



Bài 08. Phần mềm mã độc

ONE LOVE. ONE FUTURE.

1

1

Nội dung

- Giới thiệu về phần mềm mã độc
- Virus
- Trojan
- Worm
- Phát hiện và giảm thiểu nguy cơ tấn công bằng phần mềm độc hại

2



1. Giới thiệu chung

ONE LOVE. ONE FUTURE.

3

3

Khái niệm

- Phần mềm độc hại (malicious software hoặc malware) là những chương trình máy tính mà khi thực thi sẽ gây tổn hại tới tài nguyên của hệ thống hoặc chiếm đoạt một phần/toàn bộ quyền điều khiển hệ thống
- Phân loại:
 - Virus: cần hành động kích hoạt của người dùng để lây nhiễm
 - Worm (Sâu máy tính): không cần hành động kích hoạt của người dùng để lây nhiễm
 - Trojan: chương trình ẩn giấu trong các tệp tin có vẻ vô hại, không có khả năng tự lây nhiễm
 - Sự phân biệt các loại này là không rõ ràng.



4

Các hành vi gây hại

- Phá hủy dữ liệu, phần cứng
- Nghe trộm hoạt động của người dùng trên các thiết bị vào ra (Keylogging)
- Đánh cắp thông tin (spyware)
- Mã hóa dữ liệu (ransomware)
- Đánh cắp tài nguyên tính toán (coinminer)
- Tạo cửa hậu (backdoor) để kẻ tấn công xâm nhập và điều khiển
- Che giấu hoạt động (rootkit)
- Thực hiện các hành vi tấn công (botnet)

Các hành vi này có thể được thực hiện ngay hoặc đợi điều kiện nào đó (time bomb, logic bomb)

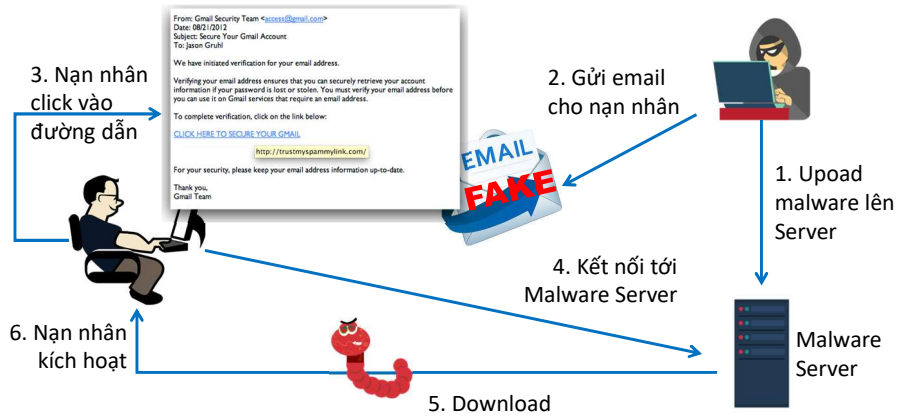
5

Các con đường lan truyền

- Email
- Ứng dụng truyền thông điệp (Instant messaging)
- Các thiết bị lưu trữ di động
- Chương trình giả mạo
- Tiện ích chia sẻ file trong mạng LAN
- Phần mềm bẻ khóa bản quyền
- Chương trình chia sẻ file
- Lỗ hổng phần mềm
- ...

