



An overview of Malware Threats

NT101 – NETWORK SECURITY

Giảng viên: Nghi Hoàng Khoa | khoanh@uit.edu.vn

- **Tổng quan về phần mềm độc hại**
 - Taxonomy
 - Propagation
 - Payload
 - Countermeasures

Malware

An overview





Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)

If you'd like to know more, you can search online later for this error: HAL_INITIALIZATION_FAILED

What is Malware?



- Malware is **malicious software** - hành động chống lại chủ sở hữu hoặc người dùng
- NIST (SP 800-83) định nghĩa rằng:

*“a program that is inserted into a system, usually covertly, with the intent of compromising the **confidentiality, integrity, or availability** of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim”*

- **Làm thế nào một phần mềm độc hại có thể xâm nhập vào hệ thống?**

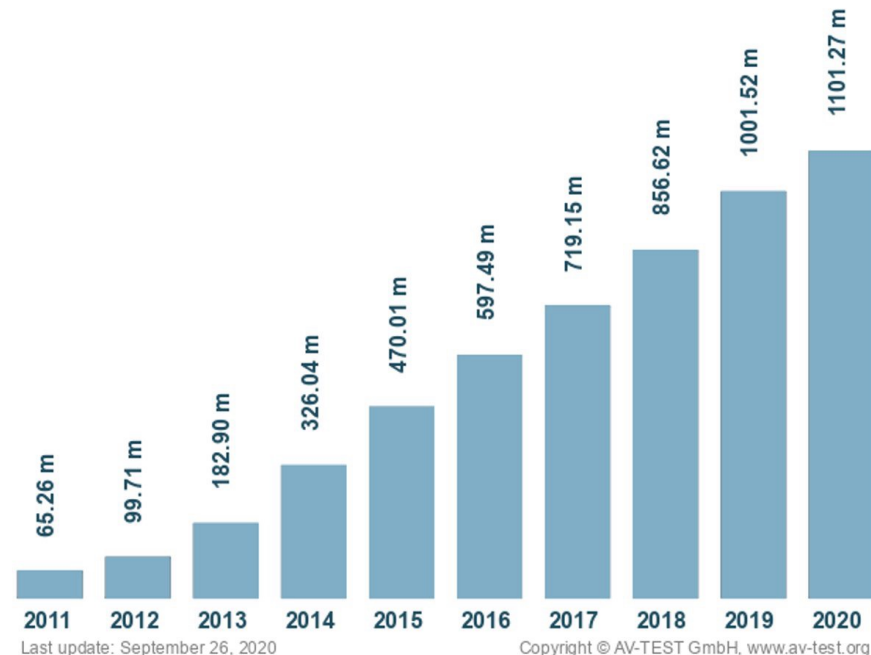
- Ứng dụng nhắn tin
- Thiết bị ngoại vi
- Lỗ hổng trình duyệt và phần mềm
- Quản lý bản vá không an toàn
- Các trang web không đáng tin cậy và ứng dụng web miễn phí
- Tải xuống tập tin từ Internet
- Tập tin đính kèm Email
- Lan truyền mạng
- Dịch vụ chia sẻ tập tin (FTP, SMB)



- Tổng số (Tháng 9 2020):

~1.101.270.000

- Hơn **350.000** phần mềm độc hại mới **mỗi ngày**
- Hơn **7** tỷ cuộc tấn công phần mềm độc hại đã được báo cáo trong năm 2019
- **4 công ty** trở thành nạn nhân của cuộc tấn công ransomware **mỗi phút**
- Tỷ lệ lây nhiễm phần mềm độc hại **IoT** tăng 33% (từ 2018 đến 2019)
- **Trojan** là phần mềm độc hại phổ biến nhất trên toàn cầu (11%)

AV-TEST



- Có bao nhiêu biến thể của malware?

- Adware
- Backdoor
- Bots/Botnets
- Keyloggers
- Mobile malware
- Ransomware
- Rootkits
- Spyware
- Trojan horse
- Viruses
- Worms
- ...

- Cơ chế lan truyền:

- Infected content – Viruses
- Vulnerability exploit – Worms
- Social engineering – Spam email, trojans

- Payload:

- System corruption – Logic booms
- Tác nhân tấn công – Zombie, Bots
- Đánh cắp thông tin – Keylogger, Phishing, Spyware
- Trộm cắp – Backdoors, Rootkits



