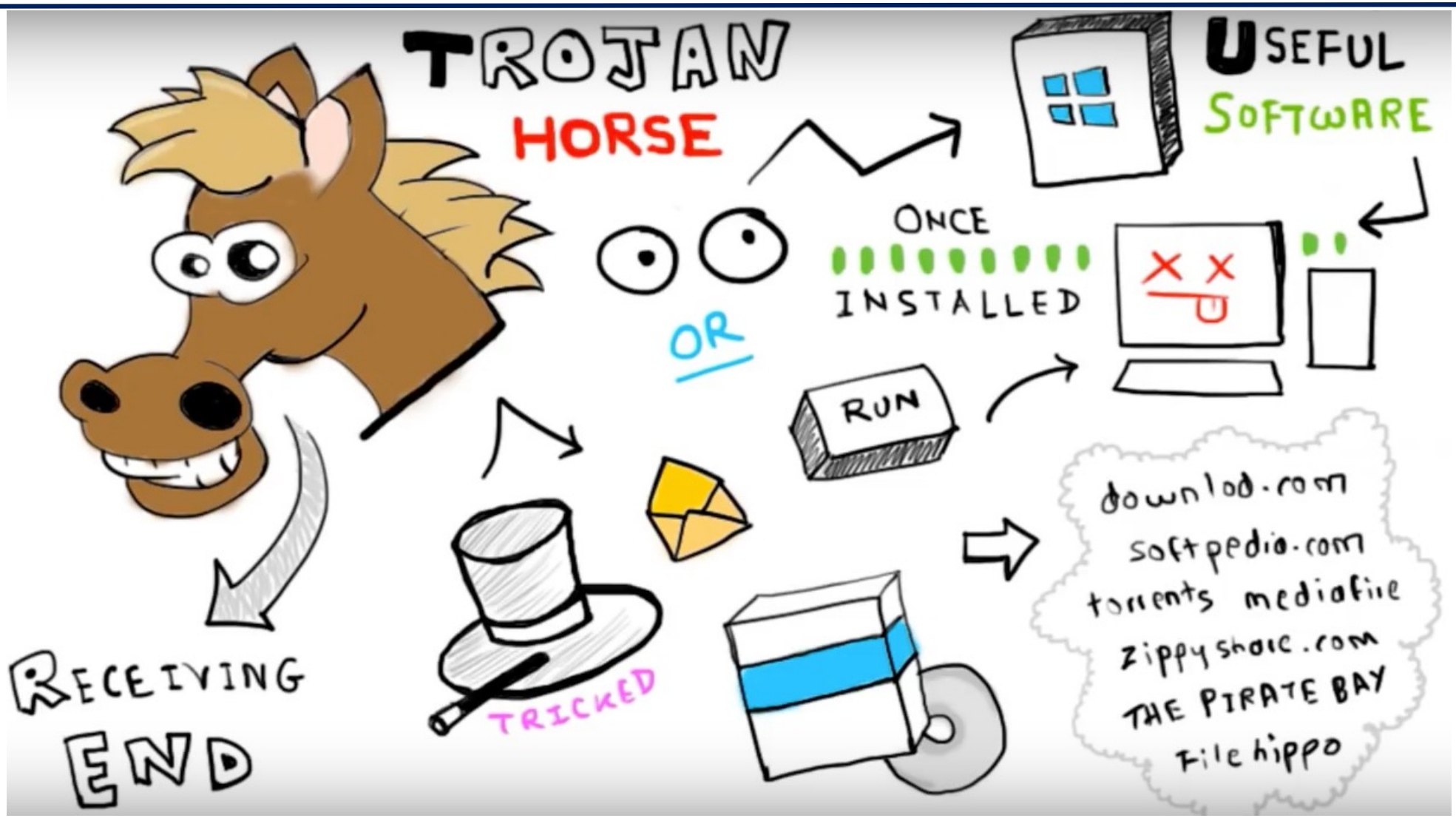


Ex: Plugin, Add-ins, update

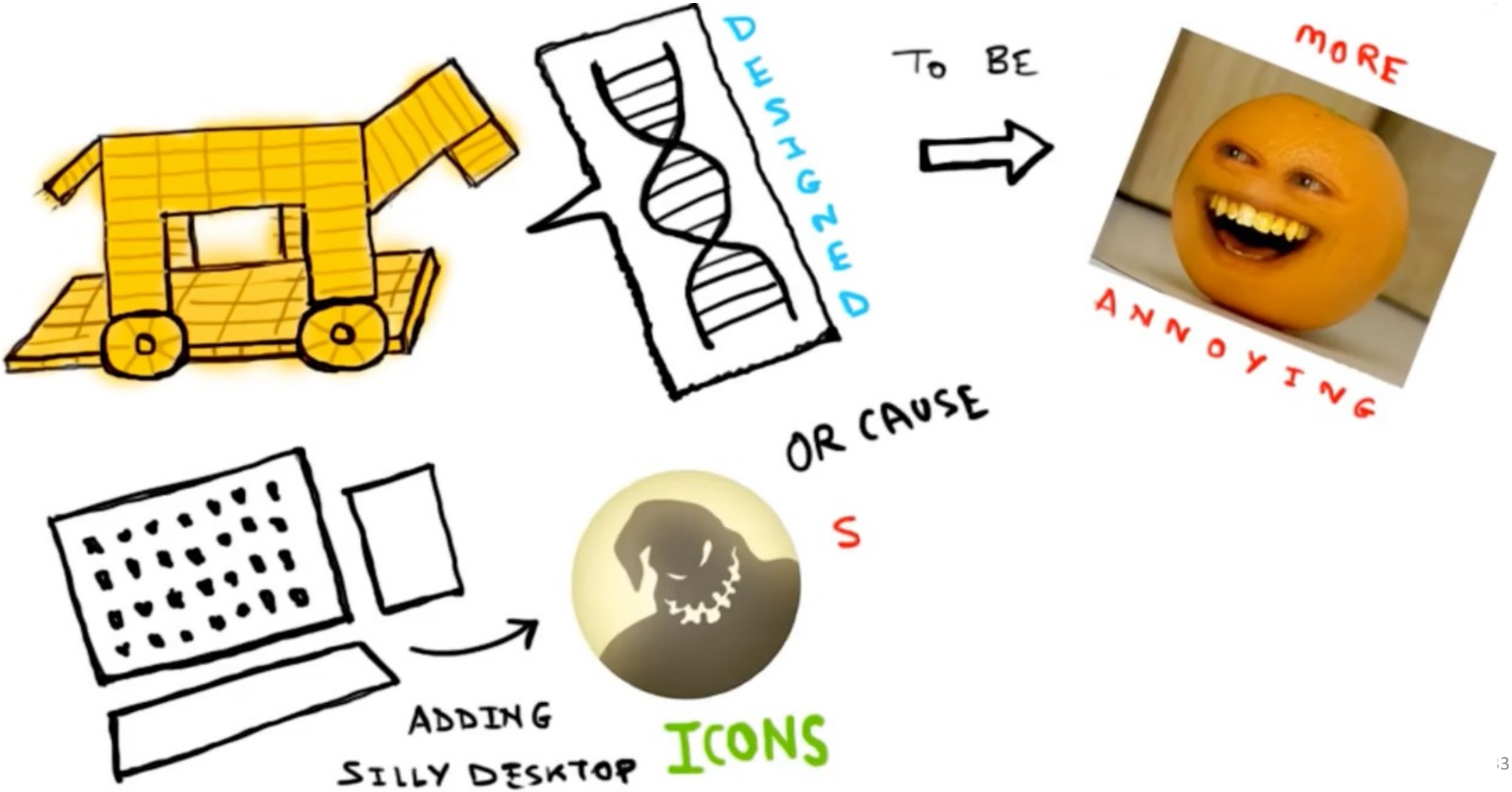
Malwares: Trojans



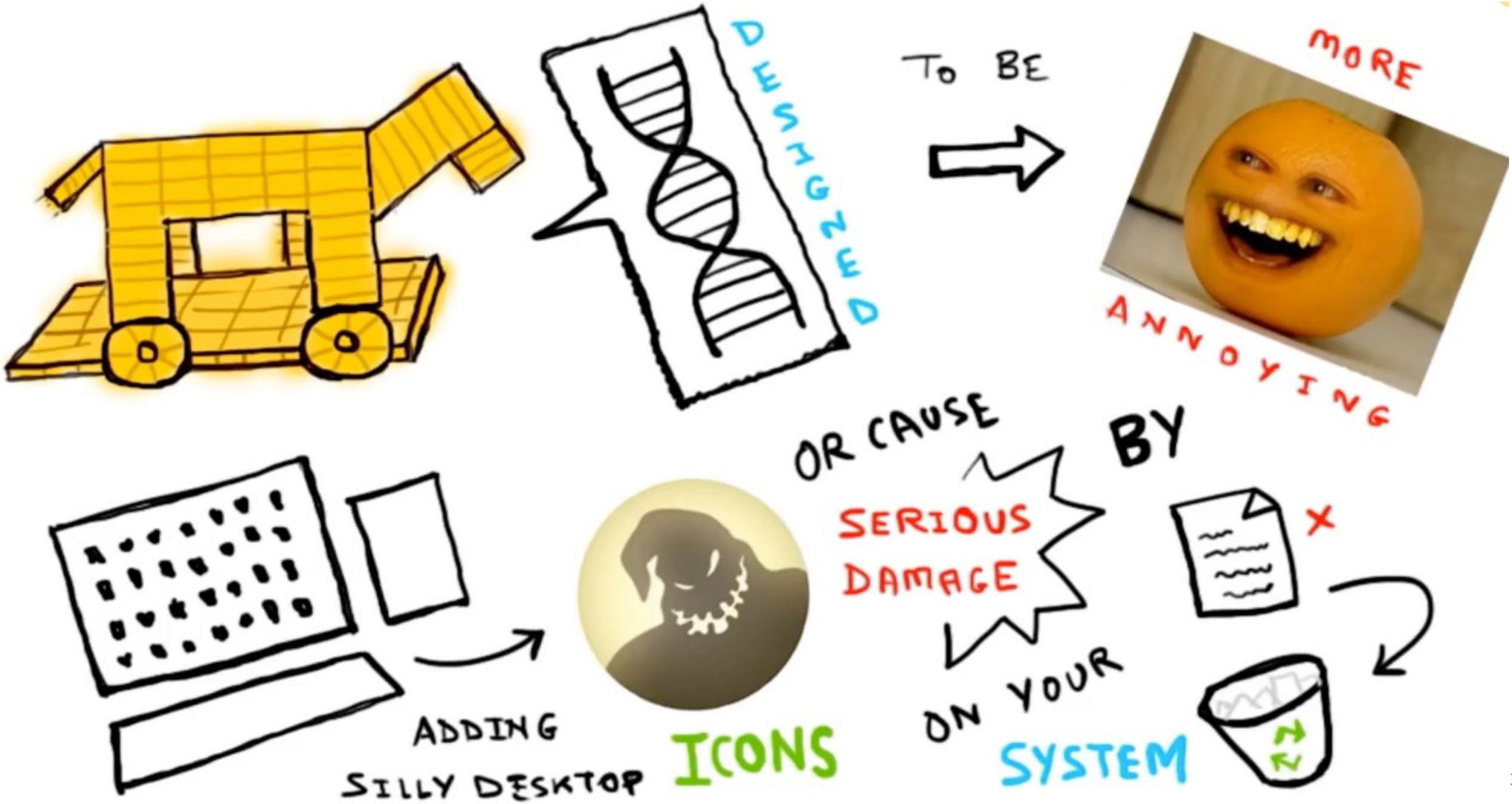
Malwares: Trojans



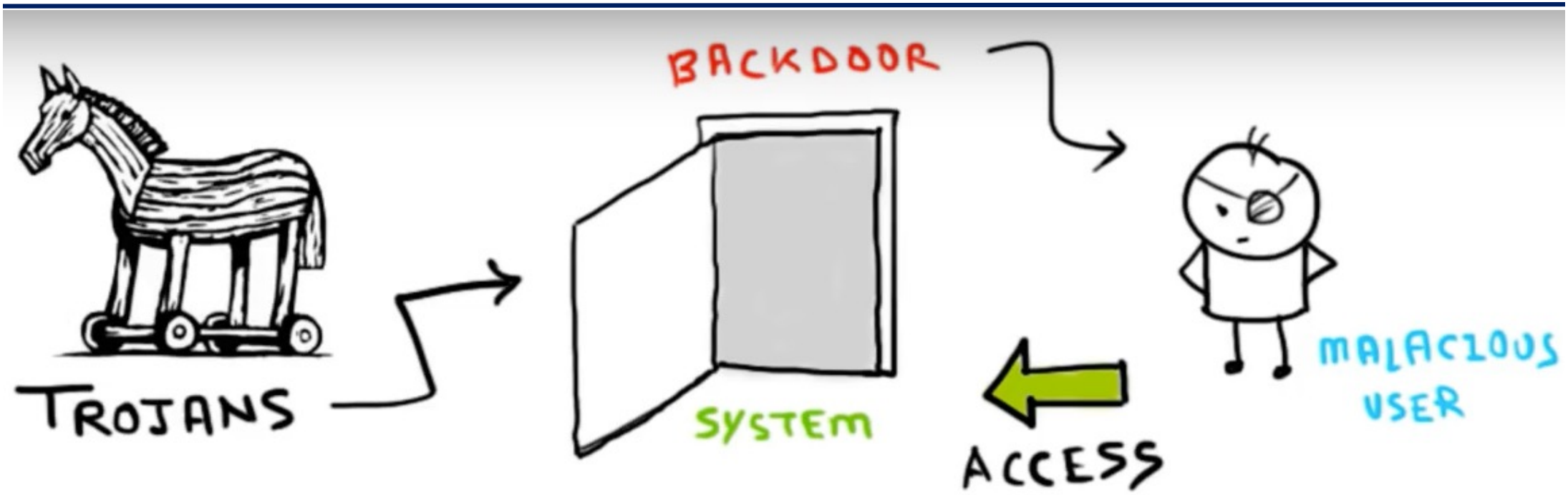
Malwares: Trojans



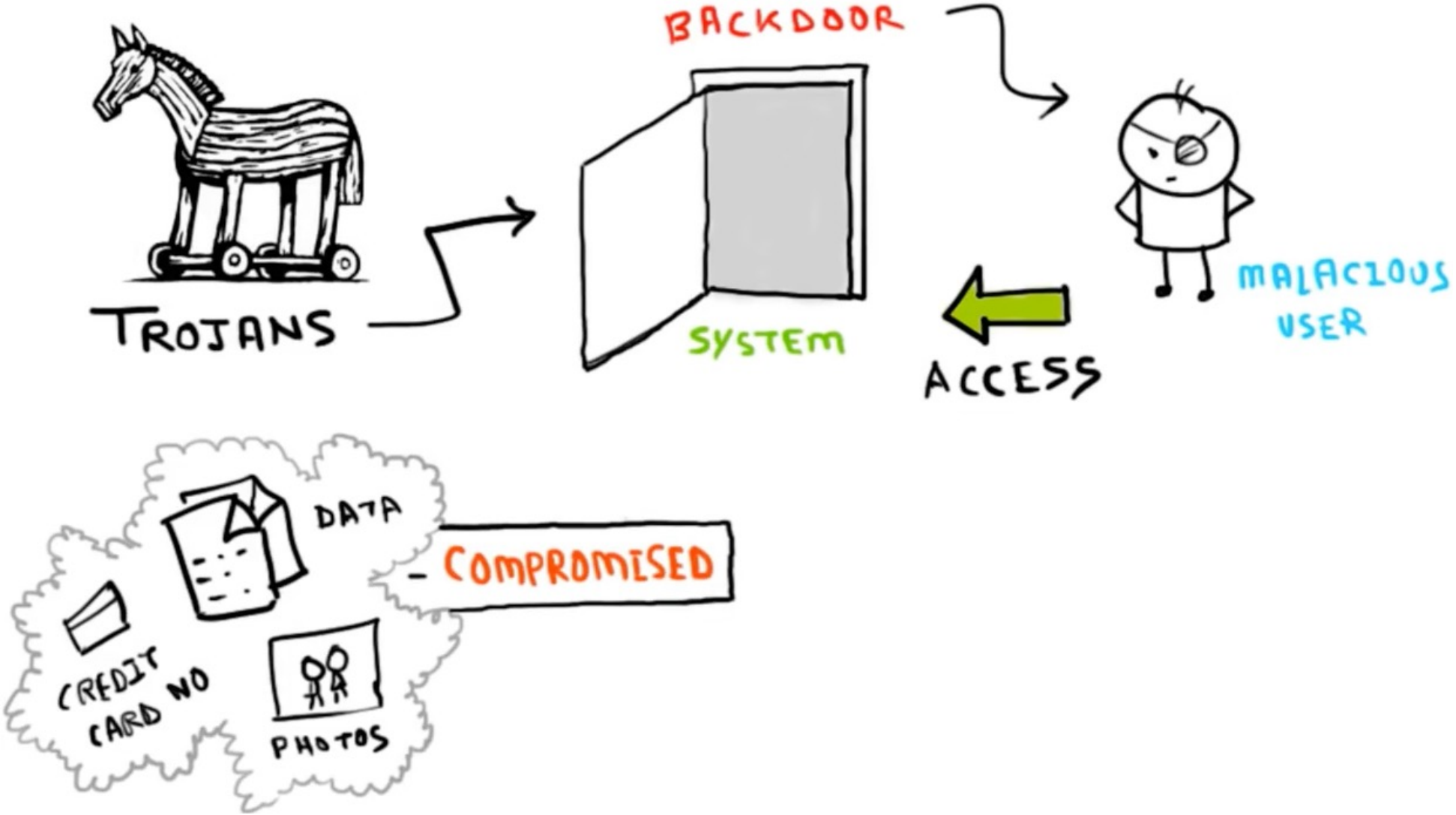
Malwares: Trojans



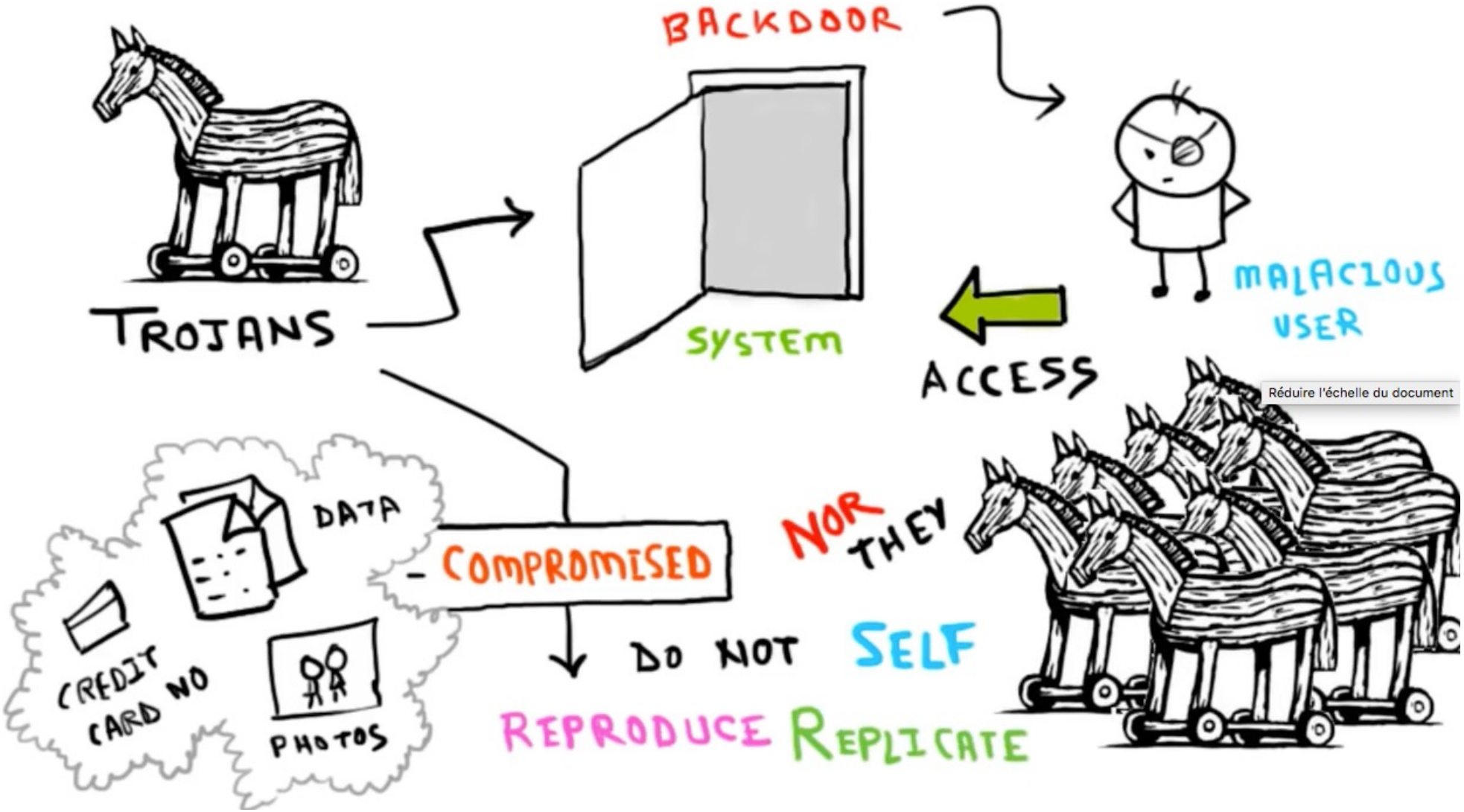
Malwares: Trojans



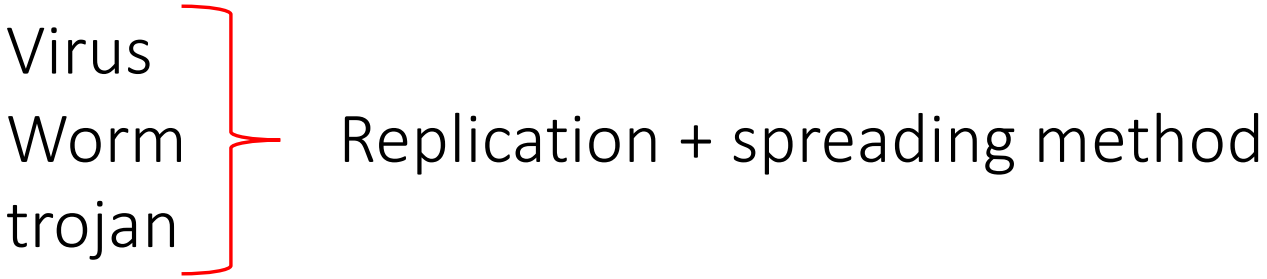
Malwares: Trojans



Malwares: Trojans



Malwares: Payload



The *payload* is the part of transmitted data that is the actual intended message. *Headers* and *metadata* are sent only to enable *payload* delivery.

