# Giới thiệu về mã độc tống tiền WannaCry

* + 1. *Sự xuất hiện của WannaCry*

Tháng 5 năm 2017, một vụ khủng bố trên Internet với quy mô toàn cầu đã diễn ra. Tính tới ngày 15 tháng 5 (sau 3 ngày được biết đến) nó đã lây nhiễm và tác động lên hơn 230.000 máy tính trên hơn 150 quốc gia, gây nên một vụ tống tiền lịch sử trên mạng Internet. Nó xâm nhập, chặn đứng mọi tác vụ trên máy tính, kể cả những phần mềm diệt virus hàng đầu. 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…và có cả Tiếng Việt. Vụ tấn công đã làm ảnh hưởng lớn đến rất nhiều Tập đoàn và công ty trên toàn thế giới. Đó chính là mã độc tống tiền WannaCry.

*Hình 1-1. Màn hình thông báo trên máy tính bị nhiễm WannaCry*

* + 1. *Cách thức hoạt động của mã độc WannaCry*
* Luồng hoạt động: WannaCry đi theo cùng con đường tấn công vẫn thường thấy ở ransomware. WannaCry sẽ kiểm tra một "dấu mốc" (beacon), nếu dấu mốc này có trả về một phản hồi thì ransomware sẽ không chạy. Đây là cách để hacker kiểm soát được con ransomware của mình. Nếu beacon không có phản hồi gì cả thì ransomware bắt đầu công việc: nó khai thác lỗ hổng ETERNALBLUE/MS17-010 vì lỗ hổng này cho phép truy cập và có quyền ghi nên sẽ dễ lây lan sang các máy tính khác. WannaCry sau đó mã hóa các file trong hệ thống và cảnh báo cho người dùng rằng họ đã "dính đòn".

*Hình 1-2. Luồng thực thi của mã độc tống tiền WannaCry*

*Bảng 1-1. Cơ chế hoạt động của WannaCry*

| Bước 1 | Chạy file Exe, tức là người dùng "lỡ" bấm nhầm vào file thực thi để chạy ransomware lên. Để lừa người dùng chạy file này không khó, dụ họ mở một email nào đó hay chạy file tải về từ Torrent với những cái tên hấp dẫn là xong. Biến thể 2.0 của WannaCry còn có thể tự thực thi khi người dùng truy cập vào một trang web đã bị chèn mã độc. |
| --- | --- |
| Bước 2 | Kiểm tra beacon. Ransomware sẽ gọi một link như sau: hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. Nếu link này có trả về phản hồi, tức là hacker đã kiểm soát tên miền này1 và muốn ransomware dừng lại, thì file exe sẽ không chạy tiếp. Còn nếu không nhận được phản hồi, ransomware tiếp tục việc tấn công. Hacker chọn một tên miền rất vớ vẩn và không có ý nghĩa để không bị chú ý tới. |
| Bước 3 | WannaCry sẽ tận dụng lỗ hổng trong cơ chế SMB2. SMB là một giao thức truyền tải file của Windows và nó mặc định được bật trên cả Windows lẫn Windows Server nên cả máy PC hay server đều có thể bị dính. Malware dùng cơ chế này để lây lan sang các máy tính khác trong cùng mạng. Với người dùng cá nhân có thể không làm lây lan nhiều. Nhưng với các hệ thống IT doanh nghiệp vốn thường kết nối các máy với nhau thì ảnh hưởng là rất kinh khủng. |
| Các bước tiếp theo | WannaCry chuẩn bị một loạt thứ cho việc vận hành của mình, bao gồm tạo ra một dịch vụ chạy nền, chuẩn bị file Tor và file ví Bitcoin nhằm phục vụ cho việc giao dịch của nạn nhân với hacker. Nó cũng chuẩn bị một file key mã hóa dạng public key. Key này sẽ khớp với private key mà chỉ có hacker đang nắm giữ, cũng là chìa khóa để giải mã các file bị mã hóa. |