6

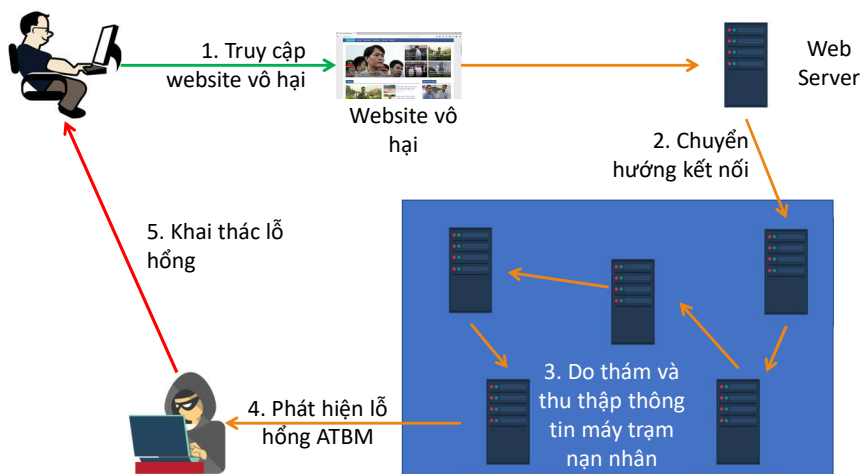
Một kịch bản phát tán và lây nhiễm



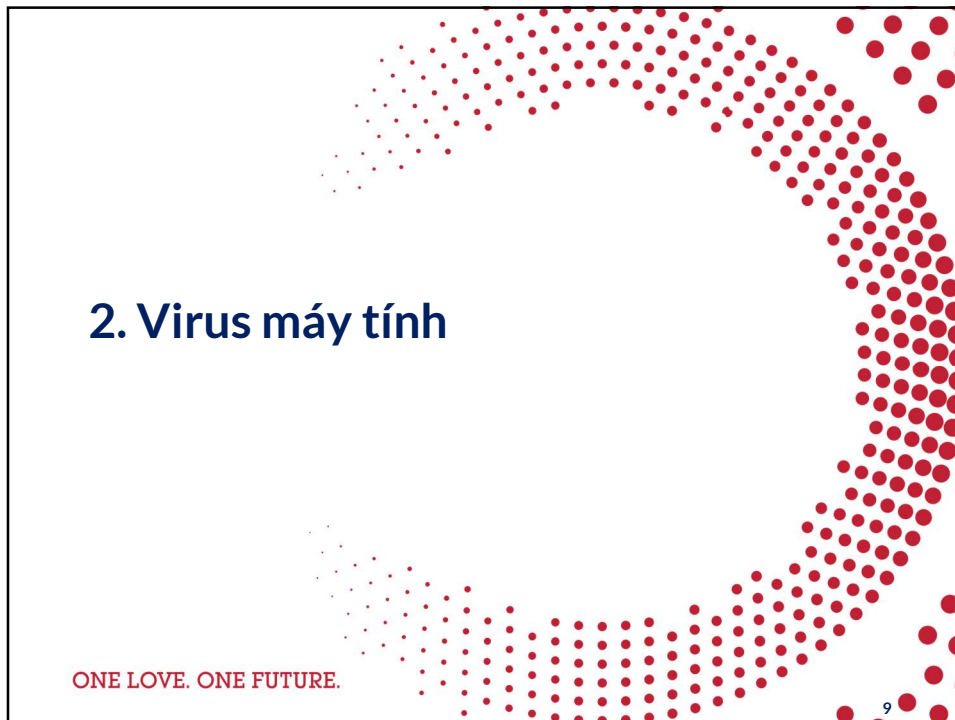
7

Kịch bản khác

- Sử dụng các công cụ khai thác lỗ hổng



8



2. Virus máy tính

ONE LOVE. ONE FUTURE.

9

Cách thức hoạt động của virus

- Virus thông thường có 3 đoạn mã:
 - Đoạn mã lây nhiễm: cho phép virus tự sao chép bản thân nó và lây nhiễm từ chương trình này sang chương trình khác
 - Đoạn mã kích hoạt: Là các sự kiện hoặc điều kiện xác định khi nào *hoạt động chính* sẽ được kích hoạt
 - Đoạn mã hoạt động: phần thực hiện các hành động phá hoại của virus
- Virus được mô tả với 2 đặc trưng:
 - Cách thức lây nhiễm
 - Các hành vi phá hoại

