MỤC LỤC

Phần 1. Sơ lược malware

1.1. Malware là gì ?

Malware (malicious software) đề cập đến bất kỳ phần mềm xâm nhập nào do tội phạm mạng (thường được gọi là tin tặc) phát triển để đánh cắp dữ liệu và làm hỏng hoặc phá hủy máy tính và hệ thống máy tính.
Mục đích của malware:

- Intelligence and intrusion (tình báo và xâm nhập).
- Disruption and extortion (gây rối và tống tiền): Khóa các mạng và PC, khiến chúng không thể sử dụng được. Nếu malware giữ máy tính của bạn làm con tin để thu lợi tài chính thì nó được gọi là ransomware.
- Destruction or vandalism (phá hoại): Phá hủy hệ thống máy tính để làm hỏng cơ sở hạ tầng mạng.
- Steal computer resources (ăn cắp tài nguyên).
- Monetary gain (Được tiền): Giao dịch trên dark web.

1.2. 7 loại malware

1.2.1. Virus

Virus là phần mềm độc hại được đính kèm vào tài liệu hoặc tệp hỗ trợ macro để thực thi mã của nó và lây lan từ máy chủ này sang máy chủ khác. Sau khi tải về, virus sẽ nằm im cho đến khi file được mở và sử dụng. Virus được thiết kế để phá vỡ khả năng hoạt động của hệ thống.

1.2.2. Worms

Sâu là một loại malware có khả năng sao chép và lây lan nhanh chóng sang bất kỳ thiết bị nào trong mạng. Không giống như virus, sâu không cần chương trình máy chủ để phát tán. Sâu lây nhiễm vào thiết bị thông qua tệp đã tải xuống hoặc kết nối mạng trước khi nó nhân lên và phân tán với tốc độ cấp số nhân. Giống như virus, sâu có thể làm gián đoạn nghiêm trọng hoạt động của thiết bị và gây mất dữ liệu.

1.2.3. Trojan

Virus Trojan được ngụy trang dưới dạng các chương trình phần mềm hữu ích. Nhưng sau khi người dùng tải xuống, vi-rút Trojan có thể truy cập vào dữ liệu nhạy cảm và sau đó sửa đổi, chặn hoặc xóa dữ liệu. Điều này có thể cực kỳ có hại cho hiệu suất của thiết bị. Không giống như các loại virus và worm, Trojan không tự sao chép.

1.2.4. Spyware

Spyware là phần mềm chạy bí mật trên máy tính và báo cáo lại cho người dùng từ xa. Thay vì chỉ làm gián đoạn hoạt động của thiết bị, spyware nhắm mục tiêu vào thông tin nhạy cảm và có thể cấp quyền truy cập từ xa cho attacker. Spyware thường được sử dụng để đánh cắp thông tin tài chính hoặc cá nhân. Một loại phần mềm gián điệp cụ thể là keylogger, ghi lại thao tác gõ phím của bạn để tiết lộ mật khẩu và thông tin cá nhân.

1.2.5. Adware

Adware là malware được sử dụng để thu thập dữ liệu về việc sử dụng máy tính và cung cấp các quảng cáo phù hợp. Mặc dù adware không phải lúc nào cũng nguy hiểm nhưng trong một số trường hợp, nó có thể gây ra sự cố cho hệ thống. Adware có thể chuyển hướng browser đến các trang web không an toàn và thậm chí có thể chứa Trojan và spyware. Ngoài ra, adware có thể làm chậm đáng kể hệ thống.

1.2.6. Ransomware

Ransomware là malware có quyền truy cập vào thông tin nhạy cảm trong hệ thống, mã hóa thông tin đó để người dùng không thể truy cập và sau đó yêu cầu thanh toán tài chính để dữ liệu được phát hành. Ransomware thường là một phần của phishing scam. Bằng cách nhấp vào liên kết không sạch sẽ, người dùng sẽ tải xuống ransomware. Attacker tiến hành mã hóa thông tin cụ thể mà chỉ có thể mở được bằng khóa toán học mà chúng biết. Khi kẻ tấn công nhận được thanh toán, dữ liệu sẽ được mở khóa.