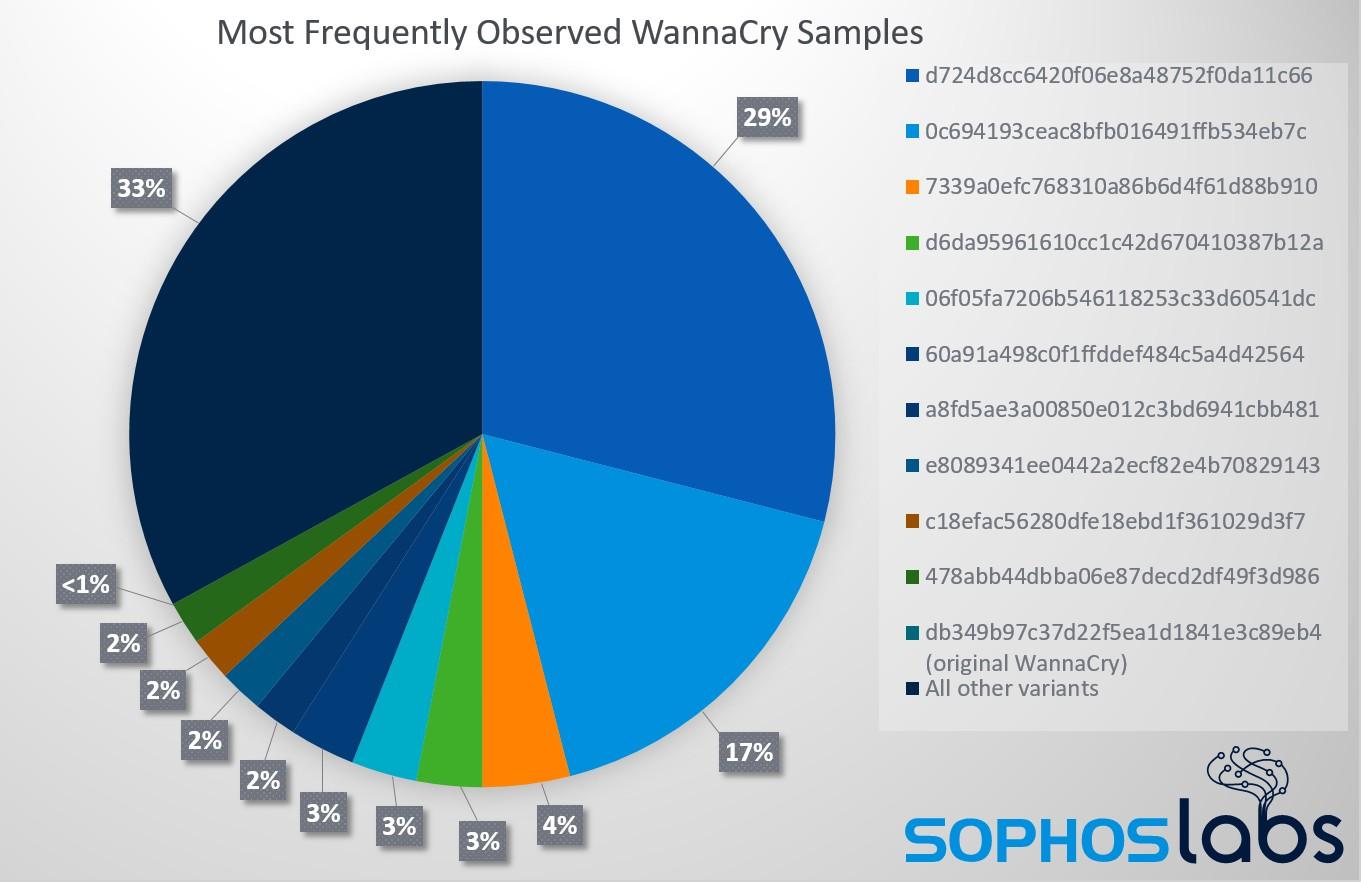
1 Liên quan đến tên miền này, có một nhà nghiên cứu sau khi xem xét mã nguồn của WCry đã phát hiện ra cơ chế beacon nói trên. Anh ta mua tên miền đó với mục tiêu nghiên cứu xem có bao nhiêu người đã bị dính, nhưng không nhờ đây lại là "kill switch" để tạm ngưng malware trong một thời gian. Sau đó anh này có cẩn thận cảnh báo rằng các biến thể mới sẽ xuất hiện bỏ qua bước kill switch này, và thực tế đã có những con ransomware như vậy ra đời sau vụ WannaCry

|  | Chuẩn bị xong, nó bắt đầu chạy tiến trình mã hóa hầu hết các file trong hệ thống, chủ yếu là file cá nhân và những file quan trọng với các phần mềm. Ransomware cũng như virus, nó cũng tự cho phép mình chạy lên cùng với Windows và tạo ra các bản backup.  Hacker cũng không quên tắt các process về cơ sở dữ liệu, cụ thể là SQL Server và MySQL, để những website, phần mềm nào đang kết nối với server sẽ không thể hoạt động được. |
| --- | --- |

2 Lỗ hổng bảo mật SMB này còn được biết tên gọi khác là EternalBlue, nó là một phần trong số các tool hacking của cơ qua an ninh Mỹ NSA đã bị lộ ra ngoài vào khoảng tháng trước bởi một nhóm hacker tự gọi mình là "The Shadow Brokers".

