Lecture 22: Malware

Stephen Huang

Content

1. Malware
2. Malware Payload Functionality
3. Malware Detection

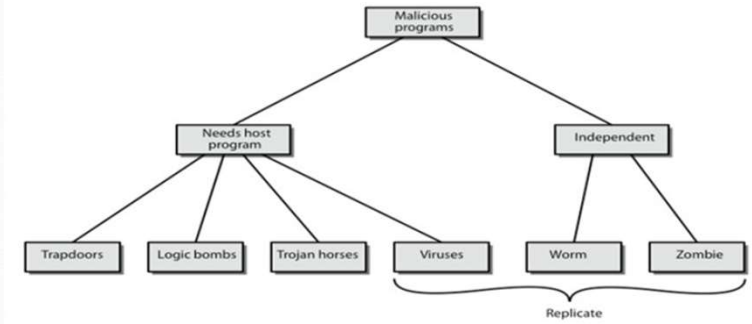
1. Malware

- Malware (short for malicious software) is software that disrupts computer operations, gathers sensitive information, or gains access to private systems.
- An umbrella term for a wide variety of software
  - Examples: virus, worm, logic bomb, trojan horse, backdoor (trapdoor), spyware, adware, rootkit, zombie, …
  - These categories overlap, and some malware fits into multiple categories.

Classification based on propagation

- Classification based on propagation
  - Non-replicating
    - does not create copies of itself
    - performs some malicious function
  - Replicating
    - creates copies of itself
    - either parasitic or independent
- A Parasitic Virus (file virus) spreads by attaching itself to another program. The computer's operating system gives the virus code the same rights as the program.

Tree



Top 5 Types

- **Crypto-mining** malware uses the infected computer's CPU resources for crypto-mining.
- **Mobile** malware are droppers that deliver other types of mobile malware.
- A **botnet** is a collection of infected computers that an attacker controls and uses to perform Distributed Denial of Service (DDoS).
- **Infostealers** or "spyware" are malware designed to spy on a computer's user.
- A **trojan** (horse) virus is malware that downloads onto a computer disguised as a legitimate program.

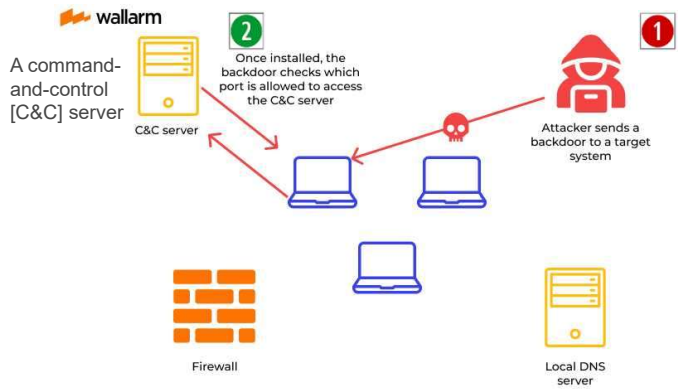
Others

- **Ransomware** is designed to infect and encrypt files on a computer.
- Computer **viruses** are malware that infects other programs on a computer.
- **Worms** are designed to spread themselves to infected additional systems.
- **Rootkits** are designed to be stealthy, snoop on a computer user, and exfiltrate data to their operators.
- **Fileless** is designed to evade detection by replacing custom malicious code with functionality built into the target system.
- **Adware** is designed to serve unwanted ads to a computer user.

Backdoors (Trapdoors)

- Secret entry point into a system or program that circumvents the usual security access procedures.
- Maintenance hook: legitimate use for debugging and testing.
- Asymmetric backdoor: can be used only by the developer, even if the implementation becomes public.
- May be introduced by a malicious compiler.
- Backdoor attacks work in two ways. Hackers might either discover and exploit a backdoor that already exists within a system, or they might install a backdoor into the system themselves.

