Bài: 7.1 Nguy cơ Malware - Cách lan truyền Malware và khái niệm Trojan

Xem bài học trên website để ủng hộ Kteam: 7.1 Nguy cơ Malware - Cách lan truyền Malware và khái niệm Trojan

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tóm tắt

Malware là từ viết tắt của cụm từ **Malicious Sofware** (phần mềm ác ý). Thuật ngữ **malware** là một thuật ngữ phổ biến chỉ nhiều loại phần mềm độc hại, được thiết kế đặc biệt để tiếp cận mục tiêu, lấy cắp thông tin và phá hoại hệ thống. Bất cứ phần mềm nào tạo ra với mục tiêu ác ý như phá hỏng, vô hiệu hóa hay giới hạn kiểm soát của người dùng chính thống và cung cấp quyền truy cập cho kẻ tấn công hay người phát triển phần mềm đều được coi là malware.

Malware được chia thành nhiều loại như **Viruses**, **Worms**, **Keyloggers**, **Spywares**, **Trojans**, **Ransomware** và các loại malware khác. Hiện nay malware là nguy cơ khá nghiêm trọng. **Malware** loại **Viruses** và **Worms** sử dụng những kĩ thuật cũ trong khi các Malware khác có những thủ đoạn mới mẻ và nguy hiểm hơn.

Cách lan truyền malware

Có rất nhiều cách để **malware** truy cập vào hệ thống. User nên cẩn thận khi tiếp cận các phương pháp lan truyền **malware** phổ biến sau:

- Phần mềm miễn phí

Khi cung cấp miễn phí phần mềm trên mạng, phần mềm đó thường được tổ chức cung cấp đính kèm một số phần mềm và ứng dụng khác. Bên thứ ba có thể lợi dụng những phần mềm thêm vào này để lan truyền malware.

Ví dụ tiêu biểu nhất của phần mềm miễn phí là những tệp crack chứa malware, hoặc chỉ có malware ngụy trang thành tệp crack.

- Dịch vụ chia sẻ tệp

Dịch vụ chia sẻ tệp như **torrent** và **Peer-to-peer** chuyển tiếp tệp qua vô số máy tính. Trong quá trình chia sẻ, tệp có thể bị nhiễm độc, hoặc tệp nhiễm độc có thể được chia sẻ kèm theo bởi vì có một máy tính bảo mật kém.

- Phương tiện có thể gỡ bỏ

Malware có thể lan truyền thông qua các phương tiện như **USB**. Có nhiều loại malware nâng cao có thể lan truyền qua khu lưu trữ của **USB** cũng như qua Firmware gắn trong phần cứng. Ngoài **USB**, **External hard disk**, **CD**, **DVD** cũng có thể chứa malware bên trong.

- Email

Hiện nay, email là phương tiện giao tiếp phổ biến nhất trong một tổ chức. **Malware** có thể lan truyền thông qua tệp đính kèm trong email hoặc email có chứa URL ác ý.

- Không sử dụng tường lửa và Anti-Virus

Vô hiệu hóa tường lửa và chương trình **Anti-Virus** hay không sử dụng các phần mềm an ninh Internet có thể gây ra việc tải về malware ngoài ý muốn. **Anti-virus** và tường lửa sẽ chặn tải về malware tự động và cảnh báo khi phát hiện malware.

Khái niệm Trojan

Trojan Horse và **Trojan** là những chương trình ác ý, hành động sai lệch với những dự định ban đầu. Thuật ngữ này bắt nguồn từ một câu chuyện Hi Lạp cổ về một con ngựa gỗ lớn chứa các binh sĩ ẩn nấp bên trong. Khi con ngựa này vào thành phố, các binh sĩ này nhảy ra và bắt đầu tấn công thành phố.

Giống như câu chuyện, **Trojan horse** hành động sai lệch với những dự định ban đầu và đợi thời cơ tốt nhất để tấn công. Phần mềm **Trojan** này có thể giúp kẻ tấn công tiếp cận thông tin cá nhân cũng như cung cấp quyền truy cập không chính thống. **Trojan** cũng có thể làm các thiết bị kết nối chung một mạng bị nhiễm độc.