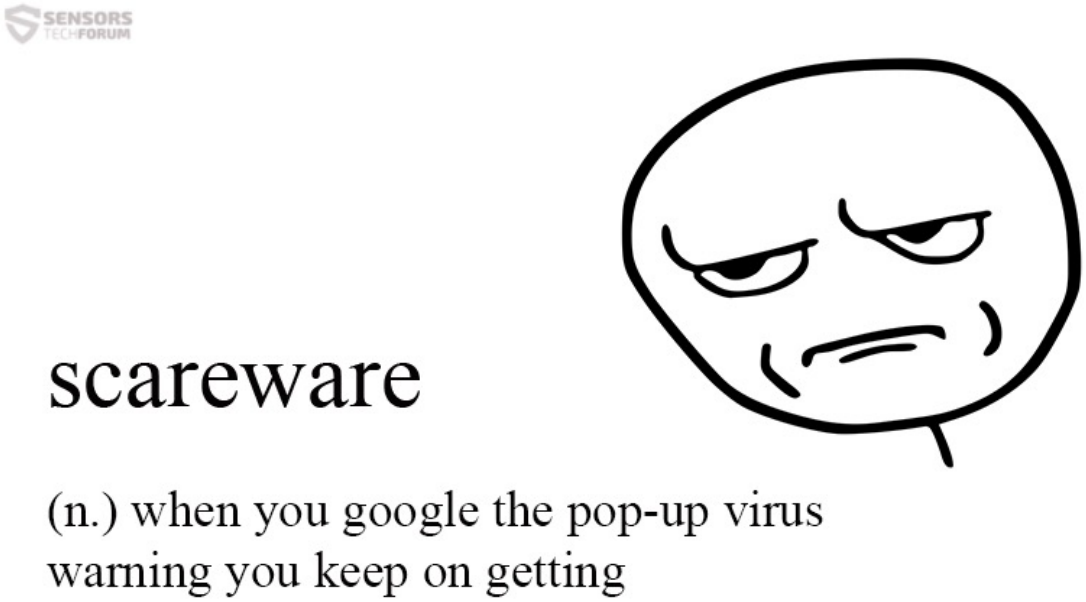
In the context of a computer virus or worm, the *payload* is the portion of the malware which performs malicious action. Thus , the term *payload* is used to describe what a virus, worm or Trojan is designed to do on a victim's computer.

Malwares: Backdoor

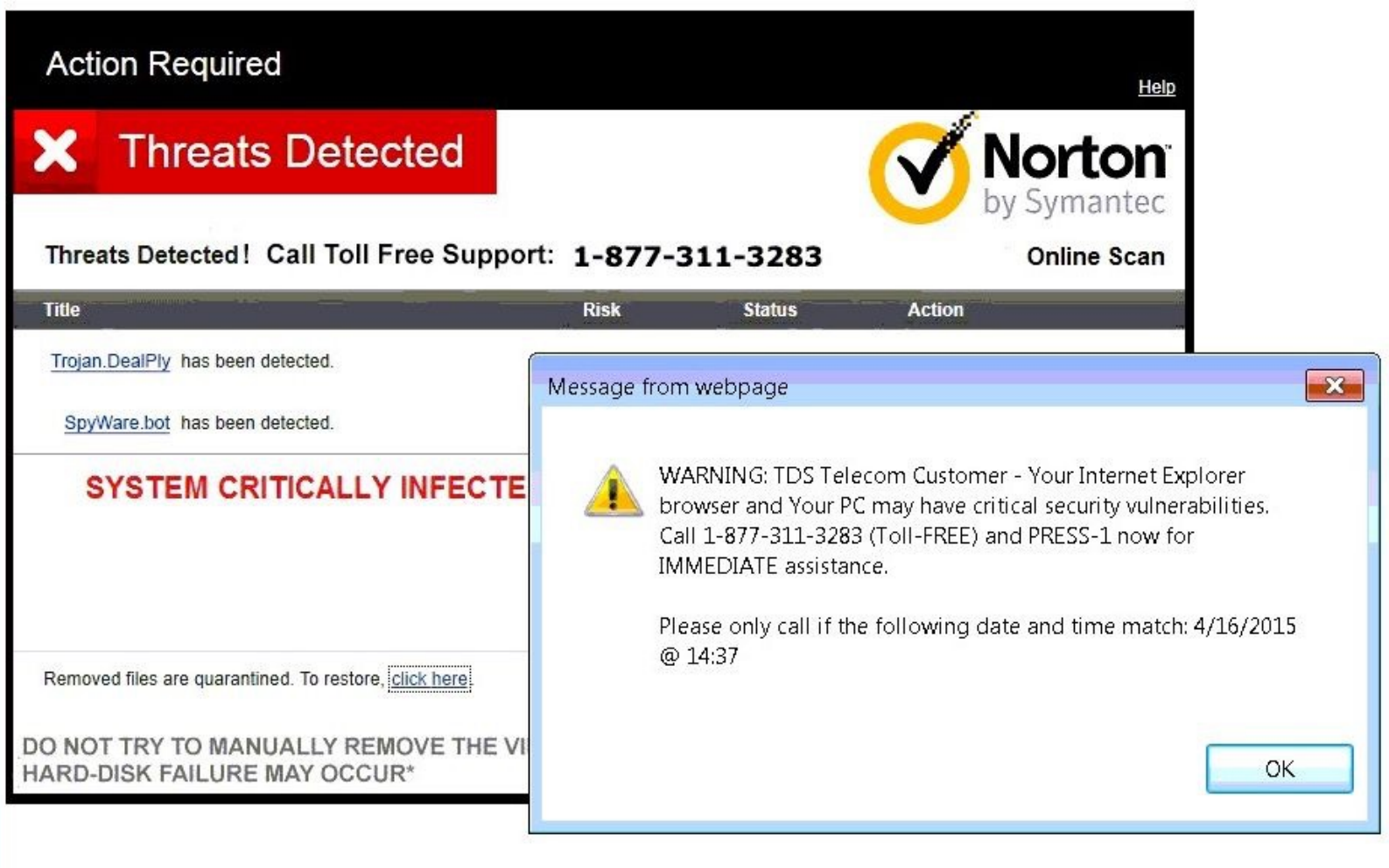
Backdoor is a malware which performs unauthorized remote access to a computer system with the intent of spying user's activities, installing illegitimate software and threats, file encryption and controlling the computing system. Backdoors log user activity and track web browsing behaviors. They have destructive capabilities causing severe damage to the user activities. They steal sensitive personal details, passwords, login names, and valuable documents. Backdoor propagates through user intervention. They infect the computers by e-mail attachments, file sharing programs, or infection of remote systems. Netcat, Finspy are examples of backdoor malware. The KeyBoy backdoor steals credentials from Internet Explorer and Mozilla Firefox and installs a keylogger module which steals credentials from Google Chrome. It also allows the attackers to acquire complete details about the compromised computers and to perform actions like browsing their directories and download or upload files.