*- Các biến thể của WannaCry:*

Theo báo cáo của Tổ chức an ninh mạng Sophos, từ lúc xuất hiện đến nay, đã có hơn 12,000 file mã độc với các mã hash khác nhau trên toàn thế giới cố gắng thực hiện những hành vi tương tự với WannaCry. Tuy nhiên không phải tất cả file mã độc này đều thực hiện thành công.

Theo thống kê, hiện nay có khoảng 11 biến thể khác nhau của WannaCry được khai thác trong thực tế:

*Hình 1-3. Các biến thể phổ biến của WannaCry trong thực tế hiện nay*

* *Cơ chế mã hóa, giải mã dữ liệu của WannaCry:*

Sau khi ransomware WannaCry được kích hoạt, nó tự động tạo ra 1 cặp khóa AES, mã độc dùng khóa này để mã hóa toàn bộ những dữ liệu trong máy nạn nhân. Sau đó khóa đối xứng AES này lại được mã hóa bằng public key của RSA đi kèm với WannaCry. Kẻ tấn công là người nắm giữ khóa bí mật của RSA. Khi người dùng trả tiền chuộc và được cung cấp khóa bí mật của RSA, nó sẽ giúp giải mã ra khóa đối xứng AES. Từ khóa đối xứng AES sẽ có thể giải mã những tài liệu đã bị mã hóa trước đó.

* *Cơ chế đòi tiền chuộc của WannaCry:*

+ WannaCry sử dụng ví điện tử BitCoin để nhận tiền chuộc

+ Tạo cảnh báo đe dọa người dùng bằng nhiều ngôn ngữ khác nhau

+ Cung cấp bản giải mã thử để tạo lòng tin với nạn nhân

+ Cho đồng hồ đếm ngược hiện lên trong ô cảnh báo để đe dọa nạn nhân

* *Cơ chế xóa file khiến cho dữ liệu không thể khôi phục được:*

Khi mã hóa các tập tin của nạn nhân, Wannacry sẽ đọc từ tập tin gốc, mã hóa nội dung và lưu vào tập tin có đuôi “.WNCRYT”. Sau khi mã hóa, nó sẽ chuyển “.WNCRYT” thành “.WNCRY” và xóa tệp gốc. Logic xóa này có thể khác nhau tùy thuộc vào vị trí và thuộc tính của các tệp của nạn nhân.

Tuy nhiên 0các nhà nghiên cứu của Kaspersky [1)a)[2]](#_heading=h.3o7alnk) đã phân tích và ghi nhận một số lỗi logic của cơ chế xóa file do WannaCry thực hiện, theo đó người bị nhiễm mã độc vẫn có thể khôi phục một số tập tin bằng công cụ khôi phục dữ liệu.

*Bảng 1-2. Thống kê các trường hợp xử lý xóa file của WannaCry và khả năng khôi phục dữ liệu*

| Các tập tin nằm trên ổ đĩa hệ thống | Nếu tệp nằm trong thư mục 'quan trọng' (theo quan điểm của kẻ tấn công - ví dụ: Desktop và Document), thì tệp gốc sẽ bị ghi đè bằng dữ liệu ngẫu nhiên trước khi xóa. Trong trường hợp này, không có cách nào để khôi phục nội dung tệp gốc. |
| --- | --- |
| Nếu tệp được lưu trữ bên ngoài các thư mục 'quan trọng',  thì tệp gốc sẽ được chuyển đến **%TEMP%\% d.WNCRYT** (trong đó% d biểu thị một giá trị số). Các |

