

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC
THÀNH PHỐ HỒ CHÍ MINH



ĐỀ TÀI MÔN
ĐIỀU TRA TẤN CÔNG

SV: Nguyễn Công Khang - 21DH110770

SV: Phạm Đức Thiên Phúc - 21DH112813

SV: Nguyễn Minh Đức – 21DH113591

GVGD: Th.S Phạm Đình Thắng

PHIẾU CHẤM ĐIỂM MÔN THI VẤN ĐÁP

Điểm phân trình bày – Điểm hệ 10

	CBCT1	CBCT2
Họ tên CBCT	<div>.....</div> <div>Chữ ký:</div>	<div>.....</div> <div>Chữ ký:</div>
Điểm	<div>.....</div> <div>Bằng chữ:</div>	<div>.....</div> <div>Bằng chữ:</div>
<div>Nhận xét</div> <div><div>• Báo cáo:2d</div><div>• Vấn đáp:2d</div><div>• Chức năng và demo :5d</div><div>• Mở rộng và ứng dụng thực tiễn:1d</div></div>	<div>Quyền báo cáo:(...) điểm...</div> <div>Vấn đáp :(...) điểm ...</div> <div>Chức năng :(...) điểm...</div> <div>Mở rộng :(...) điểm...</div> <div>.....</div> <div>.....</div> <div>.....</div> <div>.....</div>	<div>Quyền báo cáo:(...) điểm...</div> <div>Vấn đáp :(...) điểm ...</div> <div>Chức năng :(...) điểm...</div> <div>Mở rộng :(...) điểm...</div> <div>.....</div> <div>.....</div> <div>.....</div> <div>.....</div>

Điểm quá trình – Điểm hệ 10

Họ tên CBCT:

Điểm tổng kết:(Bằng chữ:.....)

Lời cảm ơn

*Trong thời gian học tập dưới mái trường Đại Học Ngoại Ngữ Tin Học Thành Phố Hồ Chí Minh, được sự truyền đạt kiến thức và giúp đỡ tận tình của quý Thầy Cô Giảng viên là hành trang quý báu cho sự nhận thức và hiểu biết của em ngày hôm nay. Em xin ghi nhận nơi này lòng biết ơn chân thành nhất đối với tất cả các Thầy Cô Giảng viên và đặc biệt là thạc sĩ **Phạm Đình Thắng**, giảng viên chuyên ngành Điều tra tấn công, người thầy đã tận tình hướng dẫn em hoàn thành bài báo cáo tốt nghiệp này. Do kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ cũng chưa hoàn hảo nên bài báo cáo sẽ còn nhiều thiếu sót, kính mong sự góp ý và giúp đỡ từ Quý Thầy cô. Một lần nữa, em xin chân thành cảm ơn!*

Lý do chọn đề tài

Hiện nay, công nghệ kỹ thuật càng hiện đại kéo theo đó là những thành phần luôn muốn tấn công nhắm vào những công ty nhằm đánh cắp thông tin phục vụ cho mục đích xấu và loại mã độc tiêu biểu cho những vụ tấn công đó là IcedID

- **Nguy cơ An ninh Thông tin:** IcedID là một mối đe dọa nghiêm trọng đối với an ninh thông tin. Nắm vững về nó giúp bạn hiểu rõ về cách mà những loại malware này tấn công hệ thống và làm thế nào chúng có thể được ngăn chặn.
- **Phân tích Mã độc hại:** Nghiên cứu IcedID cung cấp cơ hội để phân tích mã độc hại, từ đó bạn có thể hiểu được cách chúng hoạt động và cách chúng thay đổi để tránh phát hiện.
- **Bảo vệ Hệ thống:** Hiểu biết sâu rộng về IcedID giúp bạn xây dựng biện pháp bảo mật hiệu quả hơn để ngăn chặn sự xâm nhập của nó và bảo vệ hệ thống của bạn khỏi những mối đe dọa tương tự.
- **Nghiên cứu An ninh Mạng:** Nắm vững về IcedID có thể cung cấp thông tin quan trọng về các chiến thuật tấn công, kỹ thuật thâm nhập và mô hình hoạt động của các nhóm tội phạm mạng.

MỤC LỤC

Nội dung

Lời cảm ơn	3
Lý do chọn đề tài	4
Chương 1: Tìm hiểu về Malware.....	6
I. Malware là gì	6
II. Có bao nhiêu loại malware	6
Chương 2: Tìm hiểu về IcedID	7
I. Giới thiệu về IcedID	7
II. Phương thức hoạt động.....	7
III. Dấu hiệu của một cuộc tấn công	9
IV. Cách ngăn chặn	9
V. Những biến thể vừa được phát hiện	10
Chương 3: Báo cáo đồ án	12
I. Phân tích file giải nén.....	12
II. Tiến hành điều tra gói tin bằng Wireshark	17
III. Kết luận	23
TÀI LIỆU THAM KHẢO	24

Chương 1: Tìm hiểu về Malware

I. Malware là gì

Malware (viết tắt của malicious software) là một thuật ngữ chung được sử dụng để mô tả bất kỳ phần mềm nào được thiết kế để gây hại hoặc xâm phạm máy tính, hệ thống máy tính, mạng hoặc người dùng mà không được sự cho phép của họ. Malware có thể thực hiện nhiều loại hoạt động độc hại, bao gồm việc gây mất dữ liệu, hủy hoại hệ thống, đánh cắp thông tin cá nhân, hoặc thậm chí kiểm soát máy tính từ xa.

II. Có bao nhiêu loại malware

- **Virus**: Là một loại malware có khả năng tự nhân bản và lây nhiễm các tập tin khác trên hệ thống.
- **Worm**: Tương tự như virus, nhưng khác ở chỗ worm không cần gắn kết vào một tập tin tồn tại và có thể tự lan truyền qua mạng.
- **Trojan horse (Trojan)**: Là một phần mềm độc hại được che giấu dưới hình thức một ứng dụng hữu ích hoặc không đáng ngờ để lừa đảo người sử dụng.
- **Spyware**: Theo dõi và thu thập thông tin về hoạt động của người sử dụng mà không được sự cho phép.
- **Ransomware**: Mã hóa dữ liệu trên hệ thống và yêu cầu người dùng trả tiền (khoản tiền chuộc) để giải mã.
- **Adware**: Hiện thị quảng cáo không mong muốn để thu hút người sử dụng vào việc nhấp vào chúng, thường đi kèm với một số hình thức thu thập thông tin cá nhân.
- **Botnet**: Sử dụng một mạng các máy tính bị nhiễm malware để thực hiện các hành động không đồng thuận, thường làm mục tiêu tấn công mạng lớn.

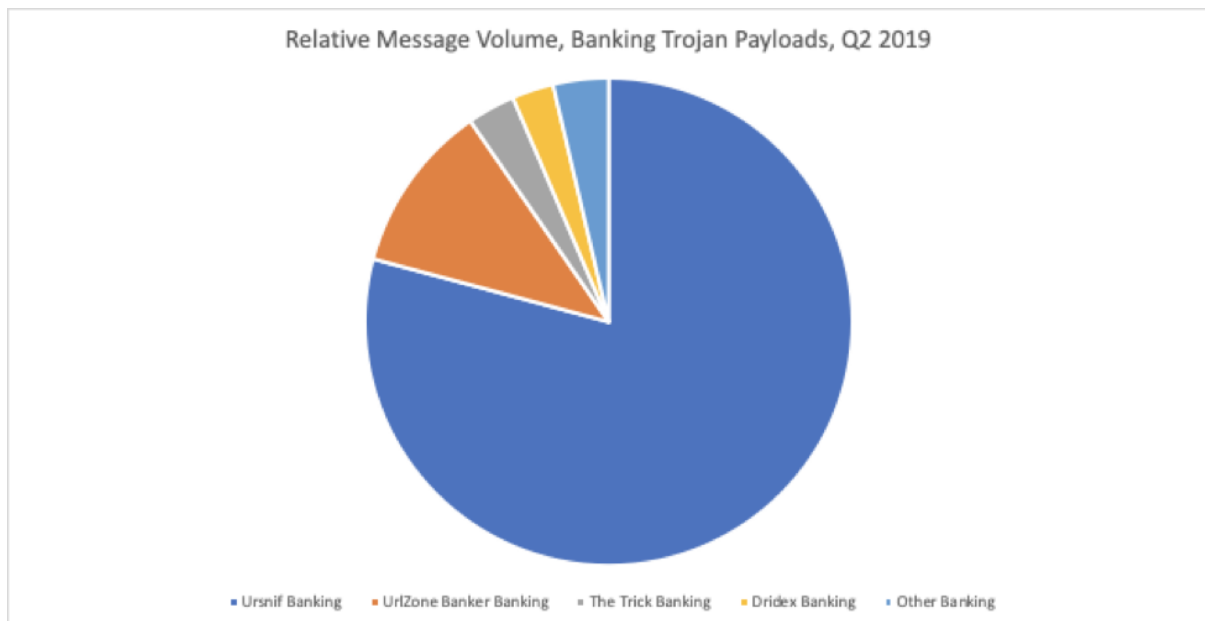
Để bảo vệ máy tính và thông tin cá nhân, người sử dụng thường cần cài đặt phần mềm chống malware và duy trì các biện pháp an ninh mạng.