Malwares: Scareware

Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software. Scareware is part of a class of malicious software that includes rogue security software, ransomware and other scam software that tricks users into believing their computer is infected with a virus, then suggests that they download and pay for fake antivirus software to remove it. Usually the virus is fictional and the software is non-functional or malware itself



Malwares: Scareware



Malwares: Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Malwares: Ransomware

Malwares: Adware

Adware is a software that automatically displays or downloads unwanted advertisements when the user executes another program. It keeps track of confidential information of users and takes control of browser activities when it gets installed into the user's system. Some of the sources of adware programs include free games, peer-to-peer clients, etc. The plankton adware allows its payload to work in the background for collecting information. Other examples include Fireball, Appearch, DollarRevenue, Gator, DeskAd, etc.

Malwares: Spyware

Spyware is remote monitoring software which monitors user's activities and keeps track of personal and confidential details of the user without their knowledge. The gathered sensitive information is sent back to the attacker or others to perform malicious activities. When a user downloads and installs free software, spyware may also get downloaded which performs actions like changing browser settings. Examples of spyware include Caveat, CoolWebSearch, HuntBar, Cydoor, 180SearchAssistant, etc.

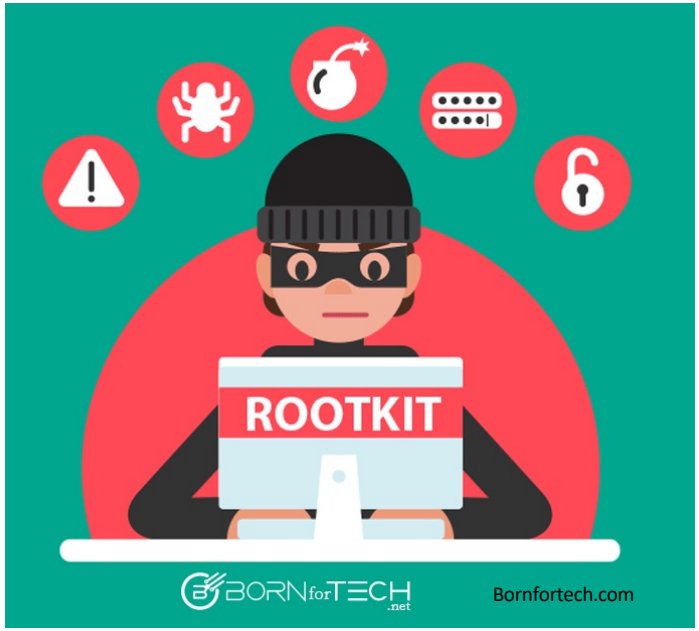
WhatsApp users targeted by spyware via in-app phone call prompting upgrade calls

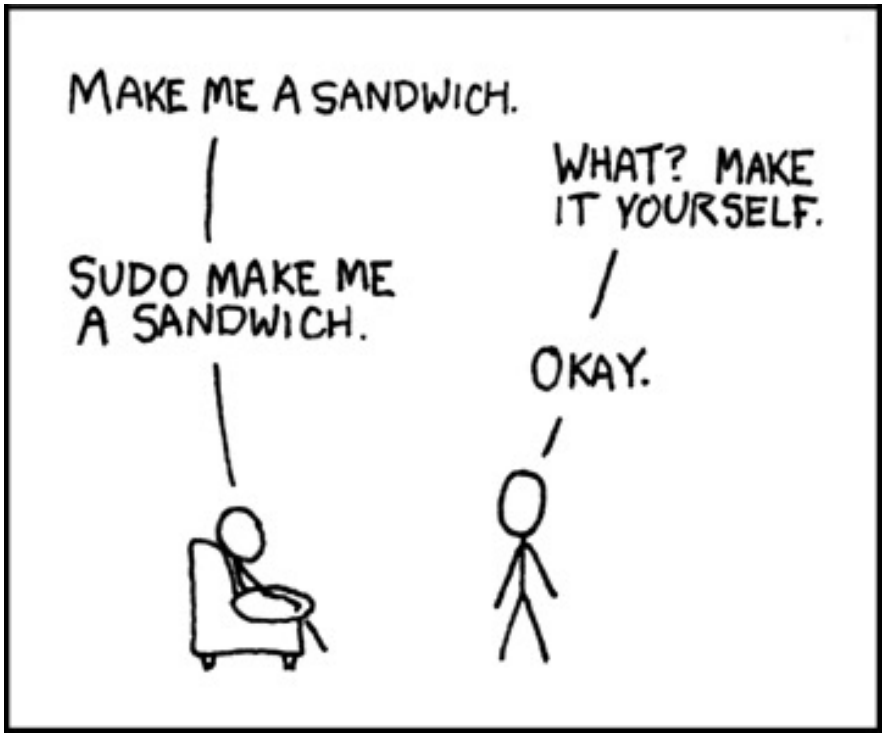
Updated 14 May 2019, 7:54am

Some WhatsApp users may have had their phones infected with sophisticated spyware through a missed in-app call alone, the company says.

Malwares: Rootkit

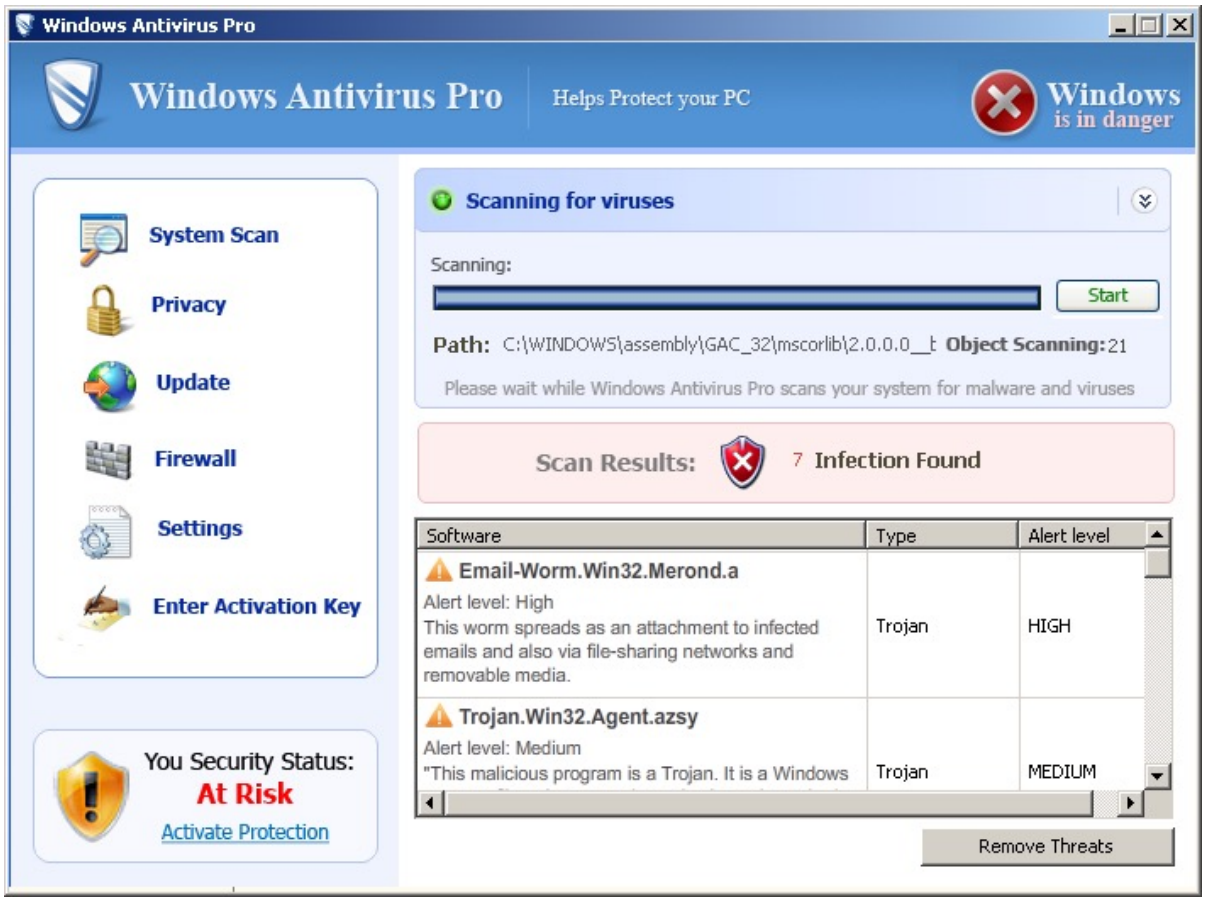
Rootkit is a type of malware which takes the privileges (root-level access) of a system administrator. Rootkits characterize undetectability by being persistent and stealthy in nature. The attacker installs a rootkit and conceals its activities from the detection systems. The two primary functions of a rootkit are (i) remote command and control, and (ii) software eavesdropping. Rootkits spread through a malicious file that appears benign, downloadable plug-in or while opening an e-mail attachment. They also spread through infected mobile apps.