|  | tệp này chứa dữ liệu gốc và không bị ghi đè, chúng chỉ bị xóa khỏi đĩa, có nghĩa là có khả năng cao sẽ khôi phục chúng bằng phần mềm khôi phục dữ liệu. |
| --- | --- |
| Các tệp nằm trên các ổ đĩa (không phải hệ thống) khác | Ransomware tạo thư mục “$RECYCLE” và đặt các thuộc tính hệ thống ẩn cho thư mục này. Điều này làm cho thư mục này ẩn trong Windows File Explorer nếu nó có cấu hình mặc định. Phần mềm độc hại dự định di chuyển các tệp gốc vào thư mục này sau khi mã hóa.  Tuy nhiên, do lỗi đồng bộ hóa trong mã ransomware trong nhiều trường hợp, các tệp gốc vẫn nằm trong cùng một thư mục và không được chuyển vào $RECYCLE.  Các tệp gốc bị xóa theo cách không an toàn. Thực tế này làm cho nó có thể khôi phục các tệp đã xóa bằng cách sử dụng phần mềm khôi phục dữ liệu. |
| Các tệp có thuộc tính chỉ đọc (ReadOnly) | Nếu có các tệp như vậy trên máy bị nhiễm, thì ransomware sẽ không mã hóa chúng. Nó sẽ chỉ tạo một bản sao được mã hóa của mỗi tệp gốc, trong khi bản thân các tệp gốc chỉ nhận được thuộc tính “hidden”. Khi điều này xảy ra, vẫn có thể khôi phục các thuộc tính bình thường của chúng. |

* *Cách thức liên lạc với người bị hại*:

WannaCry hiện thông báo với đầy đủ thông tin về cách thức để trả tiền chuộc, thông tin về ví Bitcoin của kẻ tấn công, thậm chí là đường dẫn tài liệu giải thích cho nạn nhân hiểu thế nào là Bitcoin, thanh toán như thế nào. Điều này có thể thấy kẻ tấn công đã chuẩn bị rất kỹ cho cuộc tấn công này.

# Biện pháp phòng chống

Các chuyên gia đã khuyến nghị những phương pháp phòng tránh WannaCry và các cách chống Virus WannaCry như sau:

- Đối với cá nhân:

+ Sao lưu toàn bộ dữ liệu quan trọng của máy tính ra ổ cứng cá nhân, ổ cứng di động, link google drive, USB cùng những thiết bị lưu trữ dữ liệu khác để phòng tránh virus WannaCry tấn công các file dữ liệu quan trọng.

+ Luôn luôn dùng các hệ điều hành có bản quyền và update hệ điều hành lên các phiên bản mới nhất. Các máy đang dùng Windows 8.1 trở về trước cần cài lên Windows 10 hoặc cài bản update vá lỗi ngay.

+ Tắt (disable) tính năng SMB bằng cách vào “Start”, tìm “Windows Features”, xong bỏ dấu check chỗ SMB.

+ Cập nhật các chương trình antivirus đang sử dụng. Đối với các máy tính chưa có phần mềm antivirus cần tiến hành cài đặt và sử dụng ngay một phần mềm antivirus có bản quyền.

+ Cẩn trọng khi nhận được email có đính kèm và các đường dẫn lạ được gửi trong email, trên các mạng xã hội, công cụ chat….

+ Cần thận trọng khi mở các tệp tin đính kèm tệp ngay cả khi nhận được từ những địa chỉ quen thuộc. Sử dụng các công cụ kiểm tra phần mềm độc hại trực tuyến hoặc có bản quyền trên máy tính với các file này trước khi mở chúng.

+ Không mở các đường dẫn có đuôi .hta hoặc đường dẫn có cấu trúc không rõ ràng, các đường dẫn rút gọn.

+ Không truy cập những trang web đen, web không được khuyến nghị.

* Đối với các tổ chức, doanh nghiệp

+ Tiến hành nâng cấp toàn bộ máy chủ, máy trạm có sử dụng hệ điều hành Windows.

+ Cô lập với mạng LAN hệ thống khi 01 máy bị tấn công.

+ Tận dụng các giải pháp đảm bảo an toàn thông tin đang có sẵn trong tổ chức như Firewall, IDS/IPS, SIEM… để theo dõi, giám sát và bảo vệ hệ thống. Cập nhật các bản vá từ các hãng bảo mật đối với các giải pháp đang có sẵn.

# 2.Phân tích chi tiết



*Hình 3-7. Luồng thực thi của mã độc WannaCry*

A screenshot of a computer

Description automatically generated

1. Killswitch check

Đầu tiên, Wannacry tiến hành kết nối với 01 domain (killswitch\_url) có tên miền: “[http://ww.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com](http://ww.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/)”.