Backdoors



Logic Bombs

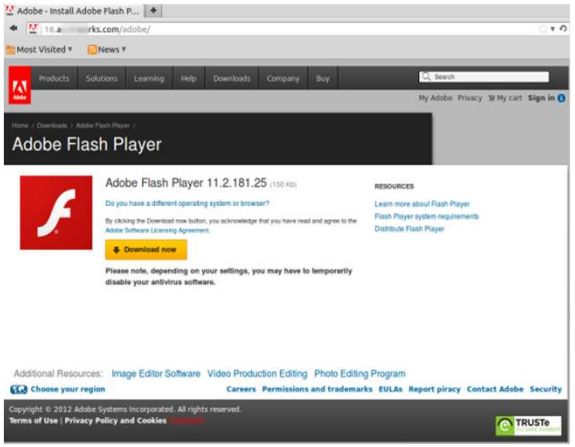
- Code embedded in a legitimate program, which "explodes" when certain conditions are met (e.g., time, presence of some files, hostnames).
- May alter or delete data, system functionality, etc.
- Example: in 1996, an employee of OMEGA Engineering set a logic bomb when he was fired, deleting software that ran manufacturing operations, causing losses exceeding $10 million.

Trojan Horse

- Trojan horse: an apparently benign application with hidden malicious functionality.
- Runs with and abuses the privileges of the victim user.
- May implement various kinds of malicious functionality.
- Typically spread using social-engineering techniques.
  - providing free (but illegal) copies of commercial software
  - sending as an e-mail attachment
  - drive-by download: authorized by the user without understanding the consequences

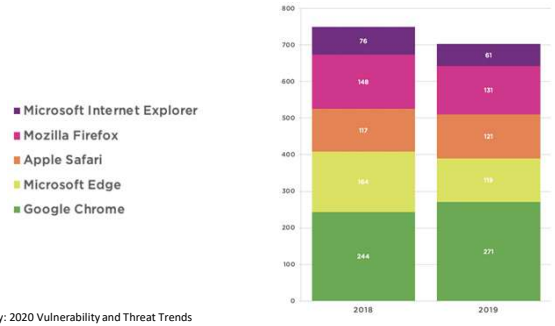
https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

Trojan Drive-by Download Example



Drive-by Download Based on Vulnerability

- Malicious websites may exploit vulnerabilities to download and install malware without user interaction.
- Vulnerability can be in the web browser or some plugin.

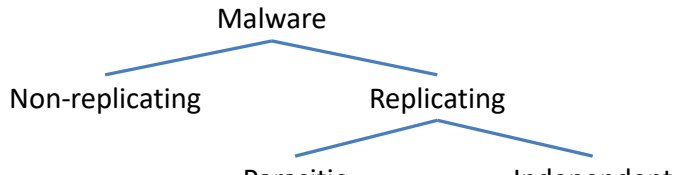


Source: Skybox Security: 2020 Vulnerability and Threat Trends

Drive-by Download Based on Vulnerability

- Malicious websites may exploit vulnerabilities to download and install malware without user interaction
- Vulnerability can be in the web browser or some plugin
- plugin examples: PDF reader, Java, Adobe Flash, …
- Example: several vulnerabilities have been discovered in Adobe Flash, some of these were actively exploited by attackers
- Many web browsers (e.g., Google Chrome) have disabled plugins and replacing functionality with HTML5 support

Replicating Malware



- fragments of code that cannot exist independently of some actual program
- executed with the infected program

- self-contained programs that the operating system can run

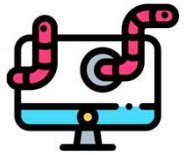
both may carry a payload

Virus

- Virus: parasitic self-replicating malware
  - resident virus: remains in memory (e.g., as part of the OS), may overwrite interrupt handlers and other functions
- Infection targets
  - boot sector: targets the boot sector or Master Boot Record of the infected host's hard drive or removable media
  - executable files: targets binary executable files
  - documents (macro viruses): targets word processor and spreadsheet documents that support embedding macro programs (e.g., Microsoft Office)
- Typical phases of operation
  - **dormant**: the virus is waiting for an external event
  - **propagation**: the virus places copies of itself into other executables and files
  - **triggering**: the virus is activated by some external event
  - **execution**: The virus executes the payload, which performs malicious actions

Worm

- Worm: runs independently, without a host program or file
- Propagates a copy of itself to other systems
  - typically by exploiting vulnerabilities, such as common software vulnerabilities or weak passwords
  - over the Internet, over a local computer network, or through removable media (e.g., USB flash drives)
  - e-mail worm: propagating as e-mail attachments (e.g., ILOVEYOU worm)
- Payload
  - either carried by the worm or downloaded from a server
  - may perform other tasks (e.g., spyware, ransomware, botnet)