Trojan

Một phần mềm ác ý đánh lừa user về mục đích thật sự của nó được coi là **Trojan**. **Trojan** thường được lan truyền qua tấn công phi kĩ thuật. Mục đích chính của việc sử dụng Trojan là:

- Tạo cửa sau
- Lấy quyền truy cập không chính thống
- Lấy cắp thông tin
- Lây nhiễm các thiết bị kết nối
- Tấn công ransomware (mã độc tống tiền)
- Sử dụng nạn nhân để spam
- Sử dụng nạn nhân như Botnet
- Tải về các malware khác
- Vô hiệu hóa tường lửa

Số port	Loại port	Trojans
2	TCP	Death
20	TCP	Senna Spy
21	TCP	Blade Runner / Doly Trojan / Fore / Invisble FTP / WebEx / WinCrash
22	TCP	Shaft
23	TCP	Tiny Telnet Server
25	TCP	Antigen / Email Password Sender / Terminator / WinPC / WinSpy
31	TCP	Hackers Paradise / Masters Paradise
80	TCP	Executor
421	TCP	TCP Wappers Trojan
456	TCP	Hackers Paradise
555	TCP	Ini-Killer / Phase Zero / Stealth Spy
666	TCP	Satanz backdoor
1001	TCP	Silencer / WebEx
1011	TCP	Doly Trojan
1095-1098	TCP	RAT
1170	TCP	Psyber Stream Server / Voice
1234	TCP	Ultors Trojan
10000	TCP	Dumaru.Y
10080	TCP	SubSeven 1.0-1.8 / MyDoom.B
12345	TCP	VooDoo Doll / NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill
17300	TCP	NetBus
27374	TCP	Kuang2 / SubSeven server (default for V2.1-Defcon)
65506	TCP	SubSeven
53001	TCP	Remote Windows Shutdown
65506	TCP	Various names: PhatBot, Agobot, Gaobot

Quy trình lây nhiễm Trojan

Kẻ tấn công sử dụng những bước sau để gây nhiễm **Trojan** cho hệ thống mục tiêu.

1. Tạo ra một **Trojan** sử dụng **Trojan Construction Kit** (bộ xây dựng Trojan).
2. Tạo ra một **Dropper**.
3. Tạo ra một **Wrapper**.

4. Lan truyền **Trojan**.
5. Thực thi **Dropper**.

Trojan Construction Kit cho phép người sử dụng tạo ra **Trojan** của riêng mình. Những Trojan tự tạo này nguy hiểm cho cả mục tiêu lẫn kẻ tấn công nếu không được thực thi đúng cách hoặc cháy ngược (backfire). **Trojans** tự tạo có thể tránh sự phát hiện từ máy quét virus và Trojan.

Một vài Trojan Construction Kit:

- Dark Horse Trojan Virus Maker
- Senna Spy Generator
- Trojan Horse Construction Kit
- Progenic mail Trojan Construction Kit
- Pandora's Box

Droppers

Dropper là một phần mềm hay chương trình thiết kế chủ yếu để chuyển một **payload** **(*)** đến hệ thống mục tiêu. Mục tiêu chính của **Dropper** là cài đặt mã malware vào máy tính mục tiêu, tránh khỏi cảnh báo và phát hiện. Nó sử dụng rất nhiều phương pháp để lan truyền và cài đặt malware.

(*) *Trong an ninh máy tính,* ***payload*** *là một phần của một malware như sâu máy tính hay virus, một đoạn code được chạy trên máy nạn nhân, dùng để thực hiện một số hoạt động độc hại nào đó, như hủy bỏ dữ liệu, gởi spam hay mã hóa dữ liệu. Thêm vào payload, những malware như vậy có thêm overhead code để lan truyền nó, hay để tránh bị nhận diện.*

Công cụ **Trojan-Dropper**:

- TrojanDropper: Win32/Rotbrow.A
- TrojanDropper: Win32/Swisyn
- Trojan: Win32/Meredrop
- Troj/Destover-C

Wrapper

Wrapper là một tệp thường gắn với tệp ác ý để lan truyền **Trojan**. **Wrappers** thường là những tệp thực thi phổ biến như trò chơi, âm nhạc, tệp video cũng như những tệp không ác ý khác.