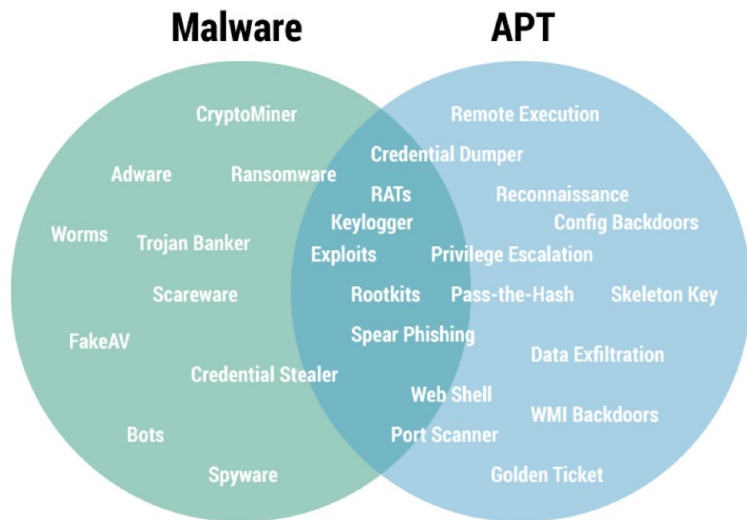
Advanced Persistent Threat



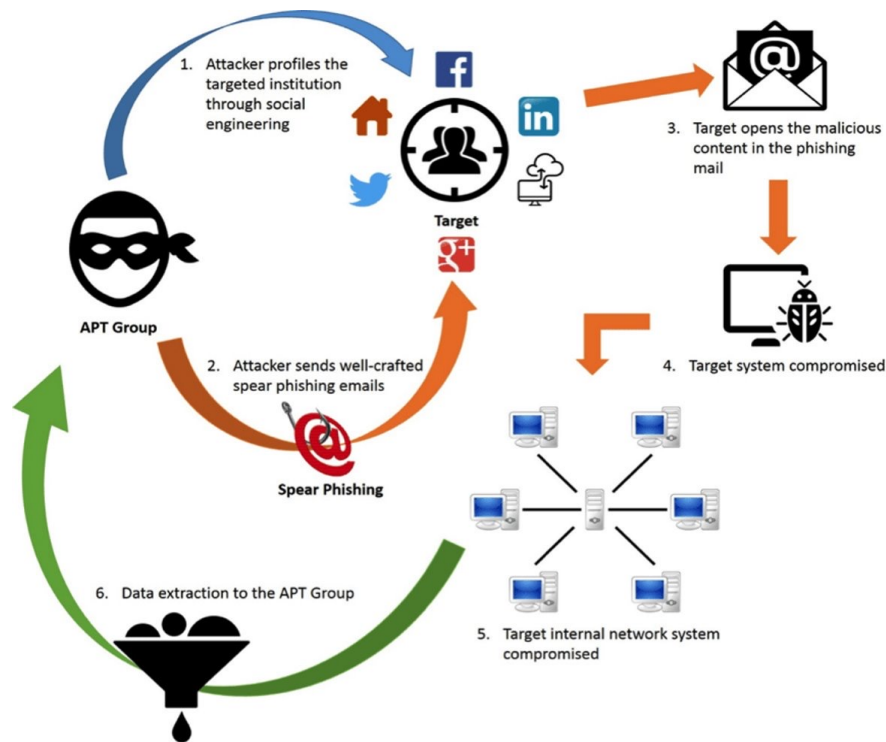
- *Cybercrime, typically a nation state or state-sponsored group, directed at **business** and **political** targets, using a wide variety of intrusion technologies and malware, applied **persistently** and effectively to **specific** targets over an extended period, often attributed to state-sponsored organizations.*
- **Advanced:** đã lựa chọn cẩn thận nhiều loại kỹ thuật thu thập thông tin tình báo và xâm nhập cũng như phần mềm độc hại.
- **Persistent:** dần dần, và thường lén lút, được áp dụng cho đến khi mục tiêu bị xâm phạm.
- **Threats:** do mục đích của những kẻ tấn công có tổ chức, có khả năng và được tài trợ tốt.
(*threat = capability + intent*)



Advanced Persistent Threat (tt)



- Các kỹ thuật phổ biến: *social engineering, spear-phishing e-mails, and drive-by-downloads...*
- Ví dụ: [Aurora](#), [RSA](#), [APT1](#), and [Stuxnet](#)



<https://www.cynet.com/blog/warning-signs-that-you-may-be-under-an-apt-attack/>



Advanced Persistent Threat (tt)



- Hai kiểu malware tự sao chép (self-replicating):
 - **Virus:** Lây nhiễm các chương trình / hệ thống bằng cách sửa đổi chúng
 - Loại malware đầu tiên phổ biến rộng rãi
 - Sự lan truyền được kích hoạt bởi hành động của người dùng (ví dụ: chạy chương trình bị nhiễm)
 - Được sử dụng như một thuật ngữ chung (“anti-virus” SW detects more than viruses!)
 - **Worm:** Phát tán các bản sao qua mạng
 - Thường là một chương trình độc lập (không được đính kèm với một chương trình như virus)
 - Thường lan truyền tự động (không có sự tương tác của người dùng)
 - Khai thác các lỗ hổng (như buffer overflow) để lây lan



Advanced Persistent Threat (tt)