Example Worms

- Morris Worm (1988)
  - one of the first worms propagating through the Internet
  - exploited software vulnerabilities in Unix finger and sendmail, as well as weak passwords
  - unintentional error in the code enabled infecting a computer multiple times, each time launching a new process → denial-of-service
  - reportedly infected 10% of all computers on the Internet, causing $100,000 - $10,000,000 damage
- Conficker (2008)
  - propagated through the Internet using software vulnerabilities in Windows, through local networks using weak passwords, or through removable drives
  - infected 9 - 15 million computers by 2009, causing billions of dollars in damage

2. Malware Payload Functionality

- Spyware
  - collect sensitive information about the user
  - may record keystrokes, mouse clicks, browsing activity, etc.
  - attacker can use it to collect personal information (*e.g.*, social security number, financial information, such as credit card numbers)
- Adware
  - display unwanted advertisements to the user (*e.g.*, pop-up windows, injecting into web pages)
  - legitimate use: advertisement-supported non-malicious software
- Cryptojacking
  - use the infected computer's resources to "mine" proof-of-work cryptocurrencies (*e.g.*, Bitcoin) for the attacker

Ransomware

- Ransomware: holds a computer system or data hostage
  - disables access to the computer system or specific files on it (e.g., screen locking, browser locking)
  - may also threaten to publish the victim's files online
  - "scareware": threaten or deceive users (e.g., fake antivirus)
- Payment
  - computer system or data is released upon payment
  - payment through Bitcoin, premium-rate text messages, wire transfers, etc.

Browser "Locking"

```
<iframe class="frame" width="0" height="0" src="us/close.html">
  #document
    <html>
      <head>…</head>
      <body style="margin:0px;padding:0px;width:100%;height:100%;">
        <script type="text/javascript">
            window.onbeforeunload = function(env){
            var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL
                alert(str);
                return str;
            }

        </script>
      </body>
    </html>
</iframe>
<iframe class="frame" width="0" height="0" src="us/close.html">
  #document
    <html>
      <head>…</head>
      <body style="margin:0px;padding:0px;width:100%;height:100%;">
        <script type="text/javascript">
            window.onbeforeunload = function(env){
            var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL
                alert(str);
                return str;
            }

        </script>
      </body>
    </html>
</iframe>
```

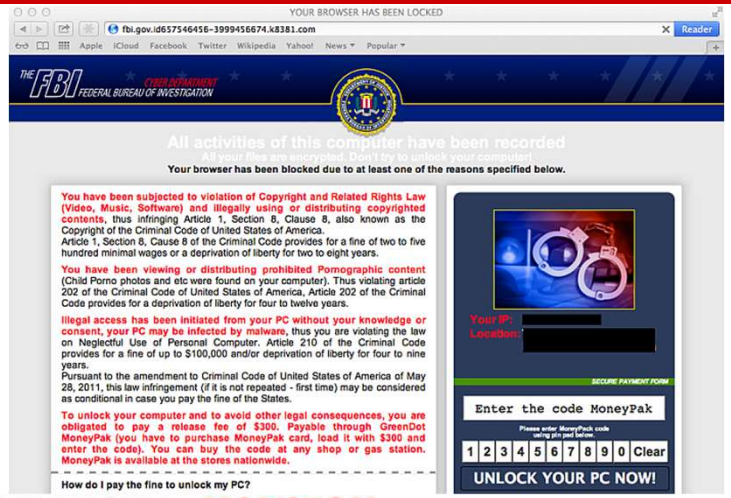
- The `onbeforeunload` handler is executed for each `iframe` when a user tries to close the webpage

