openHPI Course: Cyberthreats by Malware

Virus, Worm, Trojan

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Virus, Worm, and Trojan – so Many Malware …

By Larry Monarrez, Jim Parker
December 11, 2020 12:35 pm Published December 11, 2020 11:44 am

SISD's internal computer network taken down due to virus

'Graboid' Cryptojacking Worm Spreads Through Containers

Using Docker Containers to Spread Worm Is a New, Untested Technique, Researchers Say

Jeffrey Burt (@burttech) • October 16, 2019

Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy

March 30, 2020 | By Amir Gandler co-authored by Limor Kessem | 7 min read

December 3, 2020

Trickbot trojan takes aim at vulnerabilities in booting process

Derek B. Johnson

Follow @@DerekDoesTech

Glupteba Trojan Makes a Comeback Taking Aim at Large Enterprises [Whitepaper]

by Filip Truta on December 16, 2019

Gitpaste-12 worm botnet returns with 30+ vulnerability exploits

By Ax Sharma

December 19, 2020 01:01 PM 0

Malware: Virus

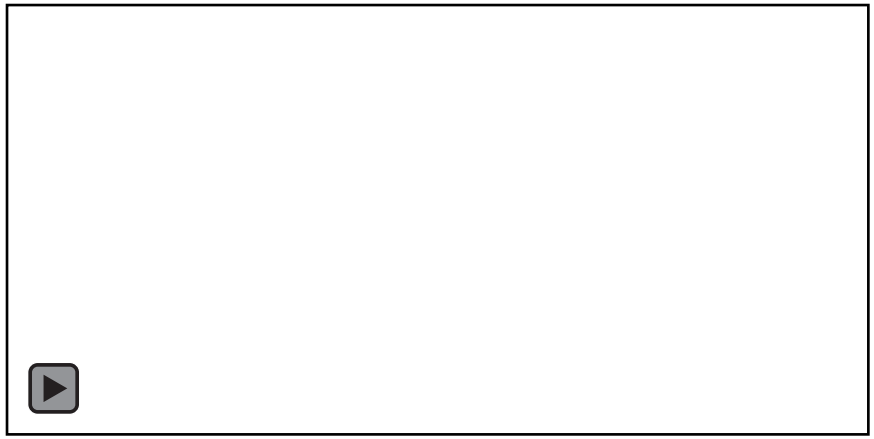
Virus is a **malware** that attaches itself to a program or a file ("**host**") and spread further to other programs/files

- If the infected host is **opened** or **run** then the target system gets infected
- Severity ranges from causing annoying effects up to damaging data, software, or even hardware
- Often no clear definition
  - colloquial term for malware
  - generic term for all malware in a host programs

Malware: Worm

Worm is a malware that can spread its copies over the network or Internet **on its own**

- Start infection by exploiting vulnerabilities on target's system or tricks the target to execute the malware
- Functions **independently** → does not need a host or a human to replicate and distribute itself
- Often worms **spread faster** than viruses, e.g., Code-Red 2001



Malware: Worms
ILOVEYOU (1/2)

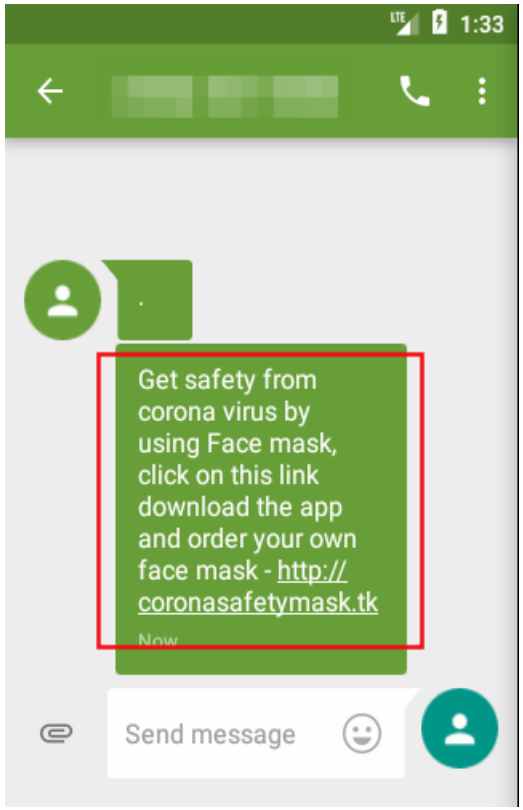
ILOVEYOU – **Worm** that uses **social engineering techniques** to infect users via an **email**

- Subject of the email: "ILOVEYOU" (I love you)
- Attachment of an alleged love letter ("LOVE-LETTER-FOR-YOU.txt.vbs")
  - contains a visual Basic Script (.vbs) that executes malicious program code when the attachment is opened
  - file extensions were not displayed → target will not suspect the attachment to be malicious
- **Email address book** of the victim of the target is used to **distribute** the worm via email

Malware: Worms
ILOVEYOU (2/2)

Safety Mask – **Worm** with a similar concept as **ILOVEYOU**

- Target will receive an SMS to download and install the application (worm) from the attached link
- **Phone address book** is used to **distribute** the worm via SMS



Source: Shivang Desai, "New Android App Offers Coronavirus Safety Mask But Delivers SMS Trojan Zscaler, 2020

Malware: Trojan (1/2)

Trojan is a malware that disguise itself as a **genuine** and **useful application** and tricks the target to install it

- Contains hidden malicious functions unknown to the target, e.g., **download** of other malwares
- Malicious function is executed in parallel to the expected functionality
- Does not **replicate** itself nor **infect** other files

Malware: Trojan (2/2)

Trojans have different objectives like installing a …

- **Backdoor**
  - Opens a backdoor in the victim‘s system to give the attacker remote control access to the his/her system
- **Spyware**
  - Monitors and sends information of victim’s system by capturing keyboard typings, gaining access to microphone or webcam, etc.
- **Botnet**
  - Adds the victim‘s system to a network of hijacked and remote controlled systems to launch cyberattacks
- **Downloader**
  - Installs other malwares to the infected system, such as ransomware or worms

Malware: Trojan
BlackNET Trojan

BlackNET RAT – Trojan that utilizes COVID-19 pandemic

- Utilizes a phishing website that encourage users to download software to "protect" computer against COVID-19 virus, which is not true
- After the "software" has been installed, the infected computer becomes a bot that can be controlled by the hacker
- BlackNET RAT is capable of launching distributed DoS attack, taking screenshots, stealing passwords, cookies, and Bitcoin wallets

Source: https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/