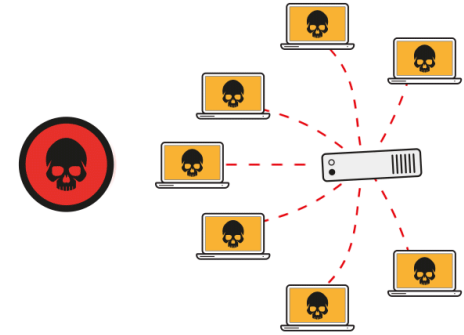
- *Làm thế nào để người dùng không biết về malware?*
- **Trojan Horse:** Ẩn đằng sau một số chức năng mong muốn
 - Malicious code included with game, utility, or other “tempting ware”
 - “Beware of geeks bearing gifts” - *Virgil, 29 B.C.* (well, not quite)
 - Ví dụ 1: [AIDS Trojan](#) (1989 - đĩa mềm được gửi qua đường bưu điện)
 - Ví dụ 2: Phần mềm anti-virus giả mạo
 - Ví dụ 3: App repackagers, app cracked
- **Rootkit:** Che giấu sự tồn tại của phần mềm độc hại
 - User-level rootkits thay thế các lệnh cơ bản của hệ thống
 - Linux: Replace “ps” (hide processes) and replace “ls” (hide files)
 - Windows: Replace Process Monitor and Windows Explorer
 - Kernel-level rootkits đi sâu hơn, ẩn mọi thứ khỏi mọi chương trình



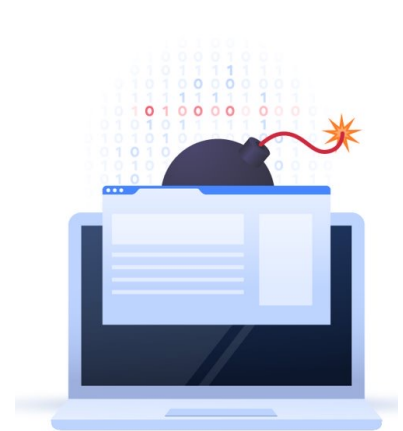
Advanced Persistent Threat (tt)



- **Backdoor:** Cho phép người dùng trái phép truy cập vào hệ thống
 - Thường là một cuộc tấn công từ bên trong - ví dụ: để giữ lại quyền truy cập sau khi rời khỏi
- **Botnets:** Cung cấp cho cuộc tấn công một tài nguyên phân tán
 - Hệ thống bị nhiễm “zombies”
 - Kiểm soát bằng kỹ thuật “command and control”
 - Thường là một kênh công khai khó theo dõi (IRC, Twitter...)
 - Sử dụng phổ biến: để khởi động các cuộc tấn công khác hoặc gửi thư rác và đào coin!
- **Privacy-Invasive Software:** Gửi thông tin về hệ thống hoặc người dùng
- **Spyware** – có thể xem lịch sử duyệt web
- **Adware** - chạy quảng cáo trên máy nạn nhân
- **Keystroke loggers (keyloggers)** – bắt được mật khẩu
 - Thậm chí khai thác webcam!
- **Ransomware:** Mã hóa các tập tin để người dùng không có quyền truy cập
 - Thường yêu cầu thanh toán bằng bitcoin để lấy khóa giải mã



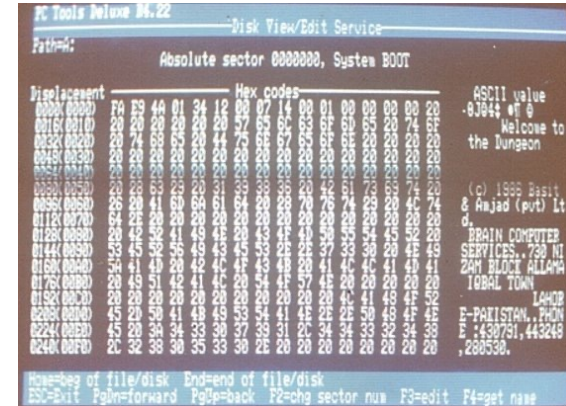
- Sự khác nhau vật trung gian truyền nhiễm (**infection vectors**)
 - Phần mềm phân tán (disk hoặc network)
 - Các dịch vụ mạng có lỗ hổng
 - Ứng dụng có lỗ hổng
 - E-mail: Tự động hoặc đánh lừa người dùng
- Kiểm soát hành vi độc hại
 - Có thể thực thi ngay lập tức
 - Có thể “**kích hoạt**” vào một thời gian cụ thể (“time-bomb”) hoặc điều kiện (“logic-bomb”)
 - Thường do nhân viên cũ bỏ lại - được kích hoạt sau khi bị sa thải
 - Ví dụ: OMEGA Engineering, 1996 (story in book)
 - Có thể được điều khiển từ xa (như trong mạng botnet)



Viruses và Worms đầu tiên



- **1986:** Brain virus (PC virus đầu tiên - MS-DOS)
- **1987:** Jerusalem
 - PC virus đầu tiên (logic bomb) gây thiệt hại trên diện rộng
 - Sử dụng tính năng DOS “Terminate and Stay Resident” (TSR)
 - Đính kèm với tập tin thực thi .COM và .EXE
 - Vào bất kỳ thứ Sáu ngày 13 nào, xóa mọi chương trình đang chạy
- **1992:** Michelangelo
 - Vào ngày sinh nhật Michelangelo (Ngày 6 Tháng 3) sẽ xóa sách ổ đĩa
 - McAfee dự đoán 5.000.000 máy tính sẽ bị nhiễm virus – chỉ có khoảng 10.000 máy tính bị nhiễm.
Mánh lới quảng cáo bán hàng?