Chương 2: Tìm hiểu về IcedID

I. Giới thiệu về IcedID

IcedID (còn được biết đến với tên gọi BokBot) là một dạng malware khá mới được phát hiện lần đầu vào năm 2017, được phân loại là một loại Trojan ngân hàng và Trojan truy cập từ xa (RAT). Nó được coi là có khả năng tương đương với các Trojan ngân hàng phức tạp khác như Zeus, Gozi và Dridex. IcedID là một loại malware giai đoạn thứ hai phụ thuộc vào các loại malware giai đoạn đầu tiên khác, như Emotet, để có quyền truy cập ban đầu và triển khai nó. Ngoài việc đánh cắp thông tin tài chính của nạn nhân, IcedID thường được sử dụng như một công cụ triển khai cho các loại malware giai đoạn thứ hai khác, bao gồm ransomware, và có khả năng tiên tiến để di chuyển qua mạng.

IcedID chủ yếu được sử dụng bởi các nhóm đe dọa Shatak (còn được biết đến với tên gọi TA551) cho dịch vụ tội phạm của họ dưới dạng MaaS (malware as a service). Các lây nhiễm của IcedID thường được cài đặt bởi malware giai đoạn đầu tiên nổi tiếng Emotet hoặc bởi một trong những mạng lưới bot malspam lớn nhất thế giới, botnet malspam Cutwail. Mặc dù không được liệt kê trong top mười loại malware của CISA cho năm 2021, IcedID được coi là một mối đe dọa tiên tiến thường xuyên được cập nhật với các kỹ thuật lạc quan và tiên tiến.



II. Phương thức hoạt động

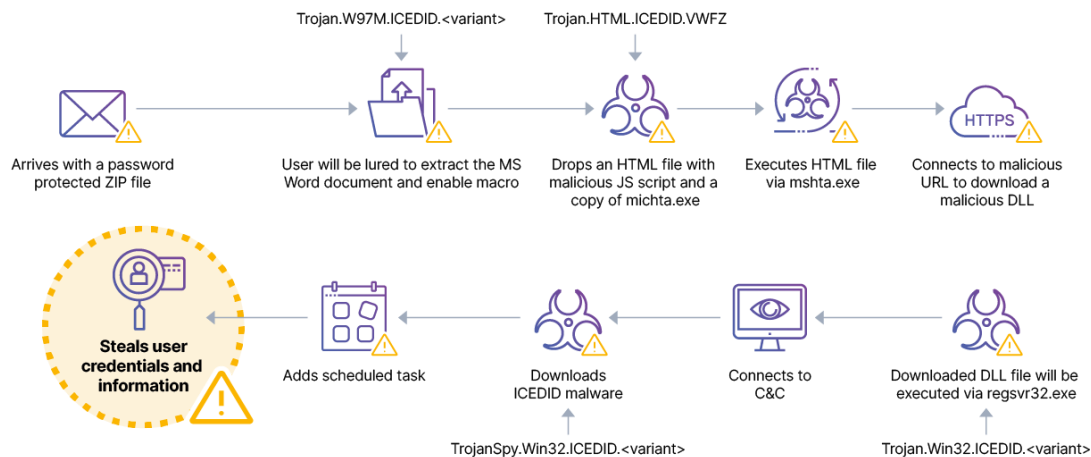
Nhóm đe dọa Shatak thường sử dụng email lừa đảo để phổ biến IcedID thông qua các tệp đính kèm tài liệu Microsoft Office chứa macro, tệp .iso hoặc các tệp nén .zip được mã hóa. Sau khi bị nhiễm, bảng tải ban đầu của IcedID liệt kê hệ thống máy chủ mục tiêu để xác định con đường nhiễm hiệu quả nhất. Bảng tải ban đầu

tìm kiếm một điểm tiêm ẩn để tự cài đặt với sự kiên nhẫn và đợi đến khi hệ thống khởi động lại trước khi khởi động mô-đun chính của nó. Bằng cách chờ đợi khi hệ thống khởi động lại, IcedID đảm bảo một mức độ ẩn nhiều hơn, xuất hiện như một quy trình hợp lệ mỗi khi hệ thống khởi động lại.

IcedID sử dụng kết hợp các kỹ thuật ở giai đoạn thứ hai, bao gồm:

- Sử dụng phương pháp "living off the land" (LOTL) để thu thập thông tin về hệ thống mục tiêu bằng cách sử dụng các công cụ nguyên bản của Windows
- Tận dụng tiện ích Windows Management Instrumentation (WMI) để phát hiện phần mềm chống virus và các phần mềm bảo mật khác đã cài đặt trên hệ thống mục tiêu và điều chỉnh chiến lược của mình để tăng khả năng thành công
- Lạm dụng tính năng WMI trong Windows để tương tác với các hệ thống cục bộ hoặc từ xa để khám phá và di chuyển theo chiều ngang qua các chia sẻ tệp trong Active Directory (AD)
- Sử dụng nhiều phương pháp tiêm để chiếm đoạt các ứng dụng hợp lệ để tránh bị phát hiện
- Thiết lập kiên nhẫn thông qua nhiều phương pháp, bao gồm công việc được lên lịch và Ru
- Kết nối với một số chức năng Interface ứng dụng (API) để tiêm chính nó vào các thư viện động hệ thống hiện tại (DLL)
- Nhập các dạng malware khác, bao gồm ransomware và các công cụ hack như Cobalt Strike
- Nhập các tệp DLL được đóng gói và được làm mờ cao mức có thể được thực thi thay vì các tệp DLL của Windows gốc trong một kỹ thuật được biết đến là "DLL hijacking"
- Lưu trữ các tệp cấu hình và bảng tải của mình dưới dạng "blobs" được mã hóa và sử dụng các loại tệp khác như PNG hoặc ICO để che giấu bảng tải
- Tiêm lệnh vào quy trình Cài đặt Windows (msiexec.exe) để che giấu việc thực thi lệnh của mình như một ứng dụng MSI điển hình

Khả năng đánh cắp của IcedID sử dụng một cuộc tấn công chèn web "man-in-the-browser" rất hiệu quả để lây nhiễm vào các ứng dụng trình duyệt lớn, cho phép kẻ tấn công xem hoạt động trực tuyến của nạn nhân, đánh cắp thông tin đăng nhập trực tiếp hoặc chuyển hướng yêu cầu tải trang của nạn nhân đến các trang web độc hại giả mạo như các ứng dụng ngân hàng trực tuyến và tài chính trực tuyến phổ biến. Điều này hiệu quả lừa đảo nạn nhân của IcedID để cung cấp thông tin đăng nhập ngân hàng trực tuyến, sau đó được sử dụng để thực hiện giao dịch gian lận.



III. Dấu hiệu của một cuộc tấn công

Như hầu hết các loại malware, việc phát hiện một cuộc tấn công hiệu quả nhất là thông qua sự nhận thức sắc bén về các chiến thuật kỹ thuật xã hội thông thường, đặc biệt là các kỹ thuật lừa đảo và malspam. Mặc dù các quy tắc YARA, chữ ký malware và phân tích lưu lượng mạng có thể hỗ trợ trong việc phát hiện sau khi bị nhiễm của các phiên bản đã biết của IcedID, nhưng những người phát triển thường xuyên cập nhật malware bằng các phương pháp mới và cải tiến để duy trì sự kiên nhẫn và tránh né, làm cho việc phát hiện một nhiễm IcedID một cách đáng tin cậy mà không cần sản phẩm bảo vệ điểm cuối tiên tiến trở nên khó khăn.