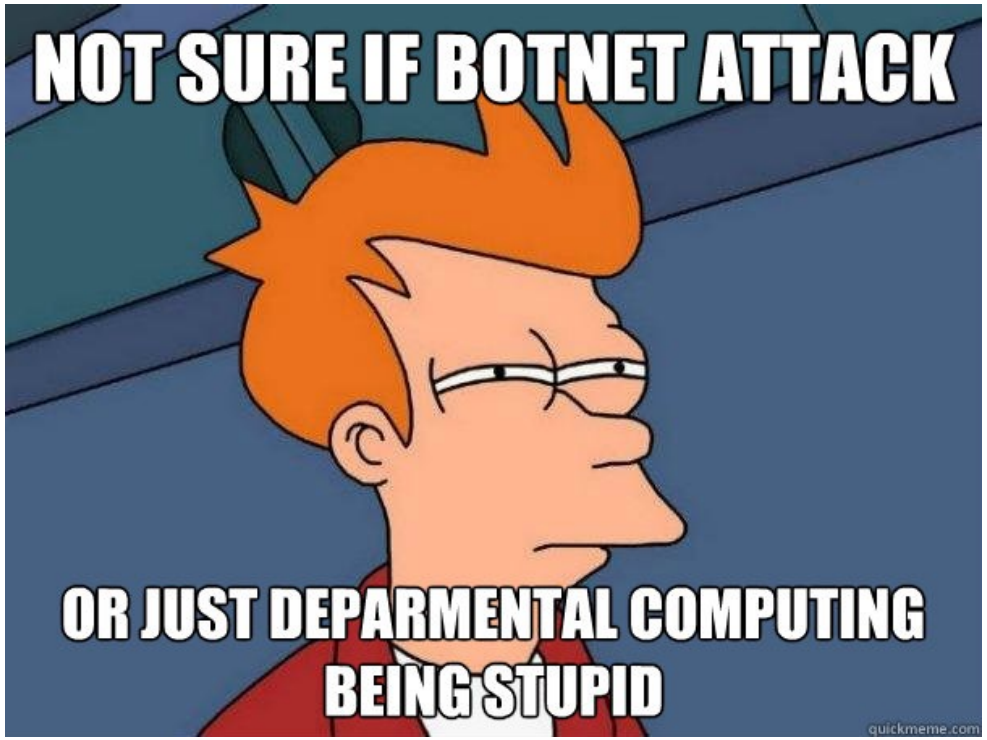
Malwares: FakeAV

Some malware imitates security product like an antivirus, and display a GUI window which scans the victims' system for malware. It reports a number of fake infections and attempts to scare victims into buying the full version of the fake software in order to clean the machine.



Malwares: Bot

Bot software conquers and infects a PC and becomes a node on the bot network. Later, it spreads and infects thousands of PCs remotely across the network. A bot network spreads viruses and worms, sends spam e-mails, allows Denial of Service attacks on websites, drive-by downloads, etc. Botnets are used extensively in DDoS attacks, credit card fraudulent operations.



Malwares: Lifecycle

1. Target finding
2. Carrier and transmission
3. Activation and infection

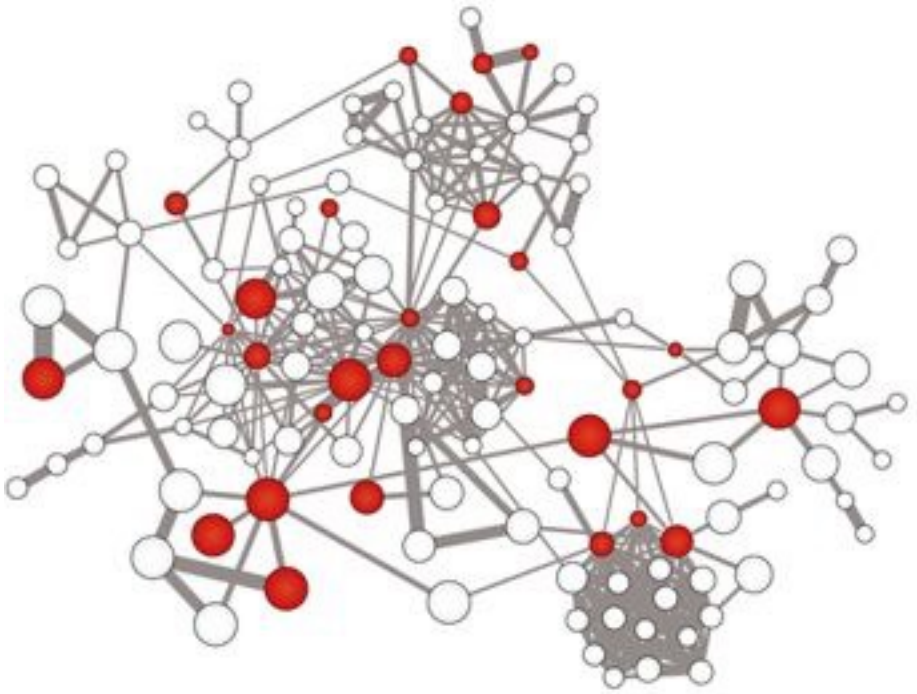
Malwares: Lifecycle: Target finding

1. Blind scanning
2. Using a hit list
3. Passive approach

Example of Mirai

Malwares: Lifecycle: Propagation

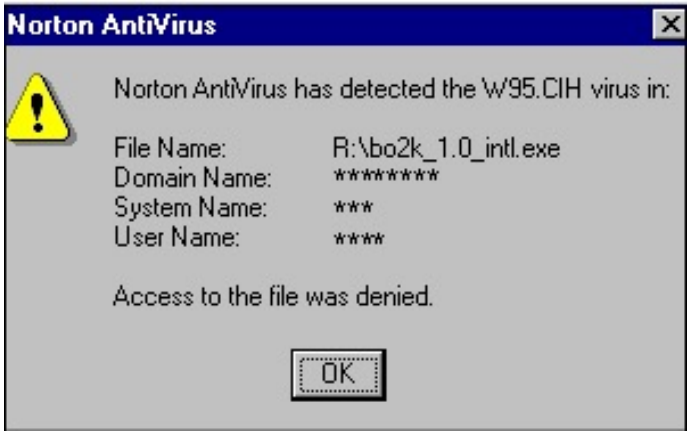
1. Propagation through wireless networks
2. Propagation through File sharing
3. Propagation through Emails
4. Propagation through downloads
5. Propagation through storage/removable media
6. Propagation through social networks
7. Propagation through virtualization techniques

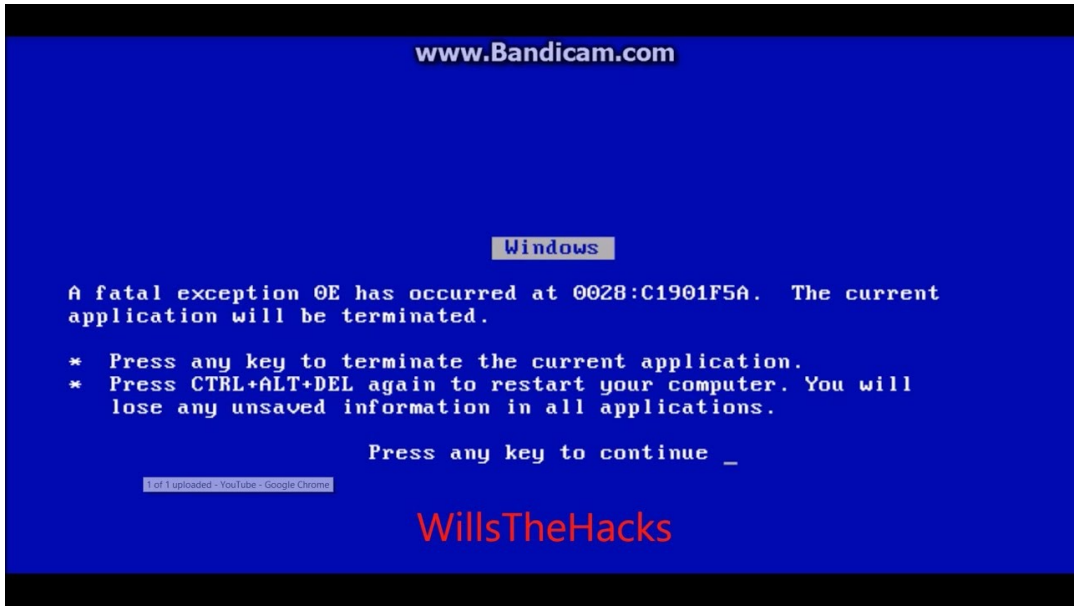


Malwares: Most Destructive Malware of All Time

1 - CIH Virus – 1998

Also known as the "Chernobyl virus", was named after the explosion of the nuclear plant in Russia because it was written to execute on the anniversary of the explosion. The virus worked by **wiping data from the hard drives of infected devices and overwriting the BIOS chip** within the computer, which rendered the device unusable. This virus caused tremendous damage because the BIOS chip was not removable on many PCs, **requiring the user to replace the entire motherboard**. The virus was created by a student at the Taipei Tatung Institute of Technology, named **Chen Ing Hau**. Although the virus caused millions of dollars in damages, Chen was never imprisoned or fined and actually got a job at a software company through his resulting infamous creation.





Malwares: Most Destructive Malware of All Time

2 – Melissa worm 1999

Named after an exotic dancer from Florida, it was created by David L. Smith in 1999. It started as **an infected Word document** that was posted up on the **alt.sex usenet group**, claiming to be a **list of passwords for pornographic sites**. This got people curious and when it was downloaded and opened, it would trigger the **macro** inside and unleash its payload.

The worm will mail itself to the top 50 people in the user's email address book and this caused an increase of email traffic, disrupting the email services of governments and corporations. It also **sometimes corrupted documents** by inserting a Simpsons reference into them.

Smith was eventually caught when they traced the Word document to him. The file was uploaded using a stolen AOL account and with their help, law enforcement was able to arrest him less than a week since the outbreak began.

He cooperated with the FBI in capturing other virus creators, famous among them the creator of the **Anna Kournikova virus**. For his cooperation, **he served only 20 months and paid a fine of $5000 of his 10 year sentence**. The virus reportedly caused **$80 million in damages**.