Viruses và Worms đầu tiên (tt)



- **1999: Melissa**
 - MS-Word macro virus
 - Khi tài liệu được mở, sẽ tự gửi cho 50 mục đầu tiên trong sổ địa chỉ
 - Không có thiệt hại trực tiếp, nhưng làm tắc nghẽn nghiêm trọng nhiều máy chủ mail và mạng
 - Ước tính đạt 100.000 máy tính trong tuần đầu tiên
- **2000: Love Bug (ILOVEYOU)**
 - Virus VBScript, lây lan qua e-mail / MS-Outlook (tương tự như Melissa)
 - Hành động độc hại: xóa các tập tin phương tiện (.jpg, .mp3,...)
 - Tác giả đến từ Philippines
- **2001: Code Red** (lây lan qua MS-IIS bug)
- **2003: Slammer** (lây lan qua MS-SQL Server bug)



- Các hình thức lây nhiễm và lây lan tương tự

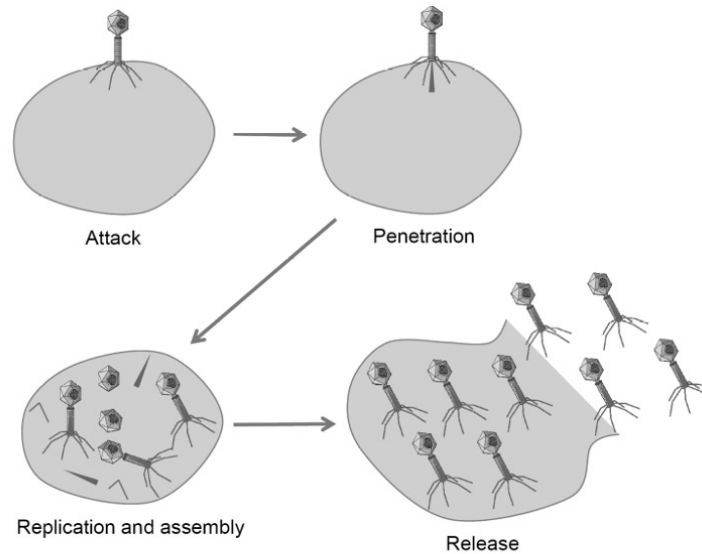
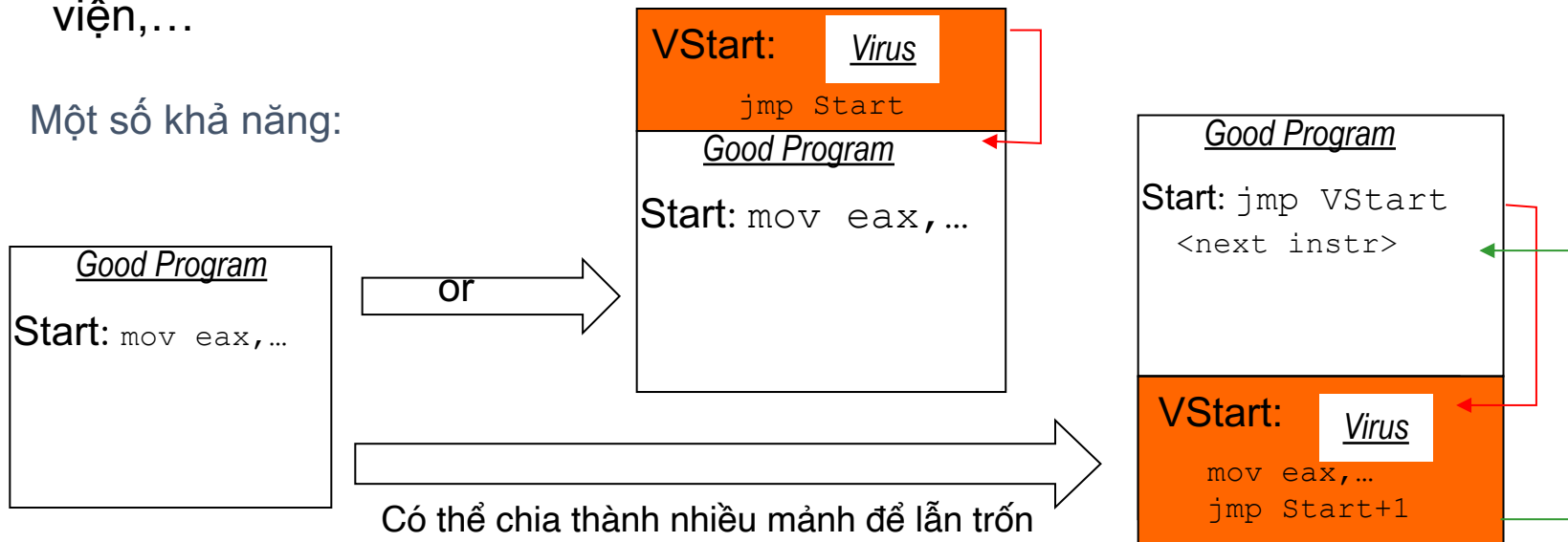