*Hình 3-8. Kiểm tra kết nối với domain (1) (tasksche.exe)*

Nếu kết nối thành công, mã độc sẽ chấm dứt thực thi. Ngược lại, nếu kết nối không thành công, mã độc sẽ bắt đầu thực thi các tính năng của nó.



*Hình 3-9. Thực thi sau khi kiểm tra kết nối (2) (2’) (tasksche.exe)*

1. Chạy mã độc (mssecsvc2.0.exe)

Sau khi kiểm tra Killswitch, mã độc chạy tiến trình mssecsvc2.0.exe để thực hiện việc duy trì (bằng cách tạo service), drop ra file tasksche.exe (từ resource) để thực hiện các tính năng khác của nó và lây lan cho các máy tính khác.

*Hình 3-10. Tạo và chạy service mssecsvc2.0 (3) (tasksche.exe)*

1. Extract ra file tasksche.exe từ resource (mssecsvc2.0.exe)

Mã độc tiến hành tìm và load resource của file mssecsvc2.0.exe. Sau đó, lấy dữ liệu từ resource và ghi vào file tasksche.exe.

*Hình 3-11. Xuất ra file tasksche.exe (WannaCry Installer) (3’) (tasksche.exe)*

1. Lây lan cho các máy tính khác (mssecsvc2.0 service)

Dropper thực hiện việc lây lan cho các máy tính khác trong cùng một mạng LAN (cùng subnet mask) và chọn ngẫu nhiên IP có kết nối với máy tính nạn nhân qua Internet bằng cách khai thác lỗ hổng MS17-010.



*Hình 3-12. : Khai thác MS17-010 để lây lan mã độc (4’) (tasksche.exe)*

1. Giải nén và chạy các thành phần còn lại của mã độc (tasksche.exe)

File tasksche.exe vừa được xuất từ mssecsvc2.0.exe tiến hành tạo service của chính nó để duy trì (persistent) và thực hiện việc giải nén và chạy các thành phần còn lại của mã độc.

A screenshot of a computer code

Description automatically generated

*Hình 3-13. WannaCry Installer tiến hành các thao tác để duy trì (4) (5) (6)*

*(tasksche.exe)*

File ZIP được lưu trữ bên trong resource có tên là “XIA” với password là “WNcry@2ol7”

*Hình 3-14. Mật khẩu để giải nén file ZIP (6)*



*Hình 3-15. Resource chứa file là XIA (6)*

Các file thu được khi unzip bao gồm:

+ b.wnry: file ảnh bitmap hiển thị hướng dẫn các bước để giải mã file;

+ c.wnry: file chứa các địa chỉ darkweb;

+ r.wnry: ransome note ở dạng text bản rõ;

**+ t.wnry:** file được mã hóa với header là “WANACRY!”;

+ s.wnry: file zip chứa các file thực thi và thư viện của Tor;

+ u.wnry: file PE, là thành phần thông báo đòi tiền chuộc và giải mã (@WanaDecryptor@.exe);

+ msg: chứa các file định dạng (RTF) chứa thông báo đòi tiền chuộc bằng các ngôn ngữ trong đó có Việt Nam;

+ taskdl.exe: công cụ xóa file;

+ taskse.exe: công cụ quản lý các phiên RDP.

Trong đó, file t.wnry là file thực hiện chức năng chính của mã độc là mã hóa file và đòi tiền chuộc.A screenshot of a computer

Description automatically generated

*Hình 3-16. Các file thu được sau khi unzip (6)*

Sau khi tất cả các file được giải nén, mã độc sẽ phân tích (parses) tệp cấu hình của C&C từ file **c.wnry** và lưu dữ liệu vào memory để sử dụng sau này.

*Hình 3-17. Đọc thông tin cấu hình C&C từ c.wnry*

Sau đó, mã độc tiến hành chọn ví Bitcoin và ghi nó vào file config. Bên cạnh các ID ví được thêm vào, cấu hình cũng chứa list các địa chỉ Tor .onion được sử dụng để giao tiếp với C&C và liên kết đến trình duyệt Tor chính thức (lấy từ file **c.wnry**).A screenshot of a computer program

Description automatically generated

*Hình 3-18. Chọn ví Bitcoin (1)*



*Hình 3-19. Chọn ví bitcoint (2)*

A computer code with green letters

Description automatically generated with medium confidence

*Hình 3-20. Danh sách ví bitcoin*

1. Mã hóa các tệp có thể trên máy tính

Ransomeware dll thực hiện chức năng mã hóa các tệp bị nhiễm trên máy tính. File dll nằm trong file **t.wnry** thu được khi unzip file lấy trong resource “XIA” của tasksche.exe. Tuy nhiên, file t.wnry đã bị mã hóa.