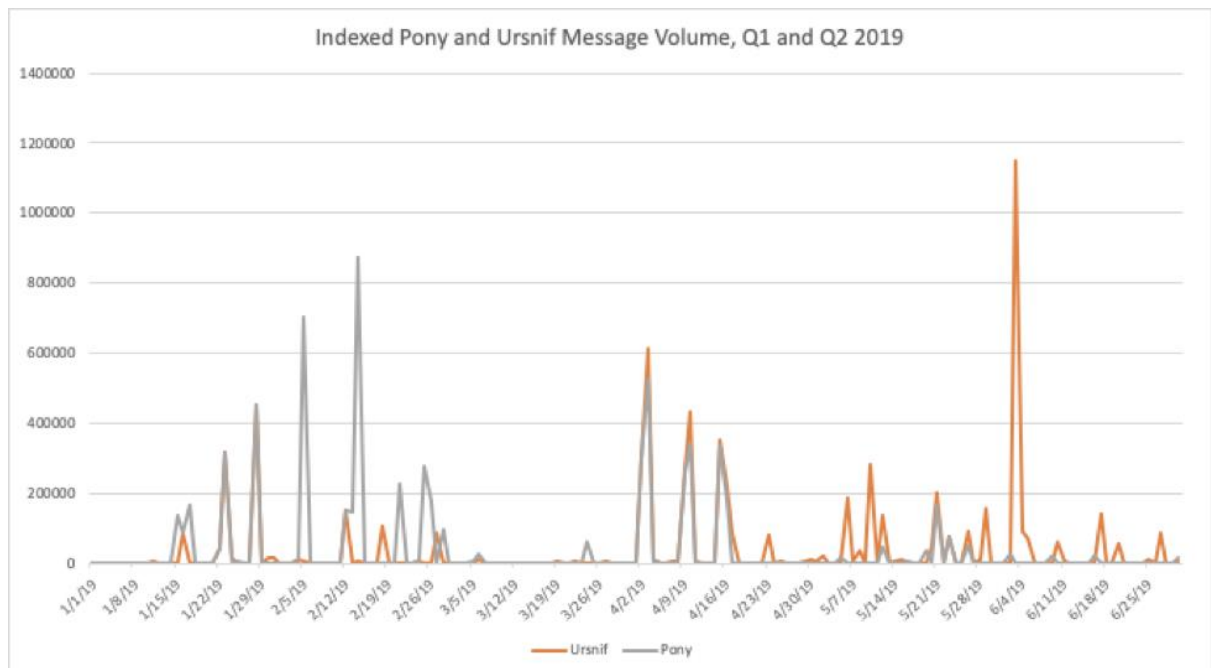
IV. Cách ngăn chặn

IcedID là một dạng malware phát triển nhanh chóng, và những người phát triển liên tục tìm kiếm các kỹ thuật tấn công mới để cải thiện sự ẩn danh và khả năng tránh né của IcedID. Một chương trình an toàn thông tin toàn diện cấp doanh nghiệp mang lại đảm bảo tốt nhất chống lại mối đe dọa như vậy. Một tổ chức có thể giảm thiểu khả năng trở thành nạn nhân của IcedID bằng cách thực hiện các biện pháp phòng ngừa thích hợp.

Dưới đây là những cách hiệu quả nhất để bảo vệ chống lại cuộc tấn công của IcedID:

- Cài đặt và cấu hình các sản phẩm bảo mật điểm cuối có khả năng quét tài liệu được mã hóa ngay sau khi chúng được giải mã.
- Triển khai các giải pháp Zero Trust mỗi khi có thể, ưu tiên cho các hệ thống quan trọng.
- Thực hiện quét lỗ hổng đều đặn và kiểm thử xâm nhập trên tất cả cơ sở hạ tầng mạng và khắc phục mọi lỗ hổng được phát hiện càng sớm càng tốt.

- Bắt buộc xác minh đa yếu tố cho tất cả các dịch vụ quan trọng, đặc biệt là tài khoản ngân hàng trực tuyến và tài khoản tiền điện tử.
- Nhận thức về rủi ro tăng cao mà các tệp được mã hóa mang lại và xác minh bối cảnh của các tài liệu như vậy một cách cẩn thận trước khi mở chúng.
- Đảm bảo rằng các ứng dụng Office được cấu hình với các thiết lập "Tắt tất cả các macro mà không cần thông báo" hoặc "Tắt tất cả ngoại trừ macro đã được ký số".
- Đảm bảo rằng chỉ có phần mềm được ủy quyền và có chữ ký số được cài đặt trên tất cả các điểm cuối và định kỳ quét và chặn bất kỳ phần mềm không được ủy quyền nào khỏi thực thi.
- Sử dụng proxy nội dung để theo dõi việc sử dụng internet và hạn chế quyền truy cập của người dùng đến các trang web đáng ngờ hoặc rủi ro.
- Xem xét việc đào tạo nhân viên về nhận thức về phishing và phát triển các quy trình hoạt động tiêu chuẩn (SOP) để xử lý email và tài liệu đáng ngờ.



V. Những biến thể vừa được phát hiện

Các nhà nghiên cứu của Proofpoint lần đầu tiên đã quan sát và ghi lại ba biến thể riêng biệt của phần mềm độc hại được gọi là IcedID. Proofpoint gọi hai biến thể mới được xác định gần đây là “Forked” và “Lite” IcedID. Báo cáo này nêu chi tiết các biến thể sau của IcedID:

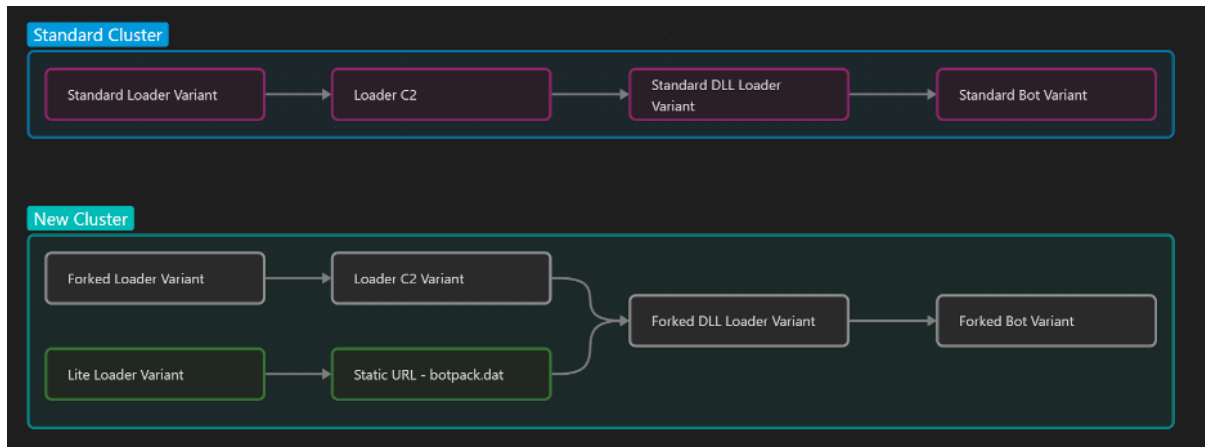
- Standard IcedID Variant: Biến thể được quan sát phổ biến nhất trong bối cảnh môi đe dọa và được sử dụng bởi nhiều tác nhân đe dọa.

- Lite IcedID Variant: Biến thể mới được quan sát là tải trọng tiếp theo vào tháng 11. Các trường hợp lây nhiễm Emotet không lọc dữ liệu máy chủ trong quá trình đăng ký của trình tải và một bot có chức năng tối thiểu.
- Forked IcedID Variant: Biến thể mới được các nhà nghiên cứu Proofpoint quan sát vào tháng 2 năm 2023 được sử dụng bởi một số ít tác nhân đe dọa, biến thể này cũng cung cấp cho bot chức năng tối thiểu.

Vào tháng 11 năm 2022, các nhà nghiên cứu của Proofpoint đã quan sát thấy biến thể mới đầu tiên của IcedID Proofpoint có tên là “IcedID Lite” được phân phối dưới dạng tải trọng tiếp theo trong chiến dịch TA542 Emotet. Nó đã bị phần mềm độc hại Emotet loại bỏ ngay sau khi nam diễn viên quay trở lại lĩnh vực tội phạm điện tử sau gần 4 tháng tạm nghỉ.

Trình tải IcedID Lite được quan sát vào tháng 11 năm 2022 chứa một URL tĩnh để tải xuống tệp “Bot Pack” có tên tĩnh (botpack.dat), dẫn đến Trình tải DLL IcedID Lite, sau đó cung cấp phiên bản Forked của IcedID Bot, bỏ đi chức năng webinjects và backconnect thường được sử dụng để lừa đảo ngân hàng.

Bắt đầu từ tháng 2 năm 2023, Proofpoint đã quan sát thấy biến thể Forked mới của IcedID. Cho đến nay, Proofpoint đã phát hiện ra bảy chiến dịch sử dụng biến thể Forked IcedID. Biến thể này được phân phối bởi TA581 và một cụm hoạt động đe dọa chưa được phân bổ, đóng vai trò hỗ trợ truy cập ban đầu. Các chiến dịch đã sử dụng nhiều loại tệp đính kèm email, chẳng hạn như tệp đính kèm Microsoft OneNote và các tệp đính kèm .URL hơi hiếm thấy, dẫn đến biến thể Forked của IcedID.