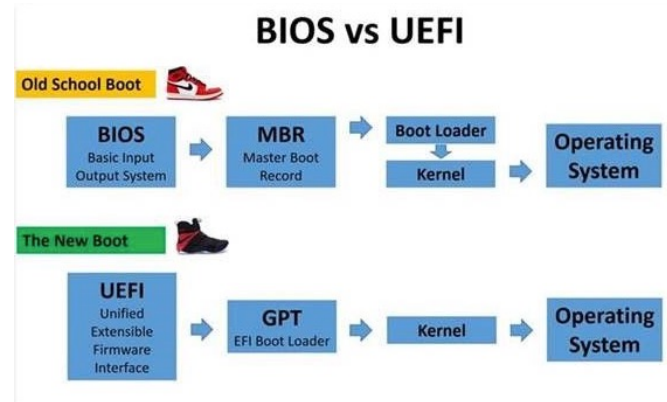
Figure 4.3: Four stages of a biological virus.

- Thuật ngữ do Fred Cohen đặt ra vào năm 1983
- Mã độc hại đính kèm với nội dung đang hoạt động (active content)
 - “active content” có thể là chương trình, tập lệnh, khu vực khởi động, thư viện,...

Một số khả năng:



- Quá trình khởi động:
 - Khởi động firmware (BIOS with POST, initialization, ...)
 - Tải first-stage bootloader (master boot record - MBR)
 - Chạy mã được tìm thấy ở đó - thường là chuỗi đến second-stage bootloader
- Virus được kiểm soát sớm và hoàn toàn thay thế MBR
 - PC Virus đầu tiên (Brain) là boot-sector virus
 - Những công cụ phức tạp hơn có thể tạo hypervisor (như BluePill)
 - UEFI Secure Boot bảo vệ tốt chống lại điều này



First PC Virus – “The Brain”



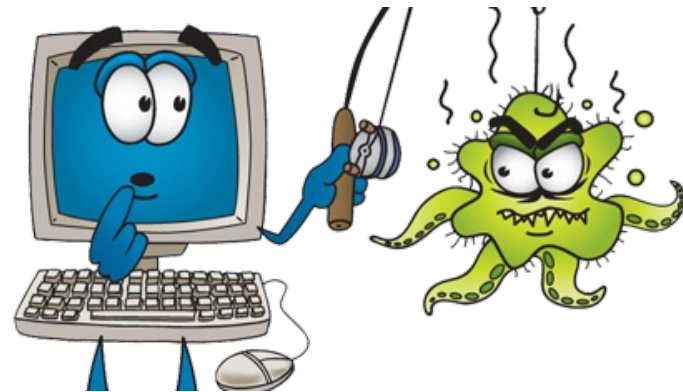
- Được cho là PC virus đầu tiên “in the wild”
- Có nguồn gốc từ Pakistan (“Pakistani Brain”)
- Những gì nó làm:
 - Nằm trong high memory và thường trú
 - Tự sao chép chính nó vào boot sector
 - Tự sao chép bản gốc boot sector và các bản sao bổ sung của chính nó vào các vị trí đĩa khác nhau, được đánh dấu là “bad sectors”
 - Chặn tất cả yêu cầu đọc/ghi đĩa để giả mạo việc đọc boot sector (thay thế bản sao gốc)
 - Trong quá trình đọc / ghi đĩa, tự lây lan sang tất cả các đĩa không bị nhiễm
 - Không có thiệt hại trực tiếp



Macro Viruses



- Không phải lúc nào dữ liệu cũng bị động!
 - Nhiều “định dạng tài liệu” (ví dụ: MS Office) có thể chứa macro
 - Nhiều tập tin (HTML, e-mail) có thể chứa VBScript hoặc JavaScript
- Sớm nhất: Melissa (1999)
 - Sử dụng macro để truy cập sổ địa chỉ Outlook
- Half-fix: MS-Word/Excel/etc hiện yêu cầu hành động bật marco
 - Có bao nhiêu người nhấn “Enable Macros” mà không thực sự hiểu việc này có tác dụng gì?!?