1.2.7. Fileless malware

Fileless malware là một loại memory-resident malware. Nó là malware hoạt động từ bộ nhớ máy tính của nạn nhân chứ không phải từ các tệp trên ổ cứng. Vì không có file để quét nên khó phát hiện hơn malware thông thường. Nó cũng khiến việc điều tra trở nên khó khăn hơn vì fileless malware sẽ biến mất khi máy tính được khởi động lại.

Phần 2. Nghiên cứu Wannacry và một vài malware khác

2.1. Wannacry

Wannacry là một encrypting ransomware được dùng trong tấn công ransomware năm 2017. Wannacry là một chương trình x32 bit được viết bằng ngôn ngữ C++ cho hệ điều hành Windows.

Cách thức lây nhiễm của WannaCry có thể bao gồm:

- Bạn vô tình hoặc cố ý click vào 1 đường link không rõ nguồn gốc, hoặc mở 1 email lạ.
- Chạy các chương trình, phần mềm không rõ nguồn gốc chứa mã virus WannaCry.
- Đặc biệt, virus tự quét (scan địa chỉ IP) các máy tính trong cùng mạng nội bộ (LAN) trong đó bao gồm máy tính của bạn để phát hiện lỗ hổng bảo mật và lây nhiễm vào máy tính của bạn ngay cả khi bạn không thực hiện các hành động ở trên, miễn là máy tính của bạn đang bật và có kết nối mạng nội bộ với máy tính đã nhiễm virus này.

Tổng quan

Cuộc tấn công gồm 3 giai đoạn:

1. Thả một tệp thực thi thứ hai bằng cách thay thế tệp task.exe trong thư mục c:\Windows.
2. Tệp thực thi thứ hai sẽ giải nén các tài nguyên như tệp DLL và tệp EXE, các khóa mật mã, địa chỉ Bitcoin, …
3. Tạo ra nhiều luồng để thực hiện mã hóa tệp trong thiết bị của nạn nhân.

Các dấu hiệu của nhiễm virus:

1. Thay đổi hình nền Desktop thành nền đen chữ đỏ.
2. Mã hóa tệp với WNCRY extension.
3. Xuất hiện khóa đăng kí HKLM\SOFTWARE\Wow6432Node\WannaCryptOr.

Mỗi nạn nhân muốn "hóa giải" đều phải bỏ ra một mức tiền chuộc "máy tính" từ 300 đến 600 Euro tính bằng Bitcoin với hơn 20 ngôn ngữ: Tiếng Anh, Tiếng Đức, Tiếng Trung Quốc, …

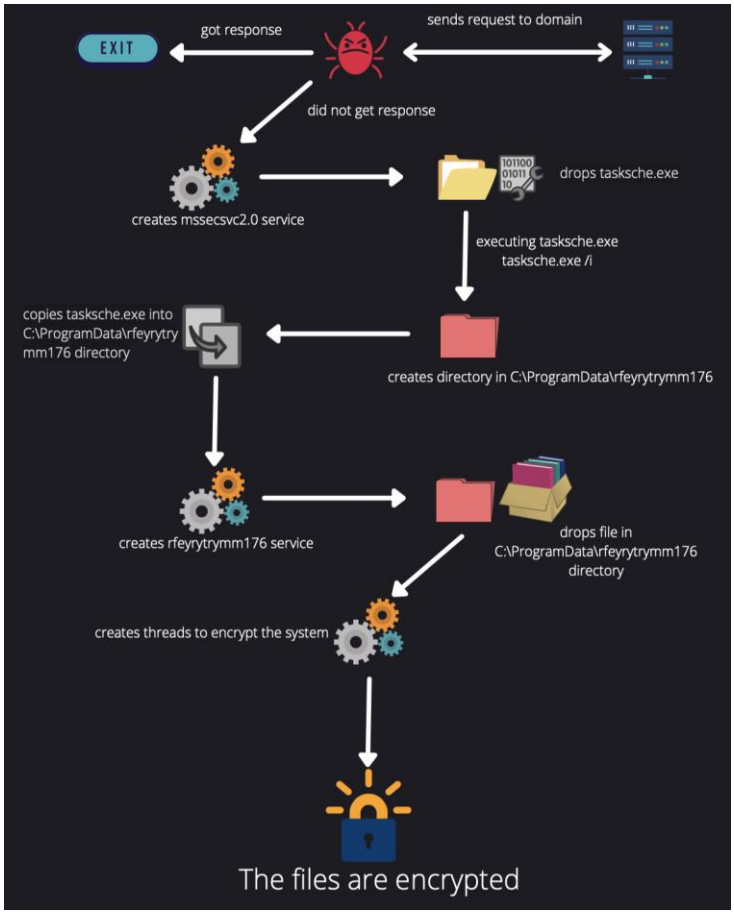
Chuyên sâu

Wannacry ransomware hoạt động qua 3 giai đoạn:

1. Tiếp cận đến một domain. Nếu domain này respond thì wannacry sẽ lập tức thoát ra và không thực hiện. Ngược lại, nếu domain không được kích hoạt, wannacry sẽ bắt đầu tấn công bằng cách tạo một window service với tên service là mssecsvc2.0, tên hiển thị Microsoft Security Center (2.0) Service và đường dẫn "<...>\wannacry.exe-m security". Service này liên tục liên hệ với nhiều địa chỉ IPv4.

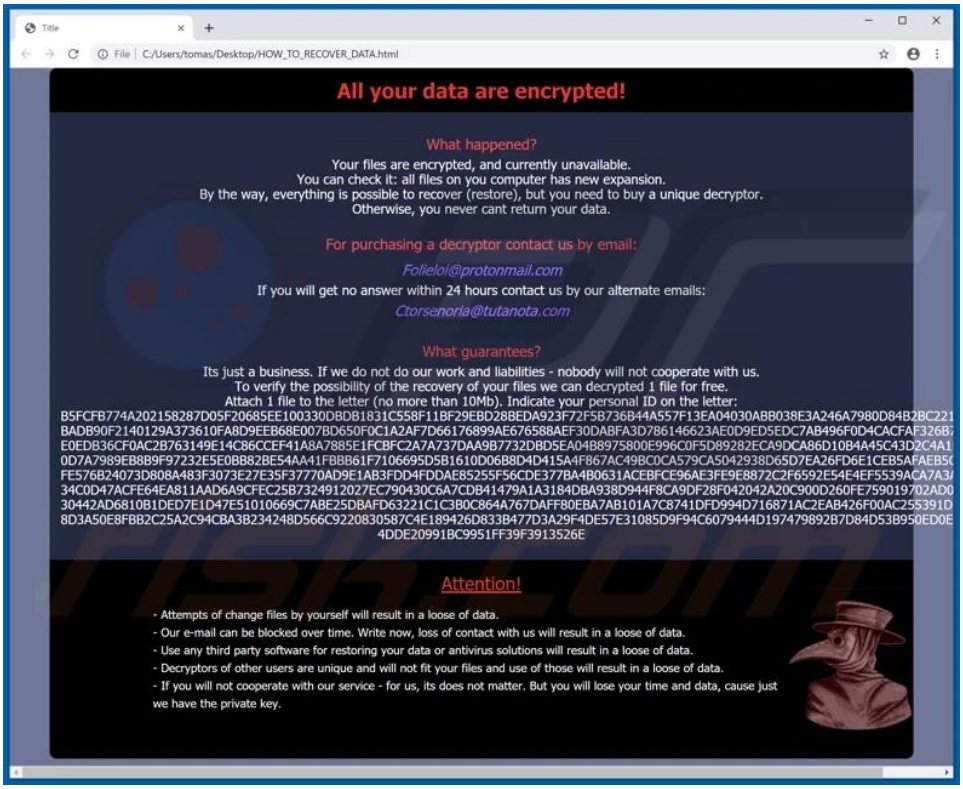
   Sau đó nó kiểm tra xem tệp tasksche.exe có tồn tại trong thư mục C:\\Windows hay không. Nếu tệp nhị phân tồn tại, sau đó nó đổi tên thành qeriuwjhrf.exe và sau đó sao chép một tệp thực thi vào thư mục C:\\Windows với tên là tasksche.exe từ section.
2. Trong Giai đoạn 2, nó tạo một quy trình mới với đối số dòng lệnh "C:\Windows\tasksche.exe /i". /i cho biết quy trình này sẽ bắt đầu quá trình khởi tạo. Trong quá trình khởi tạo này, nó tạo một thư mục trong "C:\ProgramData\rfeyrytrymm176". Sau khi tạo thư mục, nó sẽ di chuyển bản sao của chính nó vào thư mục mới được tạo này, sau đó tạo một service với binary path "C:\ProgramData\rfeyrytrymm176\tasksche.exe". Dịch vụ được tạo sẽ tiếp tục với việc sao chép và mã hóa các tệp EXE, DLL, cryptokeys, hình ảnh, địa chỉ Bitcoin vào thư mục "C:\ProgramData\rfeyrytrymm176".