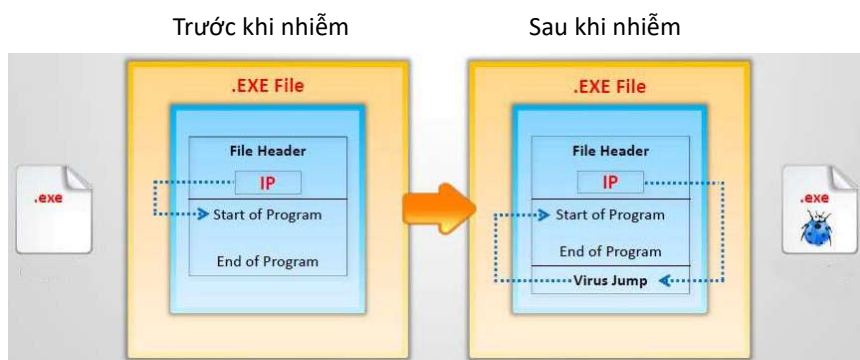
10

Cách thức lây lan

- Mã thực thi, đã cài cắm sẵn, được người dùng kích hoạt, ví dụ:
 - File chương trình ứng dụng
 - Phân vùng khởi động trên ổ cứng
 - File đính kèm email
- (Có thể) Tự sửa đổi, bổ sung mã độc thực thi khác
 - Giải mã các đoạn mã được ẩn giấu
 - Download từ máy chủ phát tán
- Tìm cách lây nhiễm sang các hệ thống khác, ví dụ:
 - Tiêm nhiễm vào file khác
 - Lây nhiễm và thiết bị nhớ di động
 - Gửi email có file đính kèm chứa mã độc

11

Cơ chế tiêm nhiễm



- Nguyên tắc cơ bản: Virus thay thế lệnh đầu tiên của file bị nhiễm (.exe) bằng một lệnh JUMP tới đoạn mã thực thi của virus. Kết thúc đoạn mã thực thi của virus là lệnh JUMP khác để nhảy tới lệnh đầu tiên của chương trình ban đầu

12

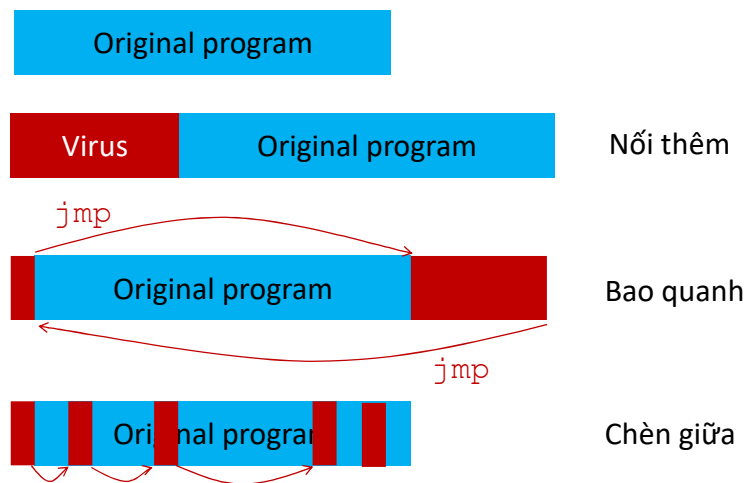
Phát hiện virus

- Phương pháp phổ biến: Phát hiện dựa trên đặc trưng
 - Thu thập các mẫu virus và xây dựng CSDL đặc trưng về các virus. Thông thường là các đoạn mã lây nhiễm ở đầu file
 - Phát hiện: So sánh các byte trên file với những mẫu virus đã có
- Đối phương sẽ làm gì?

13

Cách thức lẩn tránh

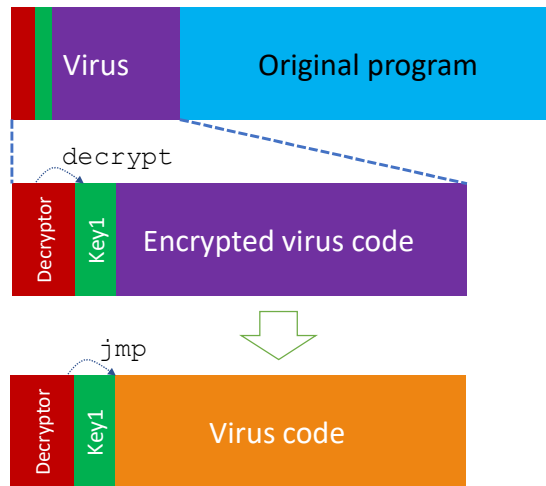
- Làm cho đặc trưng trở nên khó tìm kiếm hơn