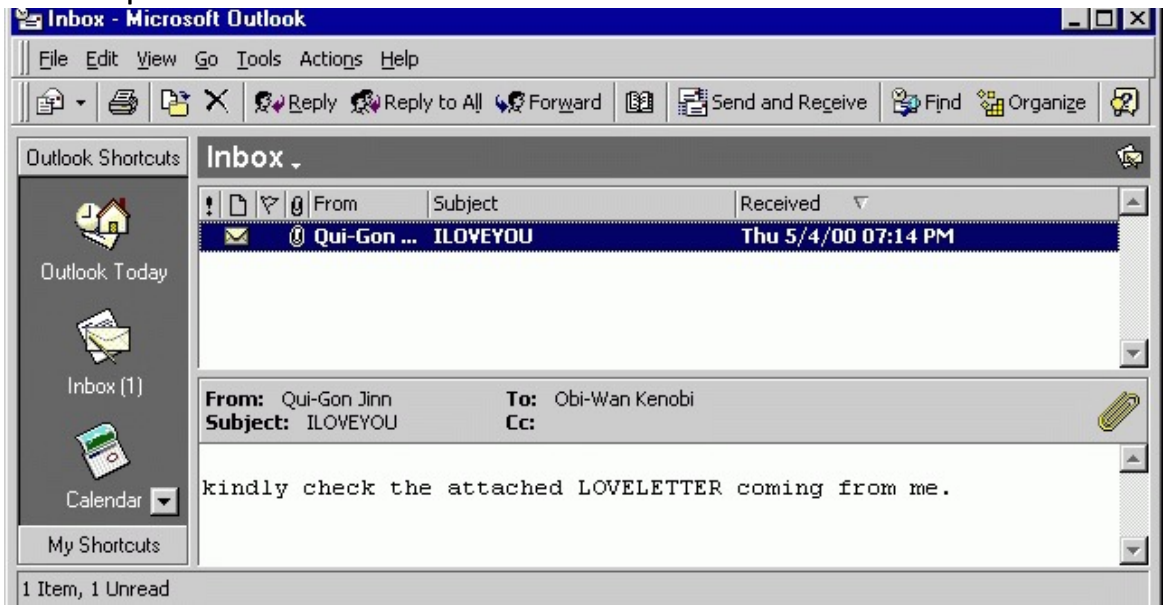
Malwares: Most Destructive Malware of All Time

3 – ILOVEYOU 2000

It managed to wreck havoc on computer systems all over the world with around **$10 billion worth of damages. 10% of the world's computers** were believed to have been infected. It was so bad that governments and large corporations took their **mailing system offline to prevent infection**.

The virus was created by two Filipino programmers, Reonel Ramones and Onel de Guzman. What it did was **use social engineering to get people to click on the attachment**; in this case, a **love confession**. The attachment was actually a script that poses as a TXT file, due to Windows at the time hiding the actual extension of the file.

Once clicked, it will send itself to everyone in the user's mailing list and **proceed to overwrite files with itself**, **making the computer unbootable**. The two programmers were never charged, as there were no laws about malware. This led to the enactment of the E-Commerce Law to address the problem.



Malwares: Most Destructive Malware of All Time

7 – Zeus 2009

Zeus is a Trojan horse made to infect Windows computers so that it will perform various criminal tasks. The most common of these tasks are usually **man-in-the-browser keylogging and form grabbing**. The majority of computers were infected either through drive-by downloads or phishing scams. First identified in 2009, it managed to compromise thousands of FTP accounts and computers from large multinational corporations and banks such as Amazon, Oracle, Bank of America, Cisco, etc. Controllers of the Zeus botnet used it to steal the login credentials of social network, email and banking accounts.

In the US alone, it was estimated that **more than 25% of computers were infected in the US**. The entire operation was sophisticated, involving people from around the world to act as money mules to smuggle and transfer cash to the ringleaders in Eastern Europe. About **$70 million** were stolen. **100 people were arrested** in connection to the operation. In late 2010, the creator of Zeus announced his retirement but many experts believe this to be false.

View report (HTTPS request, 1 253 bytes)

Bot ID:	WIN-NEDJDLJN6EQ_E532648AA7425CAC
Botnet:	-- default --
Version:	3.0.0.1
OS Version:	Seven, SP 1
OS Language:	1033
Local time:	22.12.2015 16:38:55
GMT:	+0:00
Session time:	00:12:31
Report time:	06.08.2014 12:39:34
Country:	TH
IPv4:	58.9.2.100
Comment for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Google\Chrome\Application\chrome.exe
User of process:	WIN-NEDJDLJN6EQ\user
Source:	https://s.imp.microsoft.com/zag.gif?Log=1&tntcalltype=1&tntPCID=1406910759540-752624.22_10&tntANID=00000000000000000000000000000000&t

```
https://s.imp.microsoft.com/zag.gif?Log=1&tntcalltype=1&tntPCID=1406910759540-752624.22_10&tntANID=0000000000000000000000000
Referer: https://sc.imp.live.com/content/dam/imp/surfaces/mail_signin/v3/mail/EN-US.html?id=64855&mkt=EN-US&cbcxt=mail
POST data:
 login_email: TestingOutlook@outlook.com

 login_pass: HelloOutlook
```

Yahoo: ragemystic

Malwares: Most Destructive Malware of All Time

fbi.gov

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

REMARKS

Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute

Malwares: Most Destructive Malware of All Time

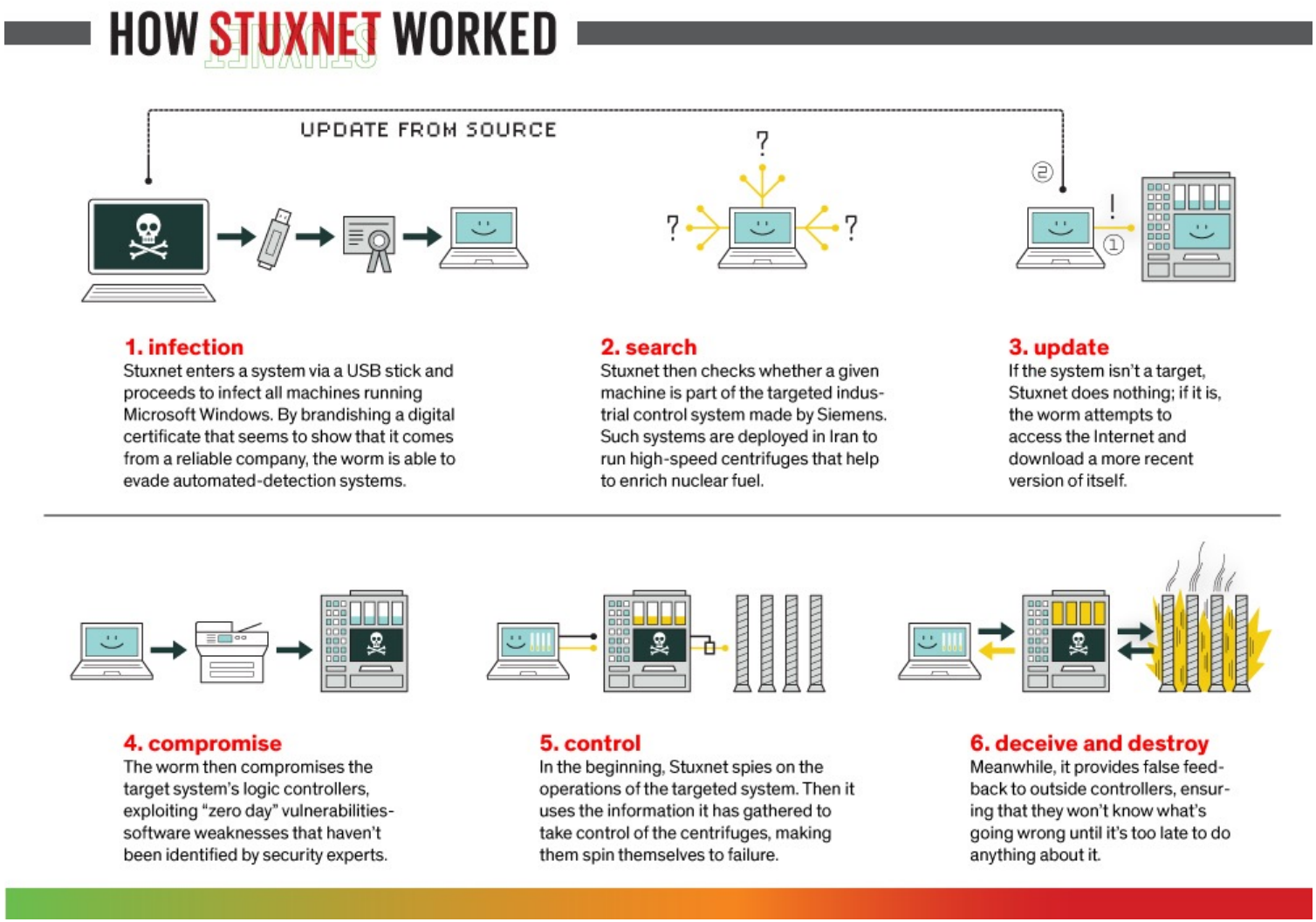
8 – Stuxnet 2010

It have been created by the Israeli Defence Force together with the American Government, Stuxnet is an example of a **worm created for the purpose of cyberwarfare**, as it was intended to disrupt the nuclear efforts of the Iranians. It was estimated that Stuxnet managed to ruin one fifth of Iran's nuclear centrifuges and that nearly 60% of infections were concentrated in **Iran**.

The computer worm was **designed to attack industrial Programmable Logic Controllers (PLC),** which allows for automation of processes in machinery. It specifically aimed at those created by **Siemens** and was spread through **infected USB drives**. It altered the speed of the machinery, causing it to tear apart. If the infected computer didn't contain Siemens software, it would lay dormant and infect others in a limited fashion as to not give itself away. Siemens eventually found a way to remove the malware from their software.

Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm **destroyed 984 uranium enriching centrifuges**. By current estimations this constituted a **30% decrease in enrichment efficiency** [http://large.stanford.edu/courses/2015/ph241/holloway1/].