3. Trong giai đoạn 3, nó tạo ra nhiều luồng (threads) để tiến hành mã hóa tất cả các tệp quan trọng trong hệ thống cục bộ, thay đổi hình nền desktop, sao chép hướng dẫn lên desktop và nhiều tác vụ khác.



2.2. MedusaLocker

MedusaLocker là một họ ransomware xuất hiện vào tháng 9 năm 2019 và được sử dụng nhanh chóng để tấn công các công ty từ khắp nơi trên thế giới.
MedusaLocker chủ yếu dựa vào các lỗ hổng trong giao thức RDP (Remote Desktop Protocol) để truy cập vào mạng của nạn nhân. Dữ liệu của nạn nhân bị mã hóa và một thông báo yêu cầu tiền chuộc kèm theo hướng dẫn liên lạc sẽ được đặt trong mỗi thư mục chứa tệp bị mã hóa. Nạn nhân sẽ được cung cấp một địa chỉ ví Bitcoin cụ thể để trả tiền chuộc. Medusa có khả năng hoạt động dưới dạng mô hình Ransomware-as-a-Service (RaaS).

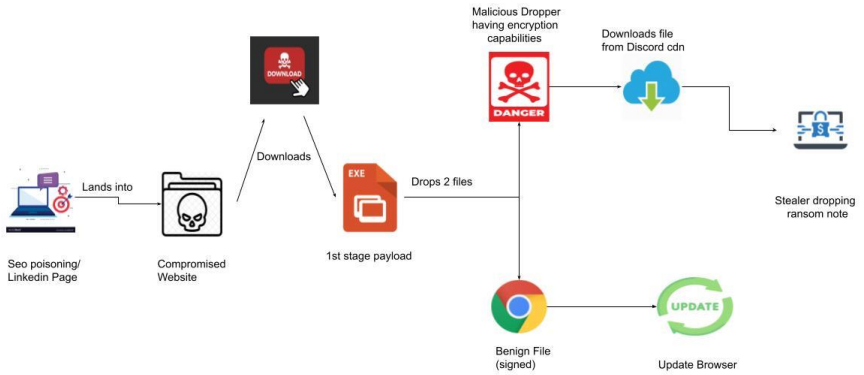


Tổng quan

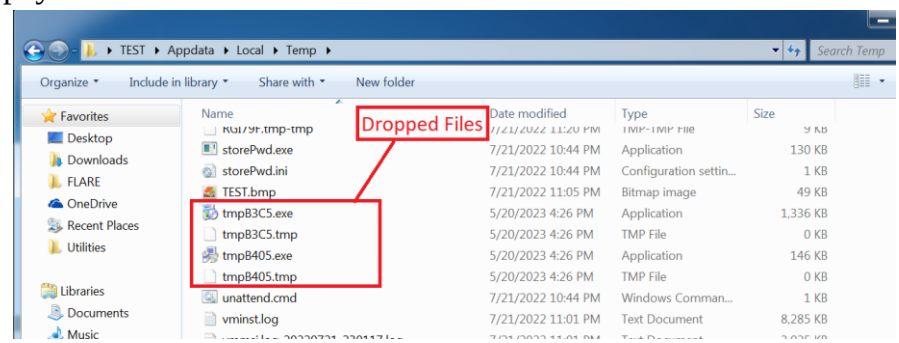
- Ransomware thực hiện UAC bypass (nâng cao đặc quyền) để chạy malware với quyền quản trị.
- Dữ liệu của người dùng bị khóa bằng AES và khóa AES được bảo vệ bằng mã hóa RSA.
- Một task được lên lịch để chạy locker mỗi 15 phút.
- Ransomware liệt kê và kết thúc các quy trình cụ thể đang chạy trên hệ thống mục tiêu. Một số dịch vụ được xóa để đảm bảo việc thực thi trôi chảy.
- Sử dụng ping scan để xác định các kết nối.
- Ransomware có khả năng khoá tệp trên cả local system và các connected system.