Trình tải phân nhánh IcedID, được quan sát lần đầu tiên vào tháng 2 năm 2023, giống với Trình tải IcedID tiêu chuẩn hơn ở chỗ nó liên hệ với máy chủ Loader C2 để truy xuất trình tải DLL và bot. Trình tải DLL đó có các thành phần tương tự như Trình tải Lite và cũng tải Bot Forked IcedID.

Hình ảnh sau đây hiển thị tổng quan cấp cao về các biến thể IcedID khác nhau mà các nhà nghiên cứu Proofpoint đã xác định.

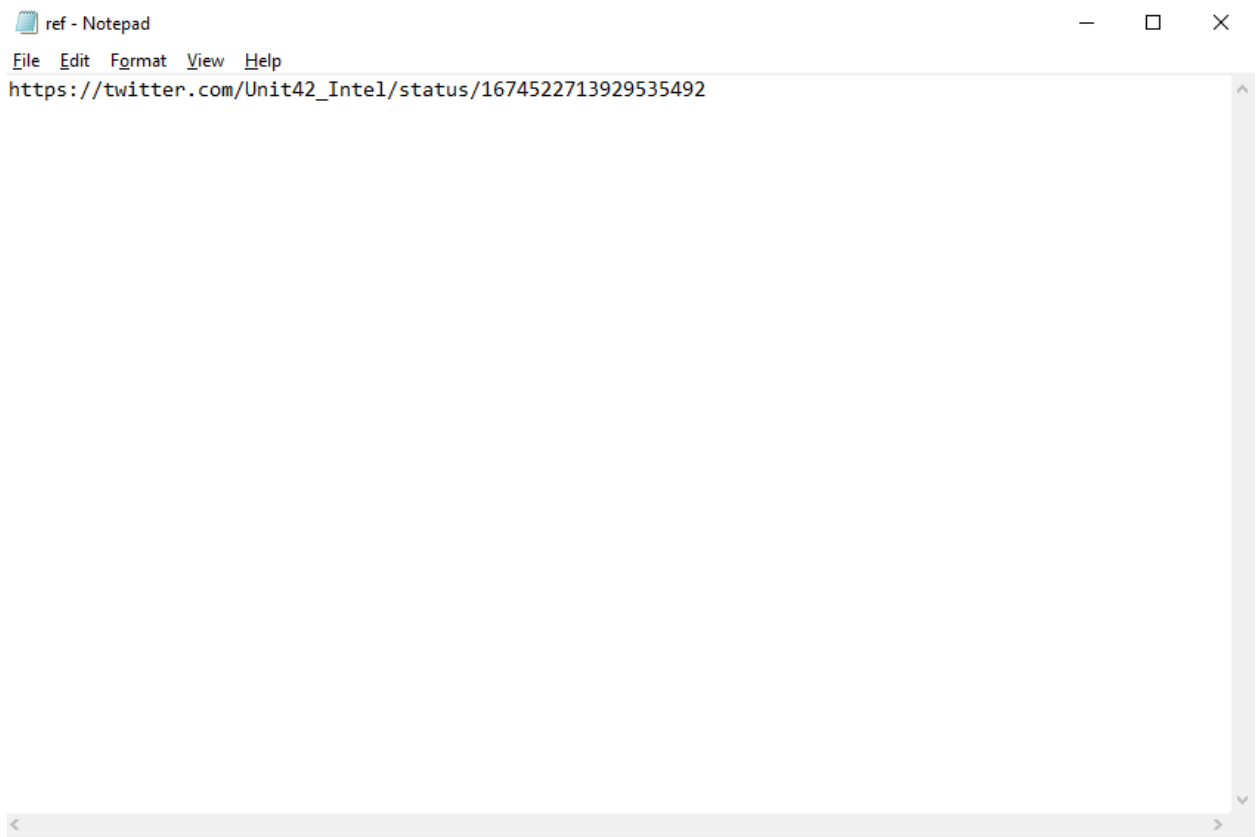
Chương 3: Báo cáo đồ án

I. Phân tích file giải nén

Sau khi ta tải và giải nén source thì ta sẽ được các file sau

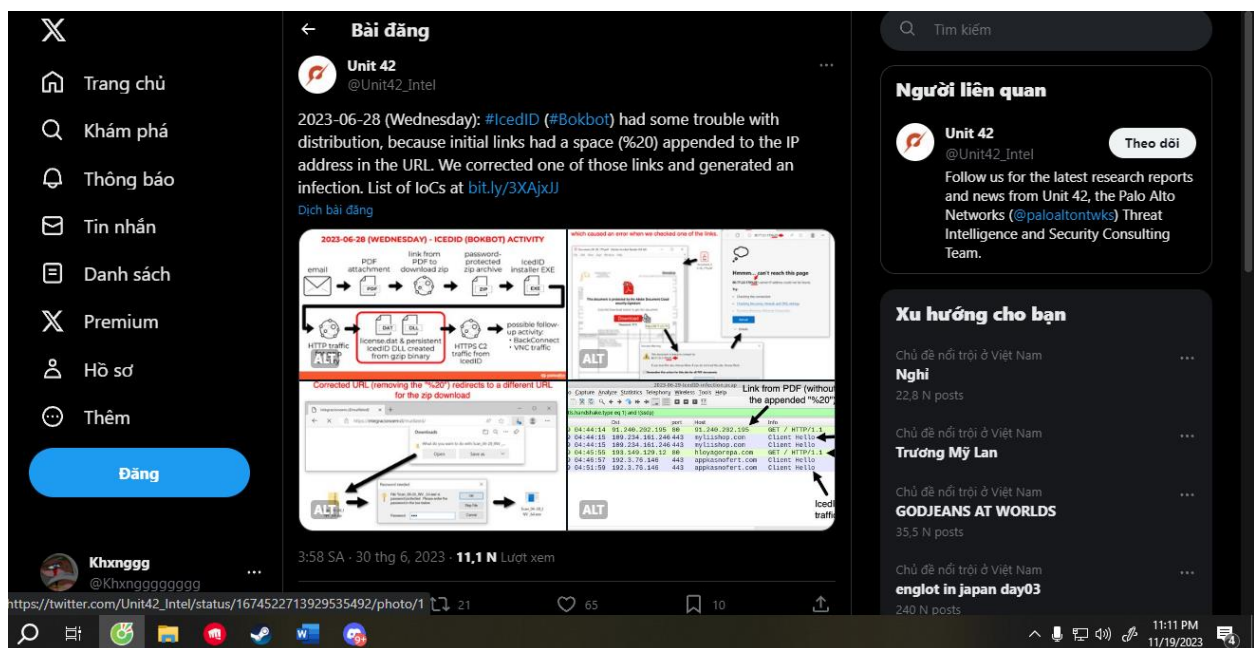
name	Date modified	type	size
 2023-06-28-IOCs-for-IcedID-activity	6/30/2023 3:22 AM	Text Document	5 KB
 2023-06-28-IOCs-for-IcedID-activity.txt	10/25/2023 6:33 PM	WinRAR ZIP archive	3 KB
 2023-06-29-IcedID-infection	6/29/2023 12:05 PM	Wireshark capture...	3,017 KB
 2023-06-29-IcedID-infection.pcap	10/25/2023 6:33 PM	WinRAR ZIP archive	2,899 KB
 ref	10/25/2023 6:42 PM	Text Document	1 KB

Hãy đến với file đầu tiên là file ref



File ref cho ta 1 link twitter dẫn đến vụ tấn công gần nhất của Icedid(Bokbot) vào Thứ 4 ngày 28-6-2023 kèm theo đó 1 đường link dẫn đến 1 file txt nói về

hoạt động của Icedid(Bokbot) cũng chính là file activity.txt mà ta đã giải nén ra trong source



Đầu tiên thì chúng ta biết được infection chain hay còn gọi là chuỗi lây nhiễm của Icedid(bokbot) được thực hiện như thế nào :