→ each displays a pop-up message

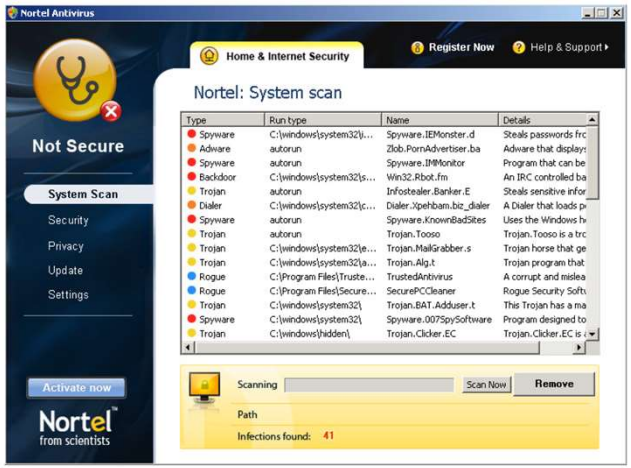
- A deceiving website may load hundreds of `iframe`

→ The user will think that the webpage cannot be closed

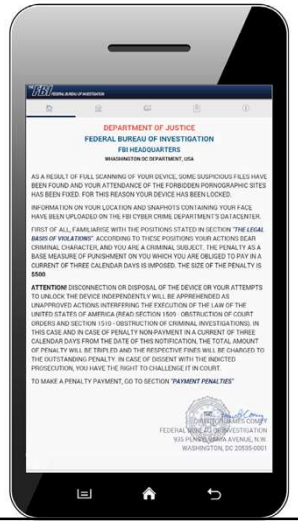
Scareware Example



Scareware Example



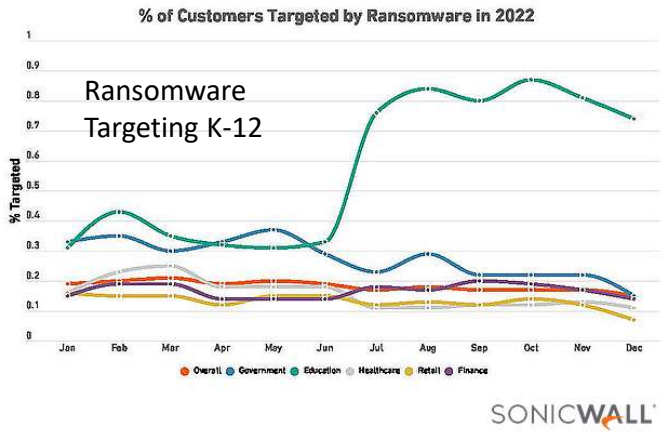
Scareware Example



Ransomware

- Ransomware: holds a computer system or data hostage
  - disable access to the computer system or certain files on it (e.g., screen locking, browser locking)
  - may also threaten to publish the victim's files online
  - "scareware": threaten or deceive users (e.g., fake antivirus)
- Payment
  - computer system or data is released upon payment
  - payment through Bitcoin, premium-rate text messages, wire transfers, etc.
- Crypto-ransomware
  1. ransomware encrypts files using a random symmetric key
  2. symmetric key is encrypted using the attacker's public key and then deleted
  3. The attacker decrypts the symmetric key in exchange for payment