Crypter

Crypter là phần mềm sử dụng khi tạo ra **Trojan**. Chức năng cơ bản của **Crypter** là mã hóa, phức tạp hóa và điều chỉnh malware và chương trình ác ý. Bằng cách sử dụng Crypter để giấu tệp, các phần mềm an ninh sẽ khó phát hiện ra malware hơn. Phần mềm này thường được hacker sử dụng để tạo ra malware có khả năng qua mặt các chương trình an ninh bằng cách ngụy trang như một phần mềm không ác ý cho đến khi được cài đặt.

Một vài **Crypter** sẵn có để giấu chương trình ác ý là:

- Cryogenic Crypter
- Heaven Crypter
- Swayz Cryptor

Triển khai Trojan

Quy trình **triển khai phần mềm Trojan** khá đơn giản. Một kẻ tấn công sẽ tải **Trojan** lên một serve và phần mềm này sẽ tự động tải về khi nạn nhấn ấn vào link. Sau khi tải lên, kẻ tấn công sẽ gửi một email chứa đường link ác ý. Khi nạn nhân nhận được email spam và click vào link, máy sẽ kết nối với Trojan Server và tải Trojan về PC của nạn nhân. Sau khi Trojan được cài đặt ở PC, Trojan sẽ cung cấp cho kẻ tấn công quyền truy cập không chính thống, thông tin cá nhân hay thực hiện một hành động kẻ tấn công thiết kế.

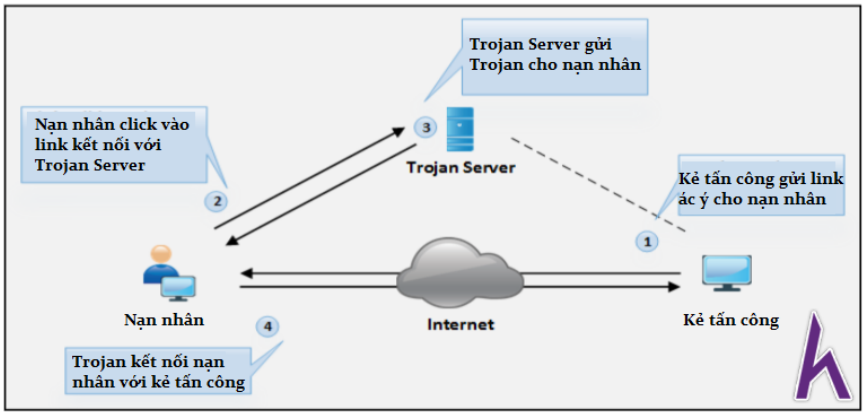


Figure 7-01 Linux Log Directory

Các loại Trojans

- Command Shell Trojans

Command Shell Trojans có khả năng cung cấp quyền kiểm soát từ xa lệnh Shell trên máy tính nạn nhân. Máy chủ Trojan của **Command Shell Trojans** như **Netcat** được cài đặt trên máy tính mục tiêu. Máy chủ Trojan sẽ mở cổng cho ứng dụng bên client kết nối với lệnh shell, ứng dụng client được cài đặt trong máy của kẻ tấn công.

- Defacement Trojans

Sử dụng Trojan này, kẻ tấn công có thể xem, chỉnh sửa và trích rút thông tin từ các chương trình Windows. Kẻ tấn công có thể thay thế chuỗi, hình ảnh và logo bằng những dấu vết của mình. Bên cạnh đó, kẻ tấn công sử dụng ứng dụng tùy chỉnh **User-Styled Custom Application** (UCA), để thay đổi nội dung chương trình. **Website Defacement** là phần mềm phổ biến nhất.

- HTTP/HTTPS Trojans

HTTP và **HTTPS Trojans** qua mặt sự thăm dò của tường lửa và thực thi ứng dụng trên máy mục tiêu. Sau khi thực thi, nó bắt đầu xây dựng đường hầm **HTTP/ HTTPS** để giao tiếp với kẻ tấn công từ máy tính nạn nhân.