1. Email: Sự lây nhiễm bắt đầu từ một email độc hại.
2. Tập PDF Đính Kèm: Email chứa một tập PDF đính kèm.

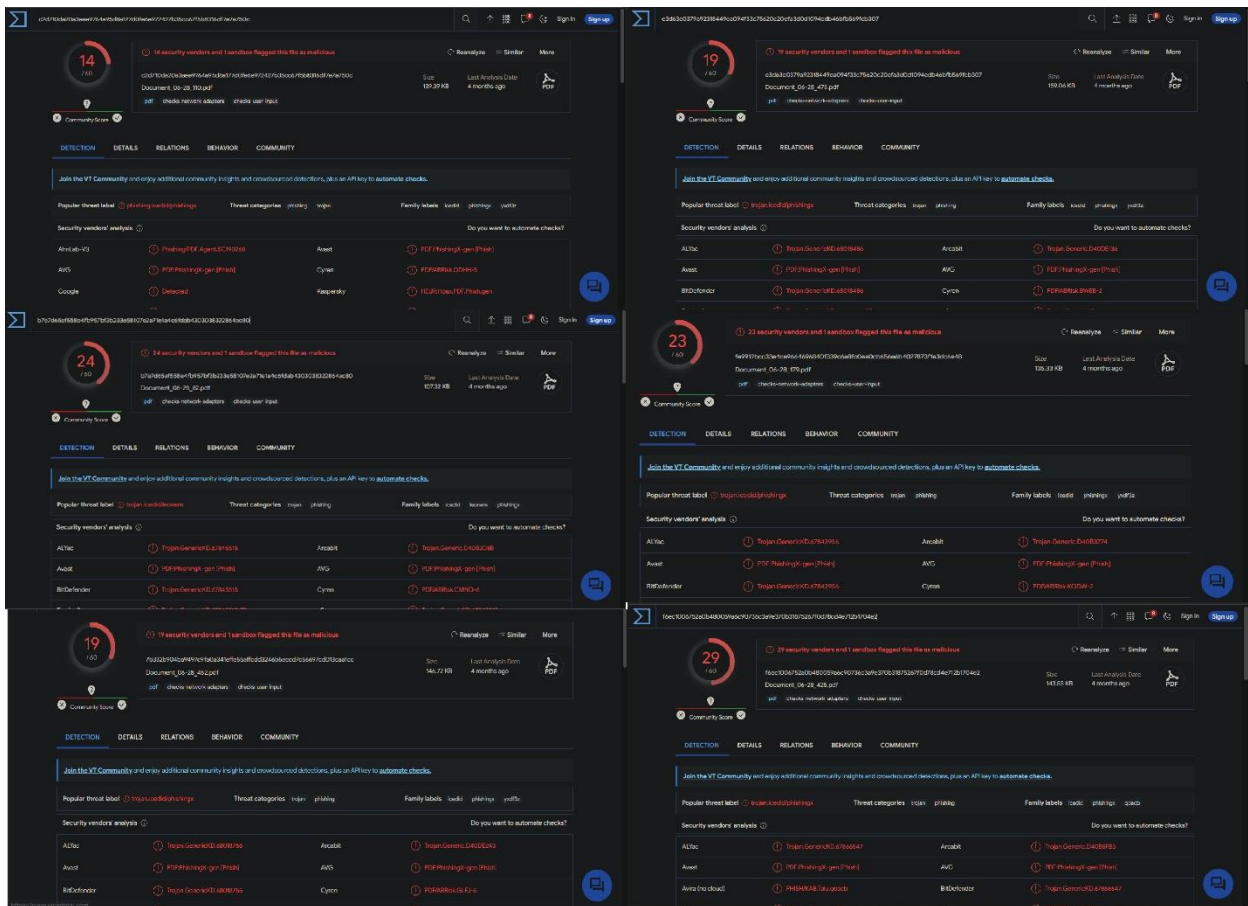
3. Liên kết từ PDF: Tập PDF chứa các liên kết dẫn đến giai đoạn tiếp theo.
4. TDS Redirect: Có một chuyển hướng thông qua Hệ thống Phân phối Luồng (TDS).
5. Bảo vệ Bằng Mật khẩu ZIP: Chuyển hướng của TDS dẫn đến một file ZIP được bảo vệ bằng mật khẩu.
6. Bộ Cài Đặt EXE cho IcedID: Bên trong file ZIP là bộ cài đặt EXE cho mã độc IcedID.
7. Gzip Binary: Sau đó là một tệp nhị phân gzip.
8. Nhiễm IcedID: Việc cài đặt EXE thiết lập sự nhiễm IcedID khôn ngoan và kiên trì.
9. IcedID C2: Kết nối với máy chủ-trạm kiểm soát (C2) của IcedID.

Đến với thông tin đầu tiên đó là file pdf được gửi đến email của nạn nhân (phishing), ta có được thông tin cơ bản của chúng như là tên file mã hash

8 EXAMPLES OF PDF FILES:

```
- b7e7d65af558e4fb957bf3b233e58107e2a71e1a4c6fdab4303038322864ac80 - 109,894 bytes - Document_06-28_82.pdf
- c2d710da20a3aee9764a95d8a177d0fe6e972427b35cc67f5b8316df7e7a750c - 142,732 bytes - Document_06-28_110.pdf
- fe9912bcc33e4ce9664696840f339c6a8fc0ea0cb656e6b4027873f1e3dc6e48 - 138,578 bytes - Document_06-28_179.pdf
- f261d118e2c1087ad250b475473c08758ad229e1265d8c214585a6679dd5df71 - 139,813 bytes - Document_06-28_250.pdf
- f6ec1006752a0b480059a6c90736c3a9e370b31875267f0d78cd4e712b1704e2 - 146,995 bytes - Document_06-28_425.pdf
- 7b332b904ba9497c9fa0a341effe55affcdd3246b5eccd7c56697cd013caa1cc - 150,237 bytes - Document_06-28_452.pdf
- e3d63e0379a92318449ea094f33c75620c20efa3d0d1094edb46bfb569fcb307 - 162,880 bytes - Document_06-28_475.pdf
- f36309b19948c880c13b30a6db56d14dd65c9d1c45cdf5ade274e5c568192f7 - 122,209 bytes - Document_06-28_494.pdf
```

Hãy đem mã hash của chúng lên Virustotal và phân tích. Sau khi phân tích 6/8 file thì cho thấy chúng đều có bao gồm mã độc và trojan gây hại đến người dung và đều liên quan đến phishing và Icedid

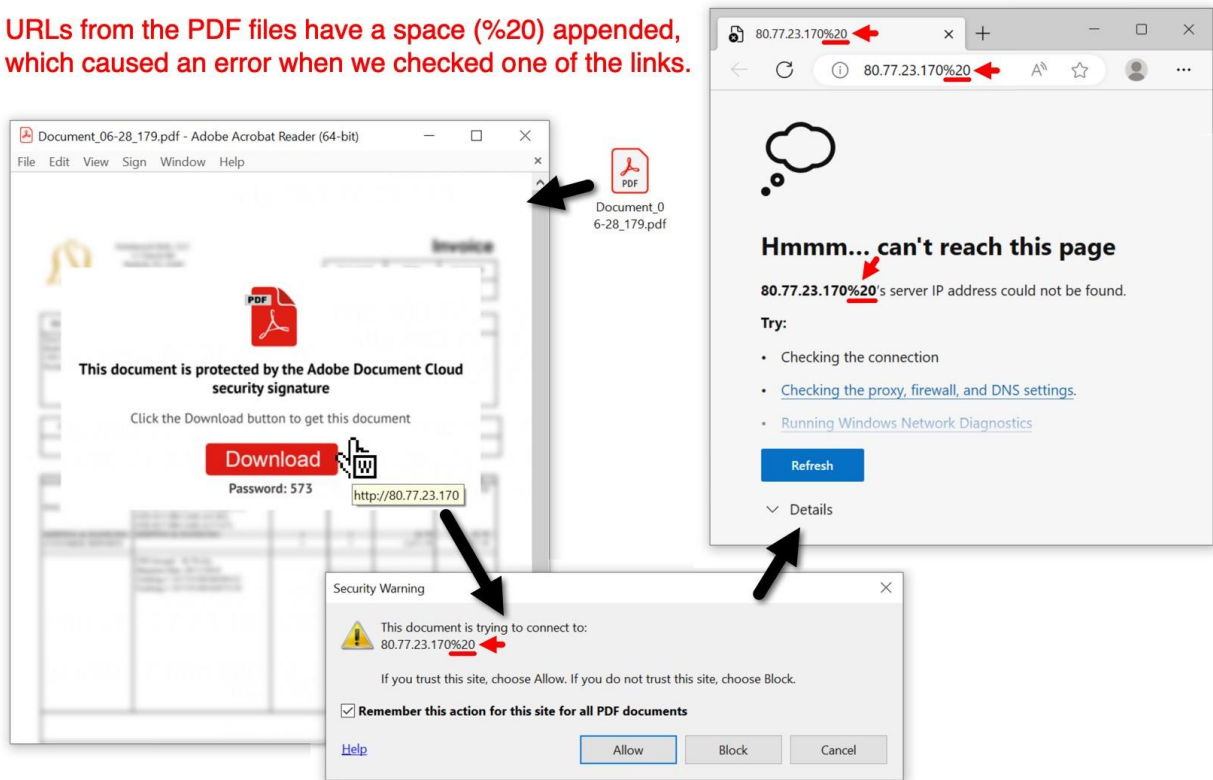


Sau khi tải file pdf đầy về chúng sẽ tạo 1 chuyển hướng đến các link dưới đây

LINKS FROM THE ABOVE 8 PDF FILES:

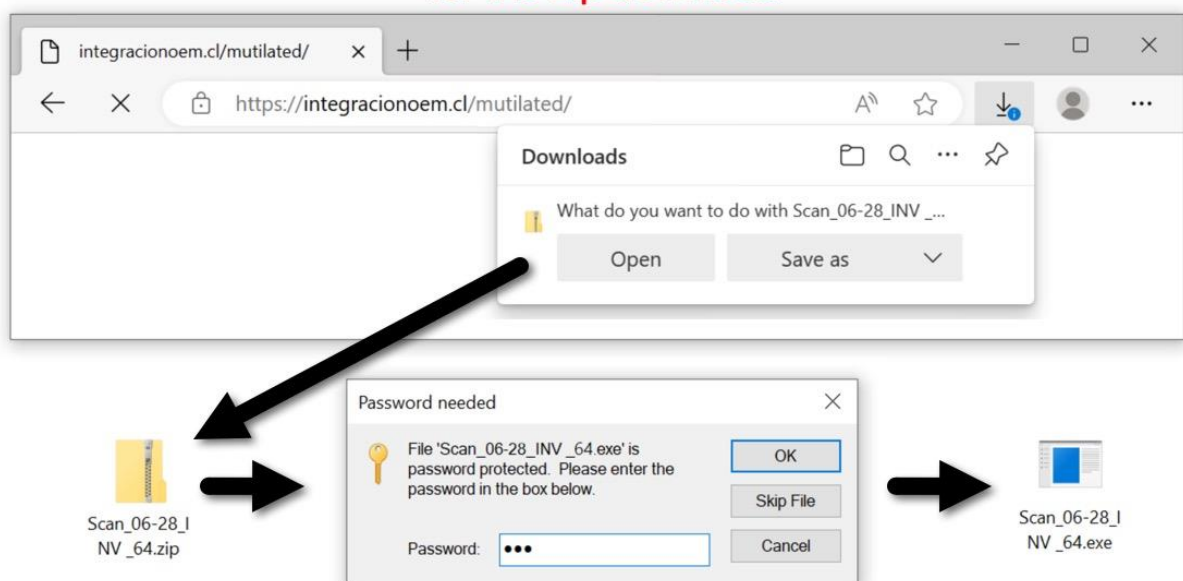
- http://80.77.23.64%20
- http://80.77.23.154%20
- http://80.77.23.155%20
- http://80.77.23.168%20
- http://80.77.23.170%20
- http://80.77.23.176%20
- http://91.240.202.190%20
- http://91.240.202.195%20

URLs from the PDF files have a space (%20) appended, which caused an error when we checked one of the links.



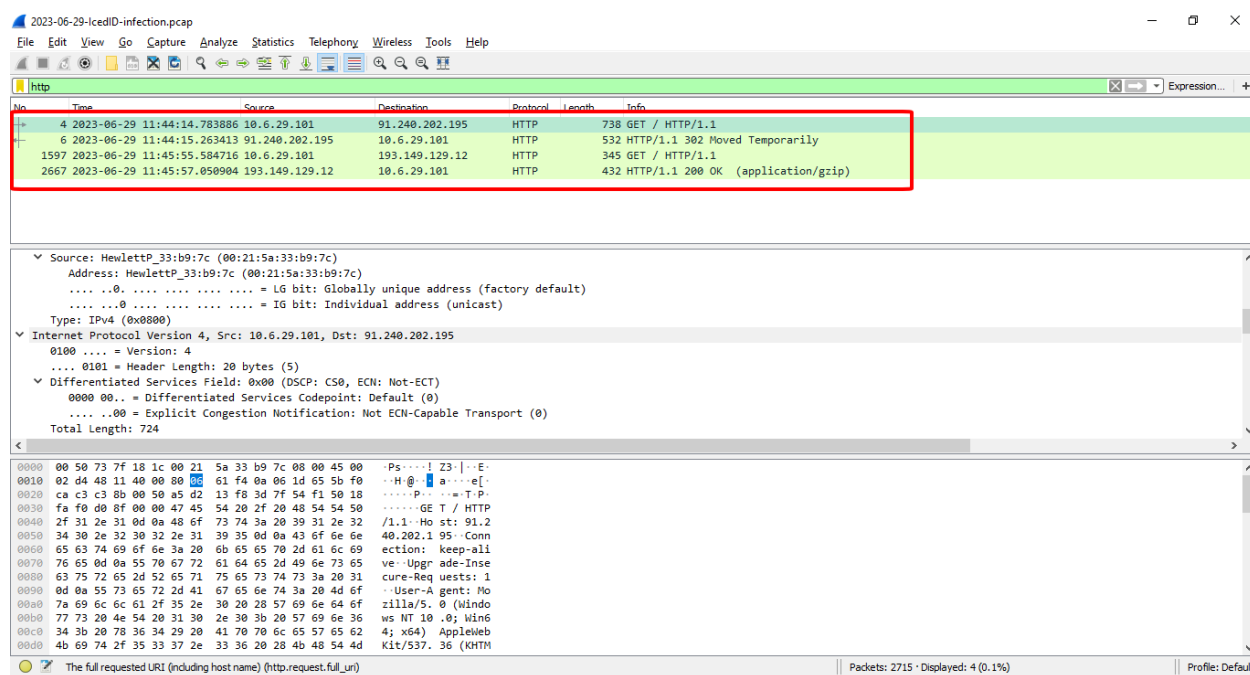
Khi ta ấn vào liên kết đó thì 1 tệp zip được bảo vệ bằng mật khẩu sẽ được tải xuống bên trong đó là file installer exe của Icedid

Corrected URL (removing the "%20") redirects to a different URL for the zip download



II. Tiến hành điều tra gói tin bằng Wireshark

Ta nhập vào filter http để điều tra và phát hiện ra rằng browser của chúng đều hướng đến port 80, tại vì ngày nay chúng ta xài port 443 nhiều hơn port 80 nên ta sẽ lưu ý điều đó



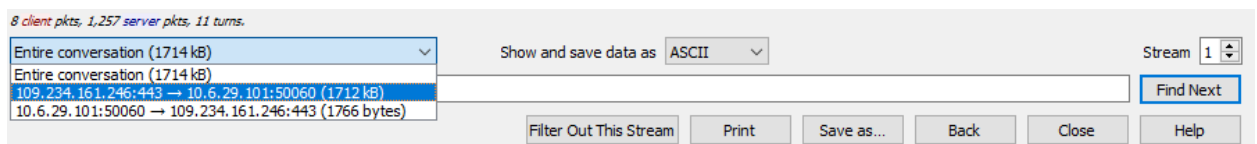
```
GET / HTTP/1.1
Host: 91.240.202.195
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Edg/114.0.1823.58
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _subid=ukiaandutn;
34ab8=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWZtc1wiOntcIjI3NFwiOjE2ODgwMTM2MTR9LFwiY2FtcGFpZ25zXCi6e1wiNjdcIjoxNjg4MDEzNjE0fScxInRpbWVcIjoxNjg4MDEzNjE0fSc3J9.CSqdncUn1Kj1pQPu0P0W9ZIKvdd_E61wQjJbJBtN-8

HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Thu, 29 Jun 2023 04:44:16 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=bnkvs03vg77bm7m78ovdavmlq9; path=/
Set-Cookie: _subid=ukiaandutv; expires=Fri, 30-Jun-2023 04:44:16 GMT; Max-Age=86400; path=/
Location: https://myliishop.com/pharmacopoeias
```