*- Tasksche.exe tiến hành giải mã file* ***t.wnry*** *để lấy file dll và thực thi nó*

Cơ chế mã hóa file **dll** thành file **t.wnry**: File dll ban đầu được mã hóa bằng thuật toán AES với 01 private key, sau đó mã độc tiến hành mã hóa private key đó bằng hard-coded và lưu trữ ở đầu file t.wnry.

Do vậy, tasksche.exe đã tiến hành giải mã file t.wnry như sau:

+ Trích xuất 1 trong các Public RSA key hard-coded trong data section.

+ Sử dụng hard-coded để giải mãi AES key được lưu trữ ở đầu t.wnry.

+ Sử dụng AES key để giải mã ra file dll. Kết quả thu được file kbdlv.dll.



*Hình 3-21.Tiến hành giải mã file t.wnry (tasksche.exe)*

+ Sau khi giải mã, ta thu được file **kbdlv.dll**, dll được tải trực tiếp vào memory và được gọi bằng cách gọi hàm TaskStart exported.

* *File* ***kbdlv.dll*** *scan các phiên RDP của máy tính để lây lan*



*Hình 3-22. Scan các phiên RDP (8.2)*

* *File* ***kbdlv.dll*** *tiến hành mã hóa dữ liệu*

+ Tạo 04 file config

00000000.res: file chứa thông tin của TOR/C2 00000000.pky: file chứa Public Key 00000000.eky: file chứa Encrypted Private Key 00000000.dky: file chứa Decryption Key

A close-up of a computer code

Description automatically generated

*Hình 3-23. Tạo các file config (kbdlv.dll)*

+ Tiến hành mã hóa các file trong máy tính:

Liệt kê tất cả ổ đĩa logic và xóa các file

%systemdrive%\$RECYCLE\hibsys.WNCRY trong tất cả ổ đĩa thuộc loại FIXED (cố định). Mã độc ghi đè tệp bằng các số 0 và đổi tên tệp thành \x99 trước khi xóa tệp khỏi đĩa.

Sau đó mã hóa các file có đuôi sau ở tất cả các thư mục:

.docx, .docb, .docm, .dot, .dotm, .dotx, .xls, .xlsx, .xlsm, .xlsb, .xlw, .xlt, .xlm,

.xlc, .xltx, .xltm, .ppt, .pptx, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .pst,

.ost, .msg, .eml, .edb, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2,

.snt, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC,

.PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .jpeg, .jpg,

.bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid,

.wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla,

.swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl,

.vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd,

.myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay,

.mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods,

.3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der

A screenshot of a computer program

Description automatically generated

*Hình 3-24. Tạo 05 thread và tiến hành mã hóa file*

A screenshot of a computer

Description automatically generated

*Hình 3-25. Danh sách đuôi file có thể bị mã hóa*

+ Tạo file m.vbs để tạo ra file shortcut của @WanaDecryptor@.exe



*Hình 3-26. Tiến hành tạo file m.vbs để tạo @WanaDecryptor@.exe shortcut (8.3)*

*(kbdlv.dll)*

Tiếp theo, DLL sẽ chấm dứt các process SQL, MS Exchange sau để dễ dàng mã hóa các tệp dữ liệu của chúng:

+ mysqld.exe

+ sqlwriter.exe

+ sqlserver.exe

+ MSExchange.\*

+ Microsoft.Exchange.\*

A computer screen shot of a computer code

Description automatically generated

*Hình 3-27. Tiến hành kết thúc một số process (8.4) (kbdlv.dll) (1)*

A screenshot of a computer code

Description automatically generated

*Hình 3-28. Tiến hành kết thúc một số process (8.4) (kbdlv.dll) (2)*

+ Tiến hành tạo thông báo đòi tiền chuộc trong thư mục cài đặt với tên “@Please\_Read\_Me@.txt”, shortcut trước đó được sao chép vào tất cả các thư mục bị ảnh hưởng bởi quá trình mã hóa cùng với bản sao của “@Please\_Read\_Me@.txt”. “@Please\_Read\_Me@.txt” được lưu **trong r.wnry**.