- Nhiều virus lừa bịp trong những năm qua:
 - “Virus Flambé”: được đồn đại là đặt tốc độ đồng bộ hóa màn hình cao đến mức nó sẽ bùng cháy!
 - Trò lừa bịp virus thiệp chúc mừng Blue Mountain: xác nhận có virus trong thiệp chúc mừng điện tử...
 - “Goodtimes” hoax (1994): Trò lừa bịp trên diện rộng đầu tiên
- Luôn kiểm tra với một công ty bảo mật có uy tín (McAfee và Symantec cung cấp thông tin tốt)



- Thay đổi các truyền nhiễm của malware
 - Bây giờ ít "disk swapping" hơn, nhưng kết nối mạng nhiều hơn
- Không hoàn toàn khác với virus
 - Có thể lây nhiễm các tập tin thực thi sau khi sử dụng mạng để phát tán
 - Nhưng thường chỉ được cài đặt trên hệ thống dưới dạng các chương trình bổ sung, hoàn chỉnh
- Sự lan truyền có thể tự động và yêu cầu người dùng làm
 - Thường cố lừa người dùng mở một tệp đính kèm đang hoạt động
 - Cryptolocker gần đây được phát tán bởi Trojan GameOver Zeus như thế này
 - Tự động lây lan qua e-mail (ví dụ: khai thác lỗi Outlook) hoặc các dịch vụ mạng có lỗ hổng (MS IIS, SQL Server,...)



“The Internet Worm”



- Sự cố Internet nghiêm trọng trên diện rộng đầu tiên
 - Ngày 02 tháng 11 năm 1988
 - Được cho là lây lan nhưng không gây ra thiệt hại nào khác
 - Nhưng: Một lỗi trong mã nhân bản đã khiến nó liên tục lây nhiễm sang cùng một máy chủ
 - Làm tắc nhiều hệ thống - sysadmins bị ngắt kết nối (đơn giản)
 - Đã khai thác 3 bug: guessed logins, fingered buffer overflow, send email “debug mode.”
 - Tracking sinh viên Robert Morris, sinh viên tốt nghiệp Cornell
 - Thường được gọi là “Morris worm”
 - Người đầu tiên bị kết án theo Đạo luật Lạm dụng và Lừa đảo Máy tính năm 1986 (phạt \$10k, 3 năm tù treo, 400 giờ phục vụ cộng đồng)
- Một kết quả đáng mừng: mọi người bắt đầu chú ý đến bảo mật
=> CERT (computer emergency response team) được tạo ra để ứng phó với các sự cố



Infamous Worms – Code Red



- Lây lan qua lỗ hổng bảo mật buffer overflow MS IIS
- Được phát hiện vào mùa hè năm 2001
 - Được phân tích trong cuộc chạy marathon (suốt đêm), được hỗ trợ bởi Mountain Dew Code Red (nguồn gốc của cái tên!)
- Ước tính có khoảng 750.000 máy chủ bị nhiễm
- Có thể có động cơ chính trị
 - Thông điệp “Hacked by Chinese” được để lại trên máy
 - Vài tháng sau sự cố “spy-plane”
 - Bao gồm các cuộc tấn công DOS timebomb trên www.whitehouse.gov
- Hai giai đoạn chính: quét / lây nhiễm và tấn công (dựa trên ngày tháng)



<https://www.lifewire.com/what-is-the-code-red-virus-4768498>



Infamous Worms – Slammer



- Còn được gọi là “Sapphire” hoặc “SQL Slammer”
- Lây lan qua lỗ hổng buffer overflow trong MS SQL Server
- Được phát hiện vào đầu năm 2003
- Khả năng lan truyền cực kỳ nhanh chóng!
 - Máy chủ bị nhiễm nhân đôi sau mỗi 8,5 giây
 - Lây nhiễm trên 90% máy chủ có lỗ hổng trong 10 phút
 - Bị nhiễm bởi dịch vụ UDP (không phải TCP)
- Mạng quá tải, vô hiệu hóa các dịch vụ khác
 - Ví dụ: Nhiều máy ATM của Ngân hàng Mỹ ngừng hoạt động



Infamous Worms – Stuxnet



- Một trong những loại worm phức tạp nhất từng được phát hiện (được tìm thấy vào năm 2010)
- Khai thác nhiều lần (ít nhất 4) 0-day được khai thác lan rộng
- Có thể lây lan qua USB cũng như mạng
- Bao gồm cả rootkit để ẩn mình
 - Ước tính đã lây nhiễm trên 200.000 hệ thống
 - Hầu hết không thấy ảnh hưởng gì ngoại trừ sự suy giảm hiệu suất
- Payload độc hại chỉ được gọi trong một số tình huống nhất định (bom logic)
 - Cấu hình máy mục tiêu trùng khớp với máy ly tâm hạt nhân của Iran
 - Đá phá huỷ 1/5 số máy



Trojan horses



- Trojan bắt nguồn từ câu chuyện thành Troy của người Hy Lạp cổ đại
- *A Trojan horse is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function.*
- Các loại Trojan và ví dụ:
 - Remote Access Trojan (RAT): MoSucker, ProRAT, Theef,...
 - Backdoor Trojans: Kovter, Nitol, Quadars, Snake,...
 - Rootkit trojan: Wingbird, Finfisher, GrayFish, Whistler,...
 - Proxy server Trojan: Linux.Proxy.10, Qbot,...
 - Mobile Trojan, IoT Trojan,...