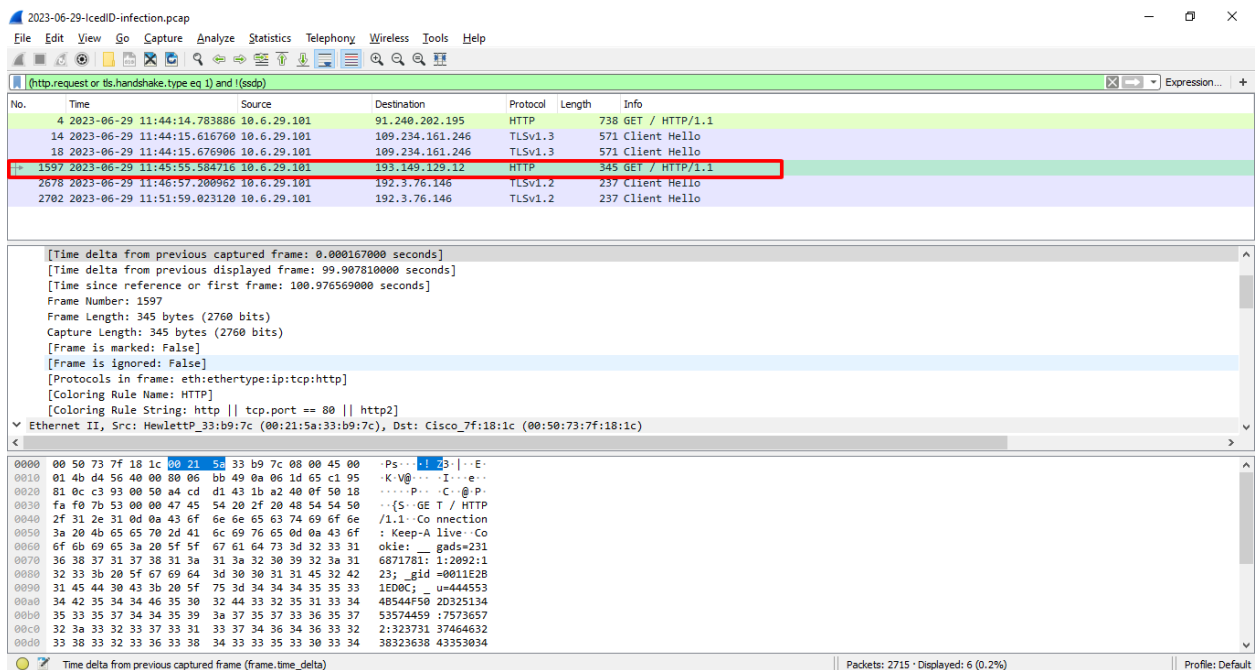
Hình trên cho ta 1 lệnh 302 Moved Temporarily, chuyển hướng đến trang web myliishop.com/pharmacopoeias để download file zip. Trang này đã bị reported

trên virustotal là có liên quan đến Icedid và google là hạ cái link này xuống và đang trong trạng thái inactive.

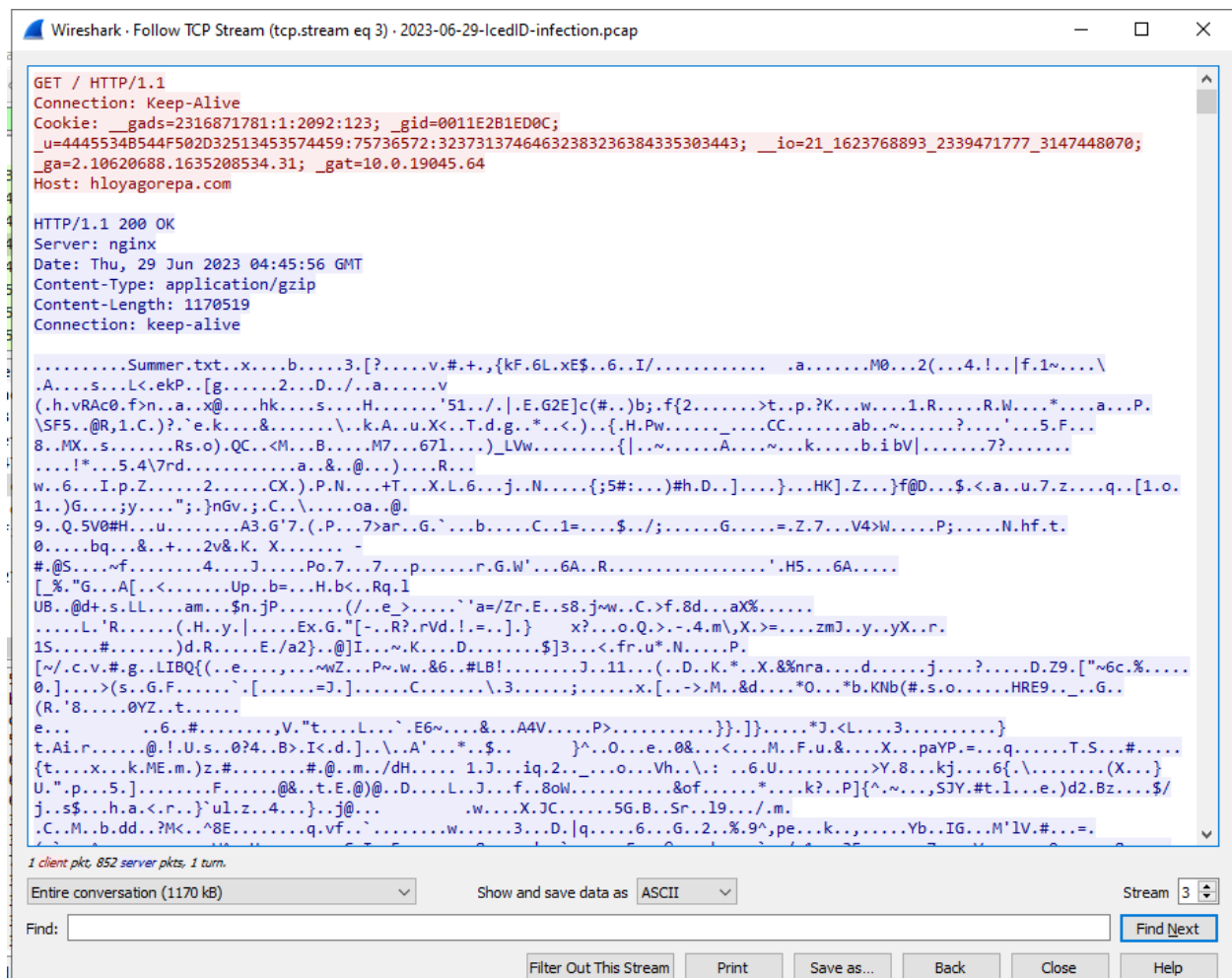
Follow TCP thì ta thấy được dữ liệu được gửi từ server tới window host, dựa vào đó ta có thể đoán được cái URL này nó gửi đến window host 1 IcedID Installer



Vào lúc 11h45 thì máy host 10.6.29.101 có tạo 1 HTTP GET đến địa chỉ 193.149.129.12 như hình dưới đây



Ta tiến hành Follow TCP của nó như hình dưới thì nó sẽ hiện ra một cửa sổ TCP Stream trong đó ta phát hiện có file gzip binary và cookie



Ở đây ta có thể phân tích được dựa vào cookie mà nó cung cấp cho ta:

Cookie: __gads=2316871781:1:2092:123; _gid=0011E2B1ED0C;
_u=4445534B544F502D32513453574459:75736572:323731374646323832363
84335303443; __io=21_1623768893_2339471777_3147448070;
_ga=2.10620688.1635208534.31; _gat=10.0.19045.64

- __gads: Định danh chiến dịch IcedID và thông tin từ máy chủ bị nhiễm.
- _gid: Giá trị được tính toán bằng địa chỉ MAC của máy chủ bị nhiễm.
- _u: Văn bản ASCII biểu diễn các giá trị hex của tên máy nạn nhân, tên tài khoản người dùng Windows, và một giá trị khác không xác định.

- __io: Định danh miền từ SID (Security Identifier) của máy chủ bị nhiễm.
- _ga: Thông tin dựa trên CPU của máy chủ bị nhiễm.
- _gat: Phiên bản Windows. Ví dụ, 10.0.22621.64 là một định danh cho phiên bản Windows 11 64-bit version 22H2 và 10.0.19045.64 là một định danh cho phiên bản Windows 10 64-bit version 22H2.