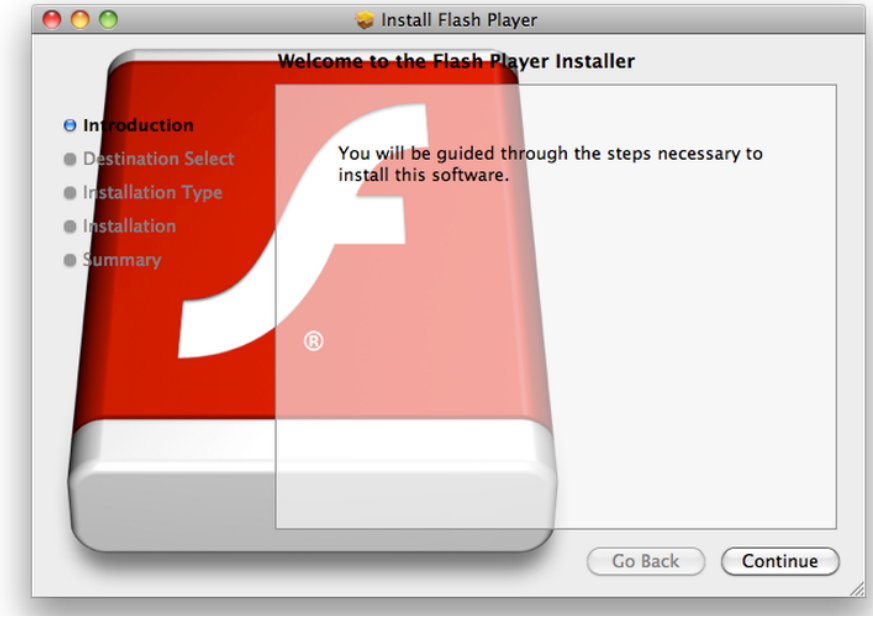
Malwares: Most Destructive Malware of All Time



Malwares: Most Destructive Malware of All Time

9 – Flashback 2011

Though not as damaging as the rest of the malware on this list, this is **one of the few Mac malware to have gain notoriety** as it showed that Macs are not immune. The Trojan was first discovered in 2011 by antivirus company Intego as a **fake Flash install**.
In its newer incarnation, a user simply needs to have **Java enabled** (which is likely the majority of us). It propagates itself by **using compromised websites containing JavaScript code that will download the payload**. Once installed, the Mac becomes part of a botnet of other infected Macs.
More than **600,000 Macs** were infected, including 274 Macs in the **Cupertino area, the headquarters of Apple**.
Oracle published a fix for the exploit with Apple releasing an update to remove Flashback from people's Mac. It is still out in the wild, with an estimate of 22,000 Macs still infected as of 2014.



Malwares: Most Destructive Malware of All Time

Malwares: Most Destructive Malware of All Time

10 – Cryptolocker 2013

CryptoLocker is **a form of Trojan horse ransomware** targeted computers running **Windows**. It uses several methods to spread itself, such as email. For example, it enters a user's system through an email, supposedly sent by a logistics company. and once a computer is infected, it will proceed to encrypt certain files on the hard drive and any mounted storage connected to it with **RSA public key cryptography**.

While it is easy enough to remove the malware from the computer, the files will still remain encrypted. **The only way to unlock the files is to pay a ransom by a deadline**. If the deadline is not met, the **ransom will increase significantly** or the decryption keys deleted. The ransom usually amount to **$400** in prepaid cash or bitcoin.

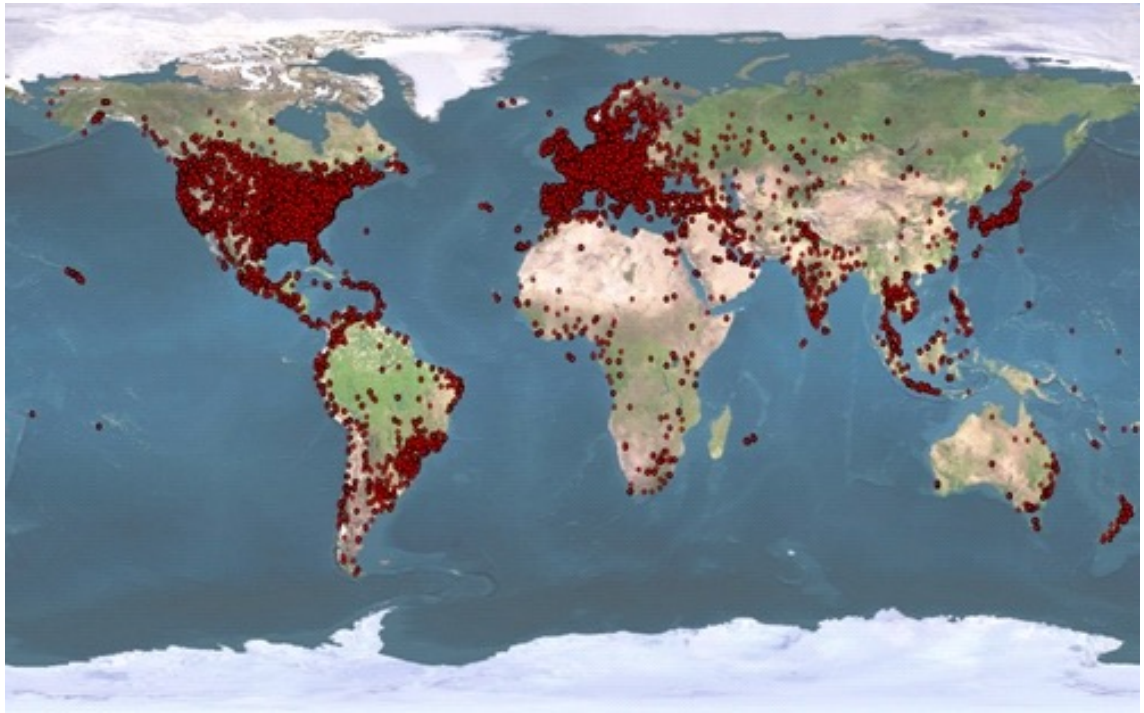
The ransom operation was eventually stopped when **law enforcement agencies and security companies managed to take control part of the botnet operating CryptoLocker and Zeus**.

Evgeniy Bogachev, the ring leader, was charged and the encryption keys were released to the affected computers. From data collected from the raid, the number of **infections is estimated to be 500,000**, with the number of those who paid the ransom to be at 1.3%, amounting to **$3 million**.

Malwares: Most Destructive Malware of All Time

11 – ZeroAccess Botnet 2011 – 2013

Known as one of the largest botnets in history. The latest version of the malware is highly disruptive and has **infected more than 9 million machines** over its lifetime. The current version affected **over 1.9 million computers**, using them to earn revenue through **bitcoin mining (cryptojacking)** and **click fraud**. It can earn a staggering amount of **$100,000 in a single day**. It is also used to send **SPAM** emails or launch HTML attacks. The SPAM emails sent by the bots **often contain malware** that is then used to infect more computers.



nakedsecurity.sophos.com

Malwares: Most Destructive Malware of All Time

12 – SuperFish 2014

Superfish adware made its claim to fame through a class action lawsuit filed against **Lenovo**, the largest maker of PCs in the world. Superfish spyware came **pre-installed on Lenovo machines without Lenovo customers being told of its existence**. **Superfish installed its own root certificate authority**. the certificate authority allows a **man-in-the-middle** attack to introduce ads even on encrypted pages. **The certificate authority had the same private key across laptops**; this allows third-party eavesdroppers to intercept or modify HTTPS secure communications without triggering browser warnings by either extracting the private key or using a self-signed certificate. More precisely, the root certificate and **an encrypted version of the root's private key** are included on all of the affected systems. It didn't take long for **Rob Graham**, CEO of security firm Errata Security. The private key were **widely available on Internet**, **attackers can generate SSL certificates which are trusted by these Lenovo systems for any site** on the internet.

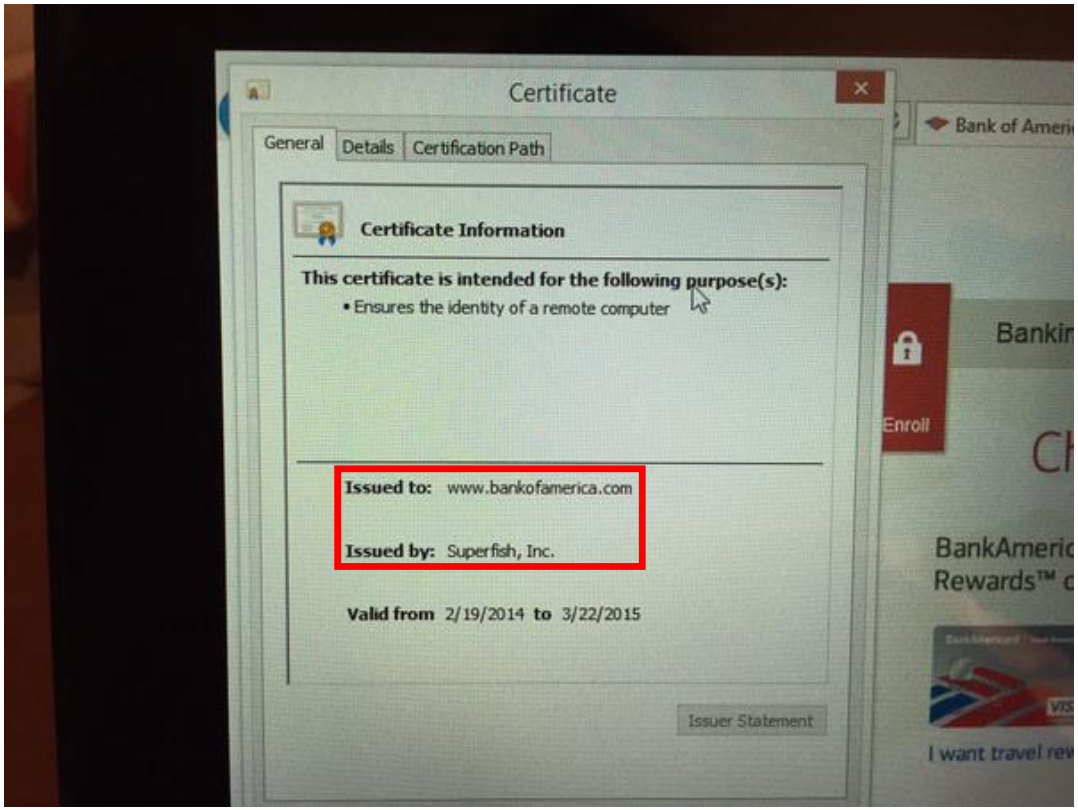
As of 2014, Superfish products had over **80 million users**. In May 2015, following the Lenovo security incident and to distance itself from the fallout, the team behind Superfish changed name and moved its activities to JustVisual.com

How it was supposed to work

Superfish uses the program "Visual Discovery" to process images in browser content and then displays ads for similar goods and services. This sounds like any other adware application, but in order to maintain SSL sessions and not alert users with security warnings, Superfish is serving up these images over https. They were able to do this by creating SSL certificates on the fly and using them in a local SSL proxy to deliver content from the Visual Discovery server over the same apparent domain.