STEP 1: Create a new Trojan packet using a **Trojan Horse Construction Kit**

STEP 2: Create a **dropper**, which is a part in a trojanized packet that installs the **malicious code** on the target system

STEP 3: Create a wrapper using wrapper tools to install Trojan on the victim's computer

STEP 4: Propagate the Trojan

STEP 5: Execute the dropper

STEP 6: Execute the damage routine

Example of a Dropper

Installation path: c:\windows\system32\svchosts.exe
Autostart: HKLM\Software\Mic... \run\explorer.exe

Malicious code

Client address: client.attacker.com
Dropzone: dropzone.attacker.com

A genuine application

File name: chess.exe
Wrapper data: Executable file

Wrappers bind the trojan with a genuine-looking application (game, office, antivirus or **full-cracked app**)



Phá hủy dữ liệu và Ransomware



- Virus phá hủy dữ liệu (Data destruction virus): xóa tất cả dữ liệu trên hệ thống bị nhiễm
 - Ví dụ: Chernobyl virus (1998)
- Ransomware: mã hóa dữ liệu của người dùng và yêu cầu thanh toán để truy cập vào khóa cần thiết để khôi phục thông tin
 - Ví dụ: PC Cyborg Trojan (1989), Gpcode Trojan (public-key crypto - 2006), WannaCry (2017)



- Bot (hay còn gọi là. Robot, zombie, drone): PC bị xâm nhập, máy chủ, thiết bị nhúng như bộ định tuyến hoặc camera giám sát được sử dụng để khởi động các cuộc tấn công vào các máy khác
- Botnet: một mạng (tập hợp) các bot
- Chức năng của bot:
 - Các cuộc tấn công DDoS phân tán
 - Gửi thư rác
 - Sniffing traffic
 - Phát tán phần mềm độc hại mới
 - Cài đặt add-ons quảng cáo
 - Tấn công mạng lưới trò chuyện IRC

```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!  
.  
.  
.  
@88> %8P  
@88> %8P  
888: x888 x888.  
8888~'888X 7888f  
X888 888X '888> .  
X888 888X '888> 888E  
X888 888X '888> 888E  
X888 888X '888> 888E  
X888 888X '888> 888E  
~*88%~*88~ '888! 888& ~8888*~  
R888~ ~Y~ ~Y~ ~Y~  
- A text-based MUD by Oscar Popodokulus -  
No account? Register at www.elrooted.com  
Enter user yop  
yop  
Enter pass yop  
***  
Disconnected by server. |  
Press any key to exit.
```

Carrying “virus” analogy forward...

Models of **biological epidemics** work:

Key variables:

- N = number of vulnerable hosts
- I_t = infected hosts at time t
- S_t = susceptible hosts at time t
- β = infection rate

Basic relations:

$$I_{t+1} = I_t + \beta I_t S_t$$

$$S_{t+1} = N - I_{t+1}$$

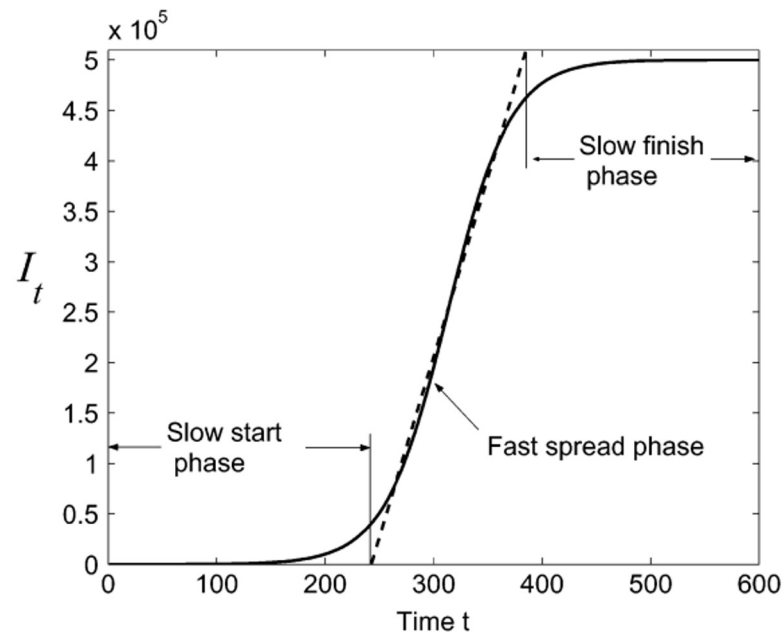


Fig. 1. Worm propagation model.

Cliff C. Zou, Weibo Gong, Don Towsley, and Lixin Gao. 2005. The monitoring and early detection of internet worms. *IEEE/ACM Trans. Netw.* 13, 5 (October 2005), 961-974.