Giải mã Hex ta được:
DESKTOP-2Q4SWDY

Giải mã Hex ta được:
user

↑ ↑

u=4445534B544F502D32513453574459:75736572:32373137464632383236384335303443; __io=21_1623768893_2339471777_3147448070;

Giải mã cho đoạn cookie ở trên

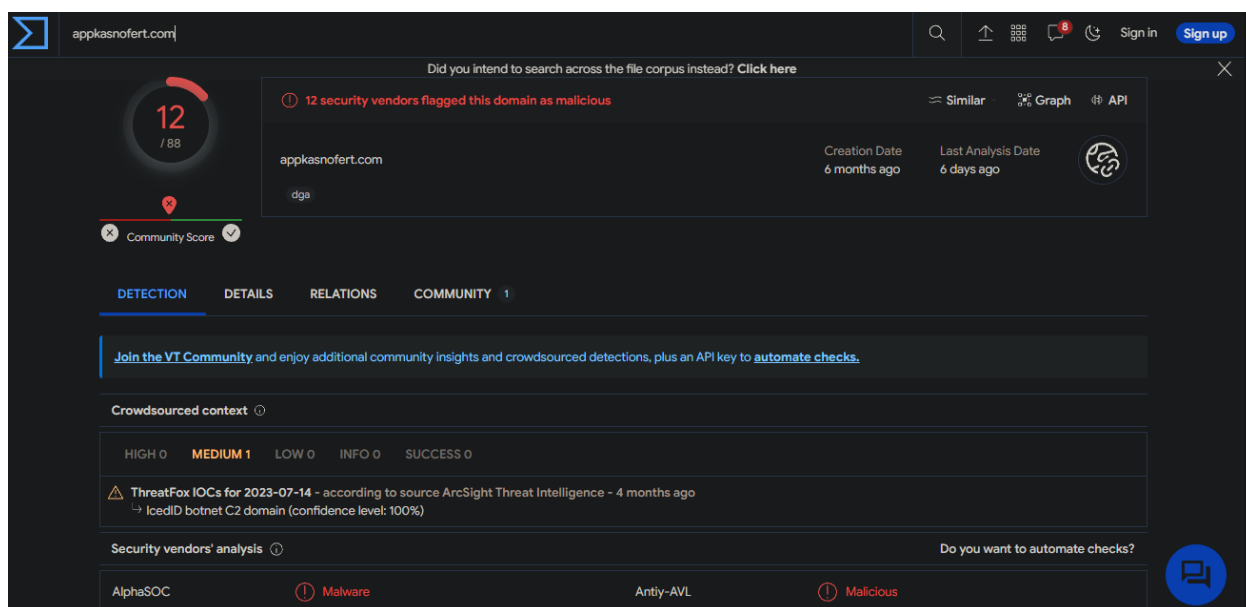
Sau khi nhận được file gzip binary, thì thiết lập một sự lây nhiễm mạnh mẽ và điều hướng tới server C2, ở đây server C2 của nó là appkasnofert.com ip 192.3.76.146

The image shows a Wireshark packet capture of a GET request to appkasnofert.com. The packet list shows a GET request to 192.3.76.146. The packet details show the request structure, including the URL and the destination IP. Annotations with arrows point to the URL and the destination IP, indicating the setup for the infection and redirection to server C2.

No.	Time	Source	Destination	Protocol	Length	Info
4	2023-06-29 11:44:14.783886	10.6.29.101	91.240.202.195	HTTP	738	GET / HTTP/1.1
14	2023-06-29 11:44:15.616760	10.6.29.101	109.234.161.246	TLSv1.3	571	Client Hello
18	2023-06-29 11:44:15.676906	10.6.29.101	109.234.161.246	TLSv1.3	571	Client Hello
1597	2023-06-29 11:45:55.584716	10.6.29.101	193.149.129.12	HTTP	345	GET / HTTP/1.1
2678	2023-06-29 11:46:57.200962	10.6.29.101	192.3.76.146	TLSv1.2	237	Client Hello
2702	2023-06-29 11:51:59.023120	10.6.29.101	192.3.76.146	TLSv1.2	237	Client Hello

Annotations in the image:

- url mà nhận gzip binary để thiết lập sự lây nhiễm (points to the GET request)
- Điều hướng tới server C2 (points to the destination IP 192.3.76.146)



Hình cho thấy appkasnofert.com là C2 của IcedID

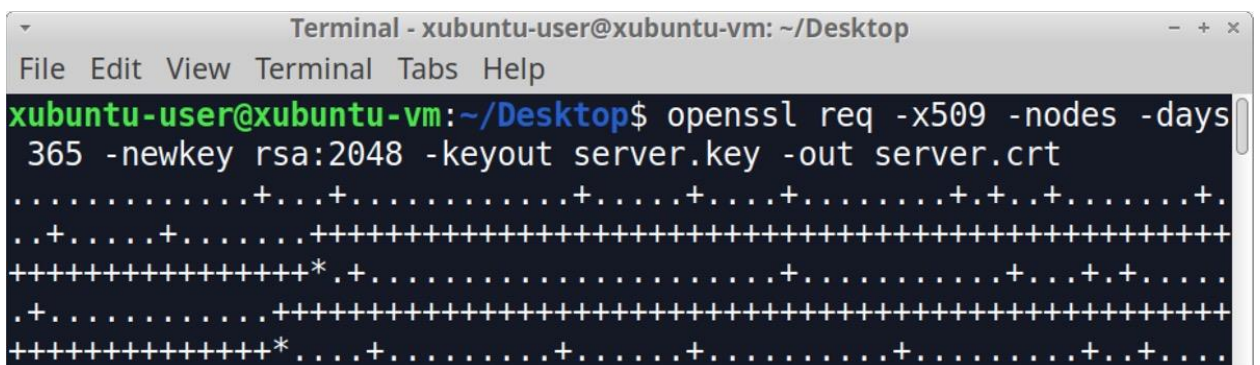
Một trang web muốn được công nhận là 1 trang web thì nó phải có chứng chỉ nhưng tội phạm thì lấy đâu ra chứng chỉ, thế là chúng phải tự tạo nên cho mình chứng chỉ tự ký(self-signed certificated) để đánh lừa người truy cập nhưng muốn tạo chứng chỉ thì chỉ có thể sử dụng những cái default value nên ta có thể check pcap sử dụng filter sau:

x509sat.uTF8String eq "Internet Widgits Pty Ltd"

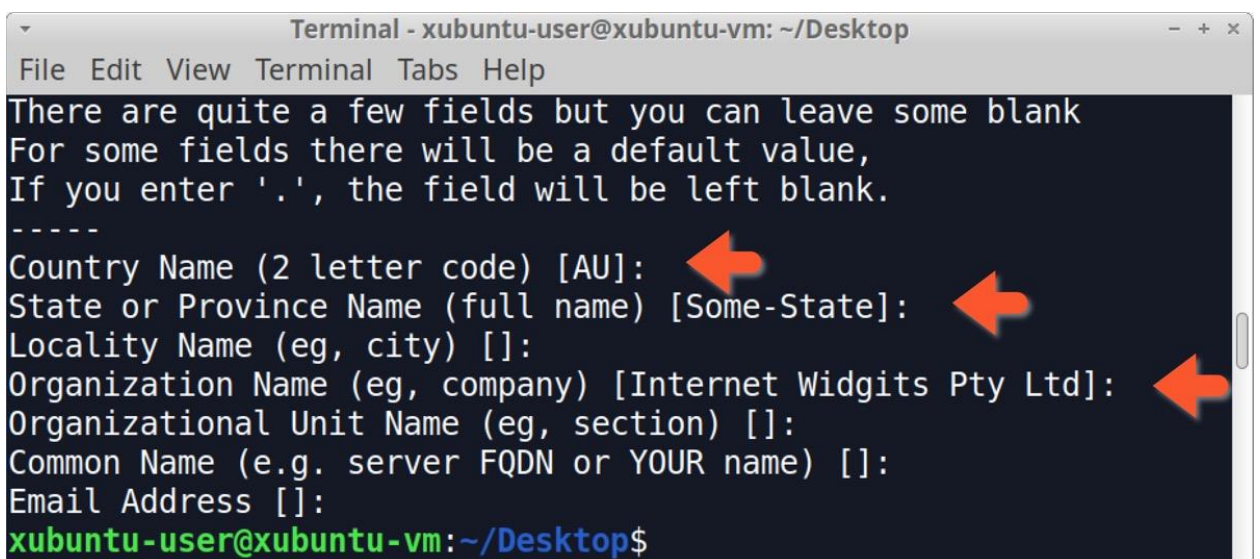


Chứng chỉ của Icedid C2 server

Như ta thấy thì chứng toàn là default value của chứng chỉ tự ký(self-signed certificate) y hệt như khi sử dụng OpenSSL để tạo chứng chỉ web server trong Xubuntu như 2 hình dưới đây



Tạo chứng chỉ trong xubuntu



Các default value mà người dùng nhập để tạo chứng chỉ

III. Kết luận

Sự lây nhiễm bắt đầu từ: 29-6-2023 vào lúc 11h46 UTC

IP của máy bị nhiễm malware: 10.6.29.101

Tên máy bị nhiễm: DESKTOP-2Q4SWDY

Account name của người dung: user

TÀI LIỆU THAM KHẢO

- https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/icedid?fbclid=IwAR3ohdsfq6iejuhFchOlyBEar3VFJKTUqMs0q_Hf61h-SAnAciwjnPYPY9t_E
- <https://antoanthongtin.vn/hacker-malware/canh-bao-ve-hai-bien-the-moi-cua-icedid-duoc-su-dung-de-phan-phoi-phan-mem-doc-hai-108839?fbclid=IwAR3tM4PZH8qMV3ewnrIl9eZtn16AV6foxsGqOyd45pQQYVmRR89E-vhZe00>
- [https://www.proofpoint.com/us/search?content\[query\]=icedid](https://www.proofpoint.com/us/search?content[query]=icedid)