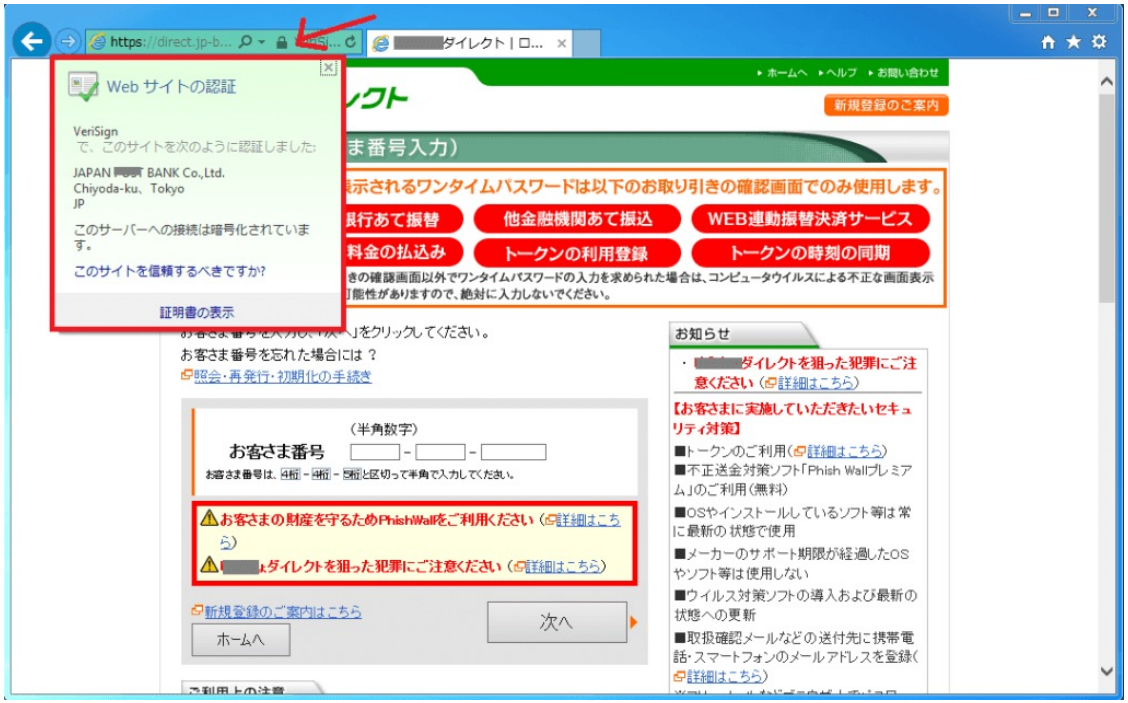
Malwares: Most Destructive Malware of All Time

SuperFish



Malwares: Most Destructive Malware of All Time

SuperFish



© Kaspersky

Malwares: Most Destructive Malware of All Time

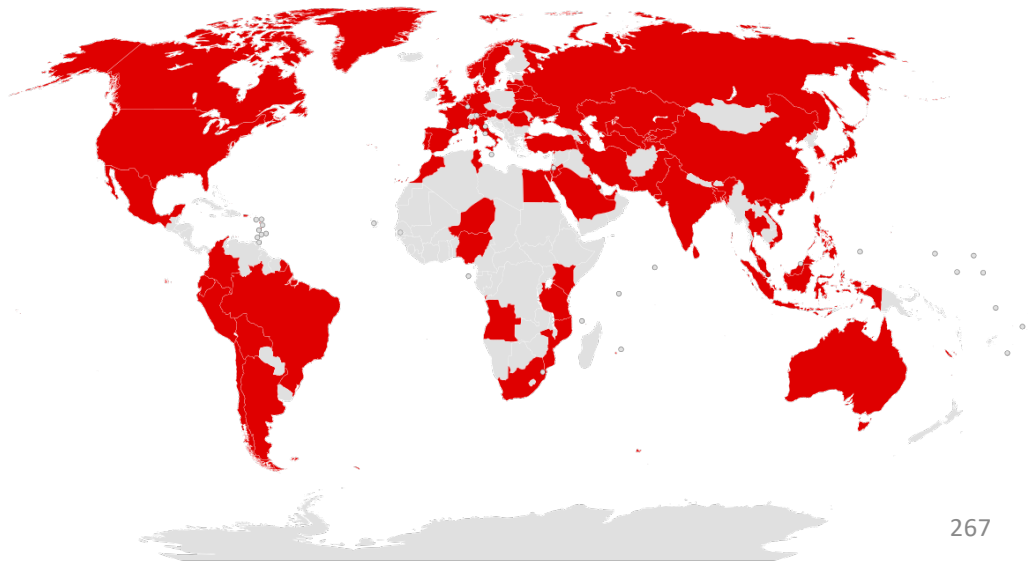
Malwares: Most Destructive Malware of All Time

13 – WannaCry 2017

Also known as WannaCrypt or WanaCrypt0r 2.0 is a **ransomware** cryptoworm. In May 12th 2017, it was used in a massive global cyberattack affecting more than **300,000 Microsoft Windows operating system computers in more than 150 countries**, mainly in India, the United States, and Russia, using the outdated Windows XP system and more generally Pre-Windows 10 versions that did not perform security updates (especially March 14, 2017) (security bulletin **MS17-010**). It propagated through **EternalBlue**, an exploit discovered by the United States **National Security Agency (NSA)** for older Windows systems. EternalBlue was stolen and leaked by a group called The **Shadow Brokers** a few months prior to the attack.

This cyber attack is considered the biggest ransom piracy in the history of the Internet. Among the most important organizations affected by this attack are **Vodafone, FedEx, Renault, Telefónica, the National Health Service, the Liège University Hospital Center, the Russian Interior Ministry, Deutsche Bahn and Honda**.

The ransom request is in bitcoins, of a relatively low value **between 300 and 600 dollars**. It is initially 300 and then increases to 600 **after three days** if the user still has not paid, **the data is then deleted after seven days**



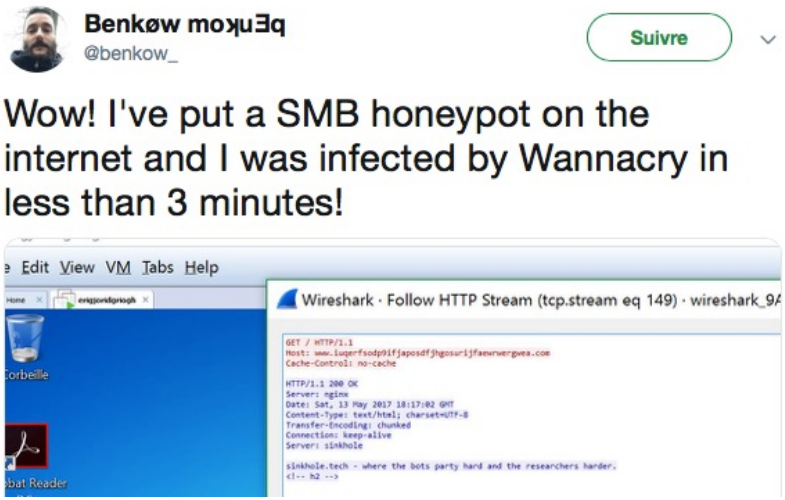
Malwares: Most Destructive Malware of All Time

WannaCry: propagation

Like most computer malwares, it is transmitted via the local network and the Internet.
Hypothesis 1: it was transmitted via contaminated attachments sent by a large number of **e-mails via a botnet** ➔ no trace of these emails has been found: "Everyone is looking for this famous initial e-mail"

Hypothesis 2: The **honeypots** connected to the Internet were very quickly **contaminated**.

This ransomware is characterized by the speed of its attack, affecting hundreds of thousands of machines around the world in a weekend. **The attack frequency was at least one attempt per second and 226,800 IP addresses assigned to its strongest point**. Similarly, it does not seem to have been the subject of **test phases** but rather of a preliminary investigation period. Thus, neither the track of a **criminal organization**, nor that of a state attack (or **supported by a State**) is discarded. Europol says no country is particularly targeted



Malwares: Most Destructive Malware of All Time

WannaCry: Authors

IT security researchers have reported about a probable connection with **North Korea.** **Neel Nehta (Google)**, has posted portions of **source code that demonstrate some similarities** between this new virus and another series of hacks attributed to this country. The suspected North Korean hackers belong to the **Lazarus Group**. Then **Kaspersky** Lab and **Symantec** have both said the code has some **similarities** with that previously used by the **Lazarus Group.**

The computer that created the ransomware language files had **Hangul** language fonts installed, as evidenced by the presence of the "\fcharset129" Rich Text Format tag. Metadata in the language files also indicated that the computers that created the ransomware were set to **UTC+09:00, used in Korea**.
In December 2017, the **United States, United Kingdom and Australia** formally asserted that **North Korea** was behind the attack

Flashpoint experts analyzed WannaCry's ransom messages in **28 different languages**. Their results show that hackers are fluent in **Chinese**, whose message is grammatically better constructed and contains more information. **The other translations were obtained from the English message (containing a serious grammatical error) and from Google Translate**. The pieces of the program pointing to the Lazarus Group could have been implanted in the malware **only to cover the tracks of the pirates**.

Malwares: Most Destructive Malware of All Time

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company – Chosun Expo Joint Venture, also known as Korea Expo Joint Venture – was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Zero day attacks

Google, Xiaomi, and Huawei devices affected by zero-day flaw that unlocks root access

by IVAN MEHTA — 2 days ago in SECURITY