14

Polymorphic virus – Virus đa hình

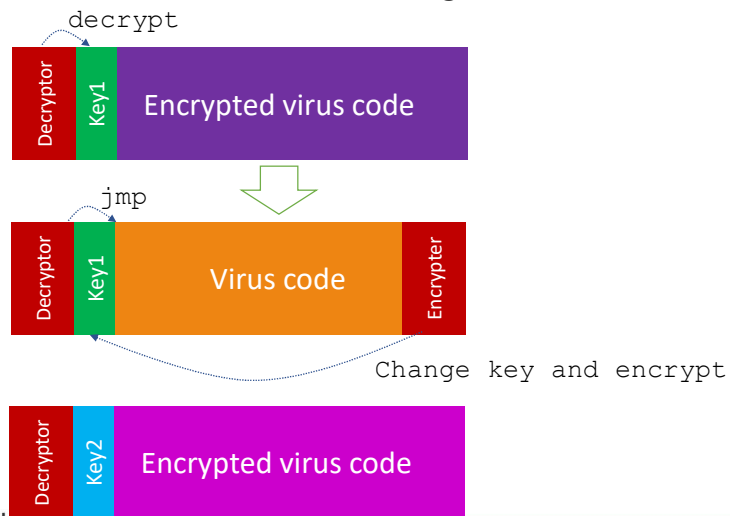
- Thay đổi mã nguồn một cách ngẫu nhiên



15

Polymorphic virus – Lây nhiễm

- Thay đổi khóa và mã hóa lại mã nguồn



16

Polymorphic virus – Phát hiện

- Ý tưởng 1: Sử dụng đặc trưng “hẹp” để phát hiện trình giải mã decryptor
 - Số byte mã nguồn cần so sánh ít hơn → dễ phát hiện nhầm
 - Tin tặc có thể nhanh chóng thay đổi trình giải mã
- Ý tưởng 2: Thực thi để phát hiện sự có mặt của đặc trưng trên mã nguồn đã giải mã
 - Thách thức: Thực thi đến thời điểm nào thì so sánh đặc trưng?
- Làm thế nào để lẩn tránh chương trình phát hiện virus?

Metamorphic Virus



T-1000 in Terminator 2

Metamorphic Virus

- Virus siêu đa hình: sử dụng đoạn mã đặc biệt (metamorphic code) để tự thay đổi mã nguồn về mặt ngữ nghĩa khi thực thi
 - Không thay đổi ngữ nghĩa ở mức cao hơn (vẫn giữ nguyên các chức năng, tính năng)
- Một số kỹ thuật thực hiện:
 - Tạo ra các đoạn mã dư thừa ngẫu nhiên
 - Thay đổi các thanh ghi
 - Thay đổi trình tự trong biểu thức điều kiện
 - Thay đổi trình tự các câu lệnh xử lý không có ràng buộc với nhau
 - Thay thế các thuật toán

Win95/Regswap(1998)

```
5A          pop  edx
BF04000000  mov  edi,0004h
8BF5       mov  esi,ebp
B80C000000  mov  eax,000Ch
81C288000000  add  edx,0088h
8B1A       mov  ebx,[edx]
899C8618110000  mov  [esi+eax*4+00001118],ebx

58          pop  eax
BB04000000  mov  ebx,0004h
8BD5       mov  edx,ebp
BF0C000000  mov  edi,000Ch
81C088000000  add  eax,0088h
8B30       mov  esi,[eax]
89B4BA18110000  mov  [edx+edi*4+00001118],esi
```

Win32/EvoI(2000)

a. An early generation:

```
C7060F000055 mov    dword ptr [esi],5500000Fh
C746048BEC5151 mov    dword ptr [esi+0004],5151EC8Bh
```

b. And one of its later generations:

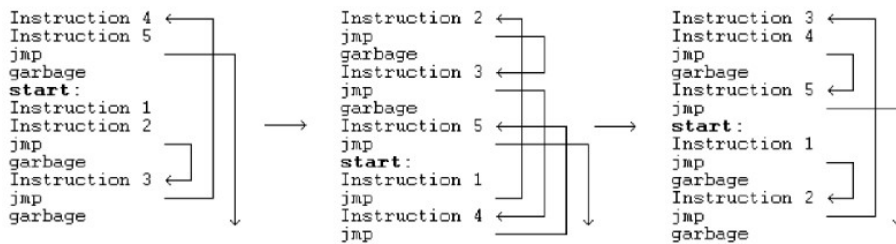
```
BF0F000055    mov    edi,5500000Fh
893E          mov    [esi],edi
5F           pop    edi
52           push   edx
B640          mov    dh,40
BA8BEC5151    mov    edx,5151EC8Bh
53           push   ebx
8BDA          mov    ebx,edx
895E04        mov    [esi+0004],ebx
```

c. And yet another generation with recalculated ("encrypted") "constant" data.

```
BB0F000055    mov    ebx,5500000Fh
891E          mov    [esi],ebx
5B           pop    ebx
51           push   ecx
B9CB00C05F    mov    ecx,5FC000CBh
81C1C0EB91F1 add    ecx,F191EBC0h ; ecx=5151EC8Bh
894E04        mov    [esi+0004],ecx
```

21

Zperm.A(2000)



ZPerm can directly reorder the instructions in its own code

22

Phát hiện virus siêu đa hình

• Phát hiện dựa trên hành vi (Behavior-based detection)

Phân tích động

- Thực thi mã độc trên môi trường Sandbox và quan sát hoạt động của mã độc
- Ưu điểm: thời gian phân tích nhanh, có thể xác định ngay cách thức hoạt động của virus
- Nhược điểm: yêu cầu môi trường an toàn để phân tích, không xác định được hết tất cả các hành vi

Phân tích tĩnh

- Sử dụng kỹ thuật dịch ngược để phân tích mã thực thi
- Ưu điểm: không cần kích hoạt mã độc, xác định được tất cả các cơ chế hoạt động, hành vi của mã độc
- Hạn chế: phức tạp, đòi hỏi trình độ nhân lực cao hơn, mất nhiều thời gian

Quy trình phân tích

Tạo môi trường Sandbox để phân tích

- Bước 1: Tạo các máy ảo (Virtualbox, Hyper-V, ...) và các môi trường ảo hóa khác nếu cần (mạng, CSDL...)
- Bước 2: Cài đặt hệ điều hành trên máy ảo
- Bước 3: Tắt hoặc hạn chế hoạt động của các mạng trên máy ảo để cách ly với môi trường thực
- Bước 4: Tắt các chức năng chia sẻ file, thư mục
- Bước 5: Chuyển mã độc vào môi trường phân tích

Môi trường phân tích phải cách ly hoàn toàn với môi trường làm việc và được giám sát đầy đủ

Quy trình phân tích

Phân tích tĩnh

- Bước 1: Dịch ngược mã nguồn
- Bước 2: Thu thập thông tin:
 - Giá trị các xâu ký tự: sử dụng công cụ BinText
 - Các kỹ thuật đóng gói, nén, mã hóa của virus và thực hiện các thao tác giải nén, giải mã cần thiết: sử dụng công cụ UPX

Phân tích động

- Bước 3: Thiết lập kết nối mạng(vật lý) cho môi trường phân tích. Lưu ý, giám sát chặt chẽ và không kết nối với mạng tác nghiệp của tổ chức
- Bước 4: Kích hoạt virus và thu thập thông tin tiến trình thực thi của virus, thông tin hệ thống khi virus hoạt động. Sử dụng các công cụ Process Monitor và Process Explorer

Quy trình phân tích

- Bước 5: Ghi nhận các kết nối mạng(logic) mà virus tạo ra. Bắt và phân tích lưu lượng phát sinh trên các kết nối này. Các công cụ có thể sử dụng: Wireshark, tcpdump, NetResistent, TCPView
- Bước 6: Xác định các tệp tin mới, tiến trình mới được tạo ra, sự thay đổi các giá trị registry trên hệ thống (sử dụng RegShot)
- Bước 7: Phân tích mã thực thi trên RAM, sử dụng công cụ OllyDbg, ProcDump