*Hình 3-29. Tạo và ghi vào file @Please\_Read\_Me@.exe*

Cuối cùng, DLL khởi động phiên bản Tor sử dụng để liên lạc giữa bên bị nhiễm và C&C bằng cách gọi TaskData \Tor \taskhsvc.exe.

A screenshot of a computer program

Description automatically generated

*Hình 3-30. Khởi động Tor bằng cách chạy taskhsvc.exe (8.6)*

Sau khi gọi Tor, DLL sẽ gọi giao diện người dùng ransomware

+ Khi giao diện người dùng lần đầu tiên mở ra, khoản thanh toán được yêu cầu là $300. Đúng với hầu hết Ransomware, nếu người dùng không thanh toán kịp thời - trong trường hợp này là 3 ngày - khoản thanh toán sẽ tăng lên $600.

Giao diện người dùng bao gồm các yếu tố sau:

+ Giới thiệu về Bitcoin - Mở https://en.wikipedia.org/wiki/Bitcoin trong trình duyệt mặc định.

+ Cách mua Bitcoin - Mở https://[www.google.com/search?q=how+to+buy+bitcoin](http://www.google.com/search?q=how%2Bto%2Bbuy%2Bbitcoin) trong trình duyệt mặc định.

+ Liên hệ với chúng tôi - Hiển thị hộp thông báo trong đó người dùng có thể nhập tin nhắn sẽ được gửi đến một địa chỉ email được chỉ định trong tệp cấu hình (nếu có). Cấu hình trong phiên bản gần đây của WannaCry không chứa bất kỳ địa chỉ email nào theo mặc định, nhưng có thể khách hàng có thể lấy một địa chỉ từ C&C sau đó.

+ Thanh toán bằng séc - Truy vấn máy chủ C&C để tìm khóa giải mã. Nếu thành công, C&C sẽ gửi khóa private được lưu dưới dạng 00000000.dky.

+ Giải mã - Kiểm tra xem có tệp 00000000.dky hay không. Nếu vậy, hãy sử dụng nó để giải mã các tệp, nếu không, hãy giải mã các tệp đã được chọn cho danh sách "giải mã thử nghiệm", được đọc từ tệp **f.wnry**.A screenshot of a computer

Description automatically generated

**C&C và Tor**

**1. Mã độc có sử dụng C&C để lây lan không?**

Mã độc k sử dụng C&C để lây lan. Mã độc lây lan bằng cách khai thác lỗ hổng MS17-010 (được tính là Zeroday tai thời điểm phát hiện). Địa chỉ IP của các máy tính được mã độc tạo ra bằng cách sinh ngẫu nhiên 4 octet rồi ghép lại thành IPv4

**2. Chức năng của tor**

Bộ trình duyện Tor được mã độc giải nén ra (lưu sẵn trong mã độc, KHÔNG PHẢI tải từ Internet). Tin tặc cung cấp bộ phần mềm này cho nạn nhân để nạn nhân có thể truy cập vào ví Bitcoin, trang web của tin tặc.

**3. Cách thức hoạt động của tor**

Tor Project là dự án phát triển một hệ thống mạng ngang hàng áp dụng mã hóa nhiều lớp dùng để né tránh sự giám sát của các ISP và chính quyền. "Phần mềm" Tor được đề câp bên trên thực chất là trình duyệt Mozilla đã được tinh giản lại và tích hợp giao thức Tor, tất cả các kết nối http và https đều được thực hiện sau khi máy tính gia nhâp Tor Network thành công.

**4. Bộ trình duyệt tor có phổ biến trên các loại rans mã hóa file không?**

Bản thân TOr là 1 phần mềm lành tính và bị lợi dụng để hướng dẫn người dùng cách chi trả bằng Bitcoin

Về mặt lý thuyết bất kì con mã độc nào có sử dụng các trang web host trên Tor node nào cũng có thể sẽ sử dụng Tor.

Tính năng mã hóa file được thực hiện bằng lập trình, không phải do sử dụng Tor.

**5. Mối liên hệ giữa C&C và Tor**

Nó sử dụng bộ Tor giải mã ra từ mã độc.

WannaCry dùng Tor để

- Gửi các tập tin có đuôi .res về máy chủ. Tập tin này chứa timestamp bắt đầu qúa trình mã hóa, thời điểm UI đe dọa được bật lên, và thời điểm các bản backup đã bị xóa thành công

- Cập nhật Wallet ID nếu có thay đổi