Ransomware Trends

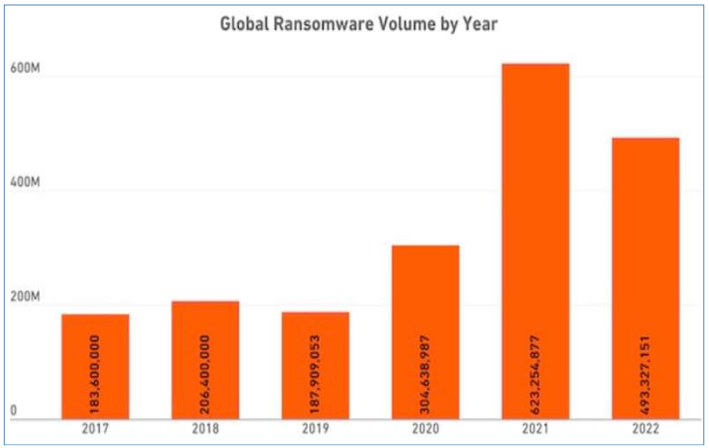


Impact of Ransomware

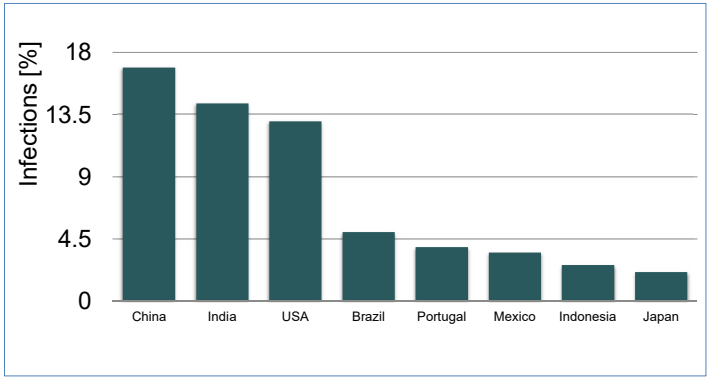
- Example: in October 2019, three hospitals in Alabama fell victim to a ransomware attack, forcing them to divert non-critical patients to other hospitals and to eventually pay the ransom
- On That Dusseldorf Hospital Ransomware Attack and the Resultant Death

https://www.schneier.com/blog/archives/2020/11/on-that-dusseldorf-hospital-ransomware-attack-and-the-resultant-death.html

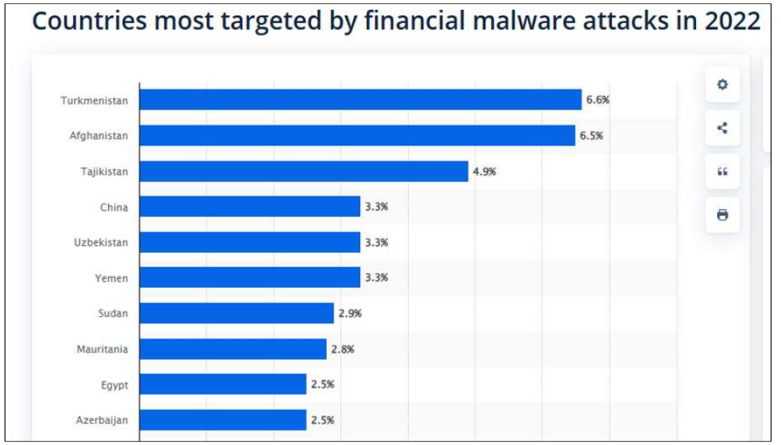
Ransomware Attacks



Countries Impacted



Financial Malware Attacks

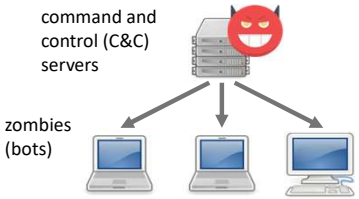


Botnets

- Botnet: a collection of computers controlled through the Internet
  - legal application: distributed computing
  - illegal application: taking advantage of compromised "zombie" computers
- Zombie computers
  - laptop and desktop computers
  - IoT devices (e.g., remote cameras, home routers, DVRs)
- Typically used by attackers to
  - send spam e-mail or perform click fraud
  - collect personal information ≈ spyware
  - attack other systems (e.g., denial-of-service attack by flooding with requests)

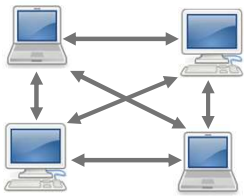
Architectures

Client-Server



- publish digitally signed commands on websites, IRC channels (Internet Relay Chat), or other standard protocols
- C&C servers are typically redundant and often implemented on compromised computers

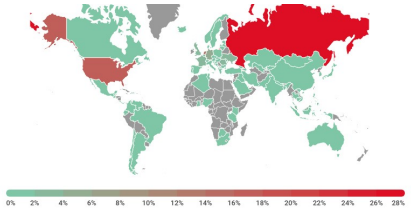
Peer-to-Peer



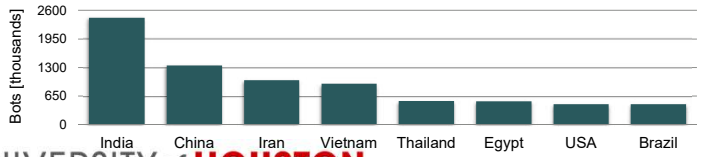
- commands distributed over a peer-to-peer (P2P) network
- no single (or few) point of failure → more resilient to shutdown or hijack

Botnet Statistics

- Location of C&C servers (*source:* Kaspersky, 2018)



- Bots per country (source: Spamhaus, 2019 October)



Next

- XSS & CSRF
- Malware
- Secure Program Development
- Detection