Lẩn tránh

- Chống phân tích tĩnh: Tạo ra các đoạn mã phức tạp để che giấu hoạt động thực sự
 - Chống phân tích động:
 - Phát hiện môi trường thực thi để thay đổi hành vi
 - Tạo ra các hành động khiến quá trình thực thi kéo dài
 - Ứng phó của phần mềm anti-virus:
 - Tìm kiếm và bỏ qua các đoạn mã/hành vi vô nghĩa
 - Gắn cờ các đoạn mã không quen thuộc
 - Tiếp tục...
- Cuộc đua giữa tin tặc và phần mềm AV mà tin tặc thường bước đi trước(Tại sao?)

Rootkit/Stealth Virus

- Có khả năng ẩn mình trước các phần mềm phát hiện virus.
- Cơ chế chung: sử dụng kỹ thuật hook để chặn các sự kiện và can thiệp vào quá trình xử lý sự kiện
- User-level rootkit: hook vào hàm thư viện
 - Dễ bị phát hiện
- Kernel-level rootkit: hook vào các hàm thực thi lời gọi hệ thống, hàm xử lý ngắt, driver điều khiển thiết bị, firmware của thiết bị
 - Khó bị phát hiện
- Virtualization-based rootkit: ẩn mình trong môi trường ảo hóa → gần như không thể bị phát hiện

Phát hiện và phòng chống rootkit

- Phát hiện dựa trên hành vi
 - Phát hiện các hành vi hook
 - Sự biến đổi của số lượng, tần suất và thứ tự thực hiện các lời gọi hệ thống
- Kiểm tra toàn vẹn tập tin hệ thống
- Phát hiện dựa trên sự sai khác với hệ thống tham chiếu

29

3. Sâu máy tính

ONE LOVE. ONE FUTURE.

30

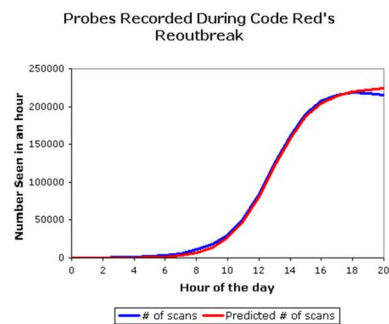
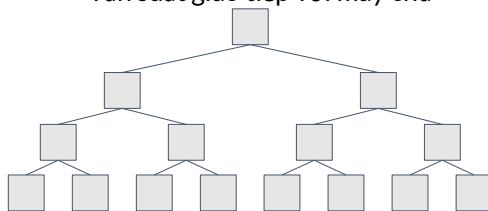
Cách thức lây lan

- Không cần hành động kích hoạt của người dùng
 - Khai thác lỗ hổng phần mềm
- Tìm kiếm nạn nhân mới:
 - Quét mạng theo địa chỉ IP
 - Chọn địa chỉ IP ngẫu nhiên
 - Sử dụng g danh sách sẵn có
 - Truy vấn tới các máy chủ bên thứ 3
 - ...
- Tấn công và lây nhiễm:
 - Quét phát hiện lỗ hổng tương tự trên hệ thống nạn nhân mới
 - Có thể kết hợp với cách thức lây nhiễm của virus

31

Mô hình lây lan của sâu máy tính

- Tương tự cách thức lây lan của virus sinh học
 - Tốc độ lây lan rất nhanh
 - Virus có tốc độ lây lan chậm hơn rất nhiều
- Các yếu tố ảnh hưởng tới tốc độ lây lan:
 - Kích thước của mạng
 - Tỷ lệ nút mạng có lỗ hổng
 - Số lượng nút bị nhiễm
 - Tốc độ quét nạn nhân mới
 - Tần suất giao tiếp với máy chủ