- Một mô hình lý thuyết là tốt, nhưng....
- Nó có phản ánh đúng thực tế không?
- **Có!!!!**

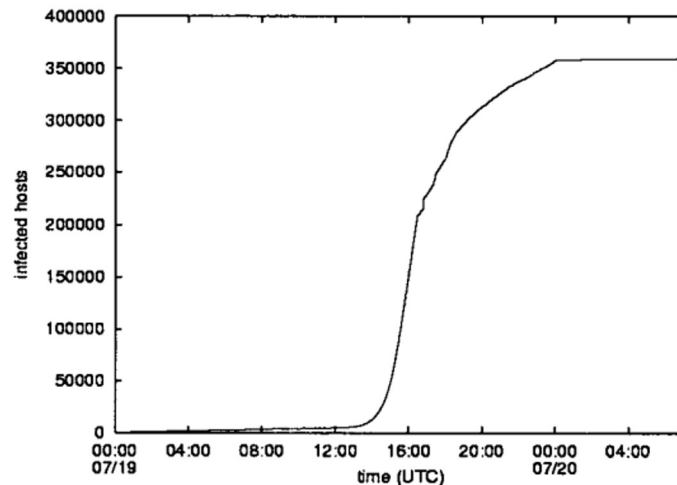


Fig. 2. Cumulative total of unique IP addresses infected by the first outbreak of Code-RedI v2.

David Moore, Colleen Shannon, and k claffy. 2002. Code-Red: a case study on the spread and victims of an internet worm. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement (IMW '02)*, pp. 273-284.

Các biện pháp đối phó: Phát hiện malware



- Signature-Based: Recognizes “known-bad” code
 - Nhà cung cấp có nhóm phân tích malware và cập nhật Signature
 - Thường có thể tránh bị phát hiện với những sửa đổi nhỏ
 - Người dùng phải cập nhật cơ sở dữ liệu virus đã biết!
 - Thận trọng: Nhiều chương trình anti-virus trên máy tính mới có “thời gian dùng thử miễn phí” giới hạn cho các bản cập nhật virus - sau đó dừng lại!
 - Có thể quét toàn bộ hệ thống tập tin hoặc giám sát động - cả hai đều tốt!
 - Tốt: Đáng tin cậy với mức dương tính giả thấp false-positives (độ sai lệch thấp)
 - Xấu: Phải biết malware, 0-days không tránh khỏi
- Anomaly Detection: Detects unusual activity
 - Đọc / ghi một số lượng lớn tập tin
 - Phát hiện mã được gắn với trình xử lý sự kiện (keyboard loggers)
 - Tốt: Có thể phát hiện ngay cả malware không xác định / 0-days
 - Xấu: Có xu hướng có nhiều kết quả dương tính giả false positives

**Misbehaving/bad software can
be quarantined.**



Attackers vs Protectors



- Các kỹ thuật phát hiện mới thường xuyên được phát minh....
- Các kỹ thuật trốn tránh mới thường xuyên được phát minh....
- *Who will win?*
- Một số kỹ thuật trốn tránh để phản hồi với AV tốt hơn:
 - **Polymorphic** or encrypted viruses (Đa hình hoặc mã hoá)
 - Code lõi được trình bày khác nhau trong các phiên bản khác nhau
 - Ví dụ: Mã virus được mã hóa bằng các khóa khác nhau
 - Thường thì một phần chính (trình giải mã hoặc trình biến hình virus) có thể được nhận dạng
 - **Metamorphic** viruses (siêu đa hình)
 - Toàn bộ code thay đổi thông qua các phép biến đổi bảo toàn chức năng
 - Có thể xáo trộn các thanh ghi đã sử dụng, thêm mã vô dụng, sử dụng các hoạt động tương đương...
 - Khó phát hiện hơn nhiều!
- **Sắp tới: Phân tích sâu hơn malware trong các môn NT230 và NT137**



- Chuẩn bị
 - Chủ đề dự kiến: **Network and Internet Security: The big picture and TCP/IP revision**
 - Tài liệu:
 - **IT005 course (Introduction to Computer Network)**, tập trung vào Chapter 8
 - **CS book, Chapter 22**
 - Hoàn tất thống nhất topic của đồ án

- Intrusion detection system (IDS)
- Honeypots
- Firewall and Intrusion prevention system (IPS)
- Security information and event management (SIEM)
- Network security monitoring
- Isolation and sandboxing techniques
- DoS/DDoS attack and detection
- Advanced Persistent Threat
- Container-based (Docker/K8s) security
- Cloud and IoT Security
- SDN Security
- Web application security
- Wireless Security
- Network security protocols
- Anonymity - Tor network and deep web
- Tracking the trackers – Web privacy
- Learning-based (ML/DL) for attack detection
- Generative Adversarial Network (GAN) attacks
- Zero-Trust Network
- DevSecOps
- Security of Routing Protocols and BGP
- Cybersecurity in Quantum era

Hôm nay, kết thúc!

- Nghi Hoàng Khoa
- khoanh@uit.edu.vn
- www.inseclab.uit.edu.vn
- NT101 – An toàn Mạng máy tính