- Botnet Trojans

Botnet là tập hợp nhiều máy tính đã bị tấn công hoặc thỏa hiệp, không bị giới hạn trong một mạng LAN nhất định mà có thể lan truyền qua một phạm vi địa lí lớn. Những botnet này được điều khiển bởi **Trung tâm lệnh và kiểm soát** (Command and Control Center). Những botnet được sử dụng để thực hiện tấn công như từ chối dịch vụ, spam, ...

- Proxy Server Trojans

Trojan-Proxy Server là một ứng dụng malware riêng, có thể biến hệ thống host thành một **proxy server**. Kẻ tấn công có thể sử dụng máy tính nạn nhân như một **proxy server** do trojans này kích hoạt tính năng **proxy server** trên hệ thống mục tiêu. Kĩ thuật này được dùng để chuẩn bị cho các tấn công tiếp theo bằng cách che giấu nguồn gốc ban đầu của tấn công.

- Remote Access Trojans (RAT)

RAT cung cấp cho kẻ tấn công quyền truy cập từ xa tới máy tính nạn nhân bằng cách mở Port cho phép truy cập **GUI** tới hệ thống từ xa. **RAT** bao gồm cả một cửa sau để duy trì truy cập quản lí và kiểm soát với mục tiêu. Kẻ tấn công sử dụng **RAT** để quan sát hành động của user, truy cập thông tin tuyệt mật, chụp màn hình, thu âm và quay video sử dụng webcam, định dạng ổ cứng, chỉnh sửa tệp, ...

Dưới đây là danh sách các công cụ RAT:

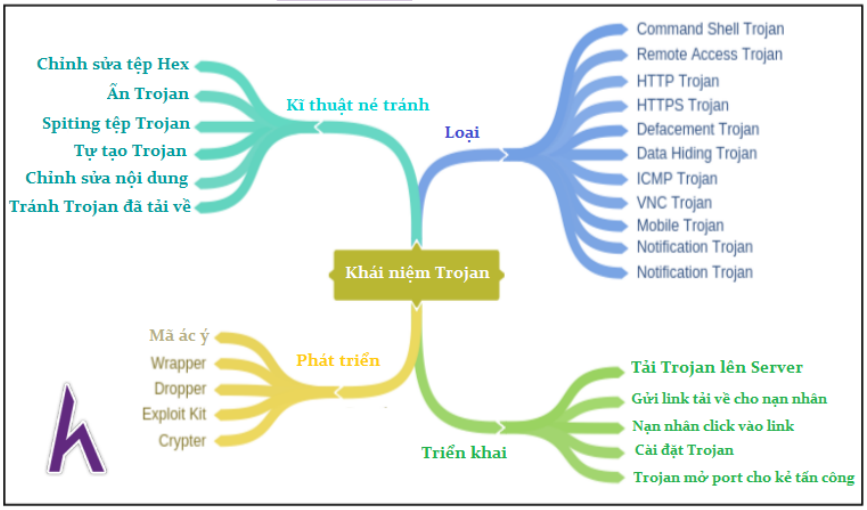
- Optix Pro
- MoSucker
- BlackHole RAT

- SSH-R.A.T
- njRAT
- Xtreme RAT
- DarkComet RAT
- Pandora RAT
- HellSpy RAT
- ProRat
- Theef

Các loại Trojans khác:

- FTP Trojans
- VNC Trojans
- Mobile Trojans
- ICMP Trojans
- Covert Channel Trojans
- Notification Trojan
- Data Hiding Trojan

Mindmap



Biện pháp đối phó Trojan

Một hệ thống hay mạng có thể đối phó với đa số các loại **Trojan** nếu thực hiện những biện pháp phòng tránh tấn công **Trojan** tiêu biểu sau đây.

- Không click vào những tệp đính kèm đáng ngờ trong emai
- Chặn những port không sử dụng
- Quan sát giao thông mạng
- Không tải về tệp từ những nguồn không đáng tin cậy
- Cài đặt phần mềm bảo mật và anti-virus phiên bản nâng cấp
- Quét những phương tiện có thể gỡ bỏ trước khi sử dụng
- Kiểm tra tính toàn vẹn của tệp
- Kích hoạt kiểm kê
- Thiết lập tường lửa host-based
- Phần mềm phát hiện xâm nhập

Cách phát hiện Trojans