32

Sâu Morris

- Năm ra đời: 1988
- Được coi là sâu máy tính đầu tiên
- Ban đầu được thiết kế để đo đặc kích thước của mạng Internet nhưng vô tình đã gây tấn công DoS
- Khai thác nhiều loại lỗ hổng khác nhau:
 - Lỗ hổng tràn bộ đệm
 - Dò đoán mật khẩu yếu
 - Quét thử các tài khoản phổ biến
- Phương thức lây nhiễm:
 - Quét các máy tính trong mạng đang hoạt động
 - Tìm đọc danh sách các máy tính trong cấu hình mạng của thiết bị
- Ước đoán khoảng 10% máy tính bị lây nhiễm và gây thiệt hại 100M\$ vào thời điểm đó

Sâu Code Red

- Năm ra đời: 2001
- Phương pháp lây nhiễm: khai thác lỗ hổng phần mềm máy chủ Web Microsoft IIS
 - Mặc dù đã có thông báo về bản vá trước đó 1 tháng
- Khoảng 300.000 máy chủ bị nhiễm sau 13 giờ
- Gây hại:
 - Payload 1: Sửa nội dung trang chủ
HELLO! Welcome to <http://www.worm.com>!
Hacked By Chinese!
 - Payload 2: Kích hoạt “bom hẹn giờ”
 - Ngày 1-20 hàng tháng: lây nhiễm
 - Ngày 20+: tấn công DoS vào website Nhà Trắng

Sâu SQL Slammer

- Năm ra đời: 2003
- Khai thác lỗ hổng của MS SQL Server
 - Sau 6 tháng mới có bản vá lỗi
- Kích thước rất nhỏ: được đóng gói trong 1 gói tin
- Sử dụng giao thức UDP để lây nhiễm và tấn công DoS
- Lây nhiễm tới 75.000 máy tính sau 10 phút
 - Số lượng bị nhiễm tăng gấp đôi sau mỗi 8.5 giây
- Đến năm 2016 quay trở lại để tấn công máy chủ ở 172 nước (26% đặt tại Mỹ):
 - Rất nhiều địa chỉ IP thực hiện tấn công là ở Việt Nam



35

Blaster

- Năm ra đời: 2003
- Lây nhiễm qua email
- Số lượng máy tính bị nhiễm: 25 triệu
- Hoạt động gây hại: Tấn công DoS
- Thiệt hại: khoảng 10 tỉ \$



36

Sasser

- Năm ra đời: 2004
- Phương thức lây nhiễm: khai thác lỗ hổng trên hệ điều hành Windows 2000/XP
- Hoạt động gây hại:
 - Khởi động 128 tiến trình quét
 - Khai thác cổng dịch vụ 445 để chiếm quyền điều khiển
 - Tấn công DoS
- Số lượng máy bị nhiễm: ~1 triệu

Conficker

- Năm ra đời: 2008
- Khai thác lỗ hổng trên hệ điều hành Windows 2000/XP/Vista/7, Windows Server 2003/2008
- Có rất nhiều biến thể với các hành vi gây hại khác nhau: A, B, C, D, E, F
- Xây dựng hệ thống mạng botnet lớn nhất vào thời điểm đó
 - Việt Nam: đứng đầu về số lượng máy tính bị nhiễm
- Sử dụng nhiều phương thức khác nhau để lây nhiễm
 - Khai thác lỗ hổng
 - Lây nhiễm qua mạng nội bộ
 - Thiết bị nhớ USB

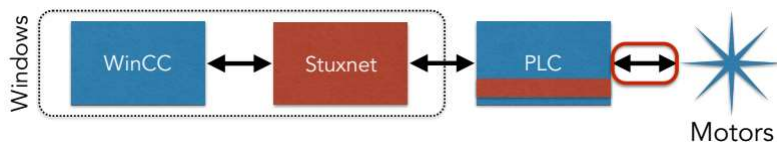
Stuxnet

- Năm phát hiện: 2010
- Mục tiêu tấn công: các máy tính trong mạng công nghiệp SCADA điều khiển hoạt động máy ly tâm
 - 59% máy tính bị nhiễm nằm ở Iran, phần lớn nằm trong các nhà máy hạt nhân
- Khai thác 4 lỗ hổng zero-day khác nhau
- Cách thức lây nhiễm:
 - Khởi nguồn bằng lây nhiễm qua thiết bị nhớ USB
 - Khi đã lọt vào trong mạng, lây nhiễm bằng cách sử dụng Windows RPC
- Cách thức ẩn mình:
 - Cài đặt 1 trình điều khiển thiết bị được chứng thực