2.3. RedEnergy stealer

Mẫu biến thể Stealer-as-a-Ransomware này sử dụng chiến dịch FAKEUPDATES để lôi kéo nạn nhân, đánh lừa họ để nhanh chóng cập nhật browser. Khi đã vào hệ thống, biến thể độc hại này lén lấy thông tin nhạy cảm và sau đó mã hóa các tệp bị chiếm đoạt. Điều này khiến nạn nhân bị thiếu hụt dữ liệu, nguy cơ tiết lộ thông tin hoặc thậm chí bán dữ liệu.



1. Sau khi thực thi, tệp thực thi RedEnergy độc hại giả mạo như một phần của bản cập nhật trình duyệt hợp pháp,
2. Trong giai đoạn này, malware thả bốn tệp vào hệ thống của nạn nhân, trong %USERPROFILE%\AppData\Local\Temp. Các tệp này bao gồm hai tệp tạm thời và hai tệp thực thi, với tên tệp theo mẫu sau: tmp[4 ký tự thập lục phân ngẫu nhiên].exe. Trong số các tệp thực thi, một tệp đóng vai trò là malware payload, tệp còn lại giả mạo Google Update hợp pháp, được ký điện tử. Tệp thực thi giả mạo cập nhật thực hiện cập nhật thực tế của Google Chrome, từ đó tiếp tục đánh lừa nạn nhân. Đồng thời, malware thực thi một tiến trình nền khác, đóng vai trò malware payload.



Để đảm bảo malware vẫn hoạt động sau khi restart lại hệ thống, nó tạo một mục trong Start Menu\Programs\Startup.

Với các mô-đun ransomware được tích hợp vào payload, malware tiến hành mã hóa dữ liệu của người dùng, gắn thêm phần mở rộng ".FACKOFF!" cho mỗi tệp được mã hóa, và người dùng không thể truy cập đến khi có tiền chuộc. Hơn nữa, tệp thực thi độc hại sẽ thay đổi tệp desktop.ini, nhằm mục đích đánh lừa người dùng và cản trở việc phát hiện tác động của phần mềm độc hại lên hệ thống tệp.

2.4. Loki Password Stealer (PWS)

Loki Bot là một phần mềm độc hại phổ biến được bán trên các trang web ngầm, được thiết kế để đánh cắp dữ liệu riêng tư từ các máy bị nhiễm và sau đó gửi thông tin đó đến máy chủ ra lệnh và kiểm soát thông qua HTTP POST. Dữ liệu riêng tư này bao gồm mật

khẩu được lưu trữ, thông tin xác thực đăng nhập từ trình duyệt Web và nhiều loại ví tiền điện tử."

Loki-Bot sử dụng hàm băm để làm xáo trộn các thư viện được sử dụng.

Loki-Bot tạo một thư mục ẩn trong thư mục %APPDATA% có tên được cung cấp bởi các ký tự thứ 8 đến 13 của Mutex. Ví dụ: "%APPDATA%\ C98066\".

Có bốn tệp trong thư mục ẩn trong %APPDATA% : ".exe," ".lck," ".hdb" và ".kdb." Chúng sẽ được đặt tên theo các ký tự từ 13 đến 18 của Mutex. Ví dụ: "6B250D." Giải thích về mục đích của các tệp :

1. .exe Bản sao của phần mềm độc hại sẽ thực thi khi mỗi khi tài khoản người dùng đăng nhập vào
2. .lck Một tệp khóa được tạo khi giải mã Thông tin xác thực Windows hoặc Keylogging để ngăn xung đột tài nguyên
3. .hdb Cơ sở dữ liệu băm cho dữ liệu đã được lọc sang máy chủ C2
4. .kdb Cơ sở dữ liệu về dữ liệu keylogger chưa được gửi đến máy chủ C2

Nếu người dùng có đặc quyền, Loki-Bot sẽ thiết lập tính bền vững(persistence) trong registry theo HKEY_LOCAL_MACHINE. Nếu không, nó sẽ thiết lập tính bền vững(persistence) trong HKEY_CURRENT_USER.