39

Stuxnet – Hoạt động gây hại

- Không kích hoạt đến khi tốc độ quay của máy ly tâm đạt 807-1210 Hz
- Từ từ tăng tốc độ của máy ly tâm đến 1410Hz → gây hỏng máy ly tâm
 - Gửi thông báo giả mạo tới trung tâm điều khiển rằng hệ thống hoạt động bình thường
- Sau đó giảm tốc độ về mức bình thường




40

Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

This article is by William J. Broad, John Markoff and David E. Sanger.



Enlarge This Image

Nicholas Roberts for The New York Times

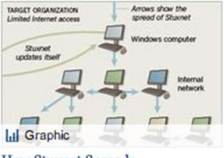
Ralph Langner, an independent computer security expert, solved Stuxnet.

The Dimona complex in the Negev desert is famous as the heavily guarded heart of [Israel's](#) never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine [Iran's](#) efforts to make a bomb of its own.


Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the [Stuxnet](#) computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear

Multimedia



Graphic

How Stuxnet Spreads



DAI HỌC BẮC HANOI UNIVERSITY OF S

RECOMMEND

TWITTER


E-MAIL

SEND TO PHONE

PRINT


REPRINTS

SHARE




41

NotPetya



- Năm phát hiện: 2016
- Bị cáo buộc do hacker Nga phát tán để chống lại Ukraine
- Khai thác lỗ hổng MeDoc Ukrainian Tax Software
- Phát tán qua việc khai thác lỗ hổng Eternal Blue(Windows) và sử dụng công cụ Mimikatz để quét mật khẩu
- Thực hiện mã hóa dữ liệu người dùng như phần mềm mã độc ransomware
 - Thực chất là thực hiện tấn công DoS
- Đánh sập hoạt động của các công ty vận chuyển: Maersk, FedEx



DAI HỌC BẮC KHOA HÀ NỘI HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

42

42

Mã độc diskperf.exe

- Năm phát hiện: 2016
- Lây nhiễm vào hệ thống máy tính của Vietnam Airlines
- Được phát hiện nằm vùng trong rất nhiều hệ thống máy tính của các cơ quan, doanh nghiệp
- Được cho là công cụ của nhóm hacker 1937cn (Trung Quốc)
- Hoạt động gây hại:
 - Mã hóa dữ liệu
 - Tạo cửa sau (backdoor) để kẻ tấn công chiếm quyền điều khiển

WannyCry

- Năm phát hiện: 05/2017
- Ransomware gây hại lớn nhất trong lịch sử
- Khai thác lỗ hổng EternalBlue trên hệ điều hành Windows XP/7/8 bằng cách sử dụng công cụ bị rò rỉ của NSA
- Số lượng máy tính bị lây nhiễm: 230.000
- Việt Nam nằm trong những nước bị nhiễm nhiều nhất

Phòng chống và giảm thiểu

- Tránh mở các file đính kèm từ các email không rõ nguồn gốc
- Sử dụng firewall chặn tất cả các cổng dịch vụ không cần thiết
- Tránh nhận các file từ ứng dụng tin nhắn
- Gia cố hệ thống, tắt các chức năng không cần thiết trên máy tính
- Kiểm soát lưu lượng nội bộ
- Không tải và thực thi các file ứng dụng từ nguồn lạ
- Cập nhật các bản vá bảo mật



Phòng chống và giảm thiểu

- Quét, rà soát virus trên các thiết bị nhớ lưu động(USB drive, CD/DVD, thẻ nhớ, thiết bị di động,...) khi kết nối với máy tính
- Phân quyền người dùng
- Sử dụng phần mềm bản quyền. Không dùng các công cụ bẻ khóa, cung cấp mã bản quyền
- Cài đặt phần mềm diệt virus
- Xây dựng chính sách và đào tạo người dùng

