Bộ Giáo Dục Và Đào Tạo

Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh

Khoa Công Nghệ Thông Tin

ĐỒ ÁN MÔN HỌC: ĐIỀU TRA TẤN CÔNG

ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI PHẦN MỀM MÃ ĐỘC ICEDID

GVHD: Phạm Đình Thắng

SV: Trần Ngọc Vinh – 21DH113413

SV: Nguyễn Hoàng Phúc – 21DH114014

SV: Lê Thành Ân – 21DH112304

TP. HỒ CHÍ MINH, 2023

NHẬN XÉT CỦA GIẢNG VIÊN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

PHIẾU CHẤM ĐIỂM MÔN THI VẤN ĐÁP

Điểm phần trình bày – Điểm hệ số 10:

	CBCT1	CBCT2
Họ và tên CBCT	..... Chữ ký:.....…….....	..... Chữ ký:.....…….....
Điểm thi	..... Bằng chữ:	..... Bằng chữ: .....
Nhận xét: Báo cáo: 2đ Vấn đáp: 2đ Chức năng và demo: 5đ Mở rộng và ứng dụng thực tiễn: 1đ	Quyển báo cáo: (...)điểm... Vấn đáp: (...) điểm... Chức năng: (...) điểm... Mở rộng: (...) điểm...	Quyển báo cáo: (...)điểm... Vấn đáp: (...) điểm... Chức năng: (...) điểm... Mở rộng: (...) điểm... ....

Điểm quá trình – Điểm hệ số 10:

Họ và tên của CBCT: ……....

Điểm tổng kết: .....(Bằng chữ:.....……)

LỜI MỞ ĐẦU

Ngày nay, việc ứng dụng công nghệ thông tin đã trở nên phổ biến trong hầu hết mọi cơ quan, doanh nghiệp, trường học đặc biệt là việc áp dụng các giải pháp tin học trong công tác quản lý hoặc để xây dựng những hệ thống phục vụ cho một mục đích nào đó. Với sự phát triển vượt bậc của công nghệ ngày một được đưa vào đời sống của chúng ta nhiều hơn, có thể nói rằng hầu hết mọi công việc, tác vụ hoặc giải trí đã và đang ngày một được gói gọn trong những thiết bị sử dụng hằng ngày.

Công nghệ thông tin trở thành một ngành học, một lĩnh vực không thể thiếu để áp dụng vào nhiều lĩnh vực khác liên quan đến mọi ngành nghề, giúp cho đời sống của chúng ta ngày một dễ dàng, tiện lợi và nhanh chóng hơn. Tuy rằng công việc tự học của học sinh, sinh viên trong lĩnh vực này là vô cùng quan trọng nhưng như thế vẫn là chưa đủ. Việc kết hợp yếu tố giảng dạy từ những giáo viên và người khác thì tốc độ tiếp tục và áp dụng kiến thức của chúng ta sẽ được tăng lên rất nhiều, giúp chúng ta có tính tư duy, vận dụng, tính sáng tạo cũng như kế thừa để phát huy những ưu điểm của người giảng dạy. Bởi vì những yếu tố ấy, để bắt kịp với tốc độ phát triển của xã hôi, những kiến thức có được nhờ việc đi học đầy đủ trên giảng đường là vô cùng quan trọng đối với chúng em.

LỜI CẢM ƠN

Trong thời gian làm đồ án bộ môn Điều Tra Tấn Công, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành cảm ơn thầy Phạm Đình Thắng - giảng viên Bộ môn Điều Tra Tấn Công - trường đại học Ngoại Ngữ - Tin Học (HUFLIT) người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm khoá luận.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường nói chung, các thầy cô chuyên ngành An Ninh Mạng thuộc Công Nghệ Thông Tin đã dạy dỗ cho em kiến thức về các môn đại cương cũng như các môn chuyên ngành, giúp em có được cơ sở lý thuyết vững vàng và tạo điều kiện giúp đỡ em trong suốt quá trình học tập.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành khoá luận tốt nghiệp.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế của một học viên, luận văn này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để tôi có điều kiện bổ sung, nâng cao ý thức của mình, phục vụ tốt hơn công tác thực tế sau này.

MỤC LỤC

DANH MỤC HÌNH ẢNH

CHƯƠNG I: TỔNG QUAN VỀ ĐỀ TÀI

1. Mục tiêu đề tài:

Hiện nay, điều tra tấn công mạng đang thu hút sự quan tâm từ phía các doanh nghiệp có hoạt động và lĩnh vực liên quan đến việc bảo mật và an ninh mạng, kể cả những doanh nghiệp vừa và nhỏ. Việc này đóng vai trò quan trọng trong quản lý hoạt động, bảo mật thông tin nội bộ, và đảm bảo tính hiệu quả của công việc. Các loại thông tin cần được quản lý đa dạng, bao gồm văn bản mật như file hồ sơ thầu và kế hoạch phát triển, dữ liệu kế toán, cũng như thông tin liên quan đến sản phẩm như phần mềm và bản thiết kế. Sự rò rỉ thông tin không mong muốn có thể mang lại tổn thất đáng kể cho doanh nghiệp. Do đó, việc tổ chức hệ thống thông tin và thiết kế mạng một cách cẩn thận trở nên quan trọng hơn bao giờ hết.

2. Phạm vi đề tài:

Phạm vị đề tài sẽ xoay quanh về phần mềm mã độc IcedID và lịch sử báo cáo hoạt động duyệt web ngày 29/06/2023 dựa vào file pcap và phần mềm WireShark.

3. Ý nghĩa:

Điều tra tấn công mạng là một phần không thể thiếu trong công cuộc giúp cho môi trường sử dụng mạng của mọi người được trở nên trong sạch và đáng tin cậy hơn. Hiện nay có rất nhiều trang web hoặc những nguồn tin giả mạo làm ảnh hưởng và gây tổn thất nhiều mặt cho nhiều cá nhân, chủ thể khác nhau. Việc phòng chống, bảo mật và phát hiện những hành vi sai trái ấy cũng giúp cho vấn đền an ninh trật tự mạng nói riêng và an ninh trật tự đời sống nói chúng được ngày một có quy củ và phép tắc hơn.

CHƯƠNG II: LÝ THUYẾT TỔNG QUAN

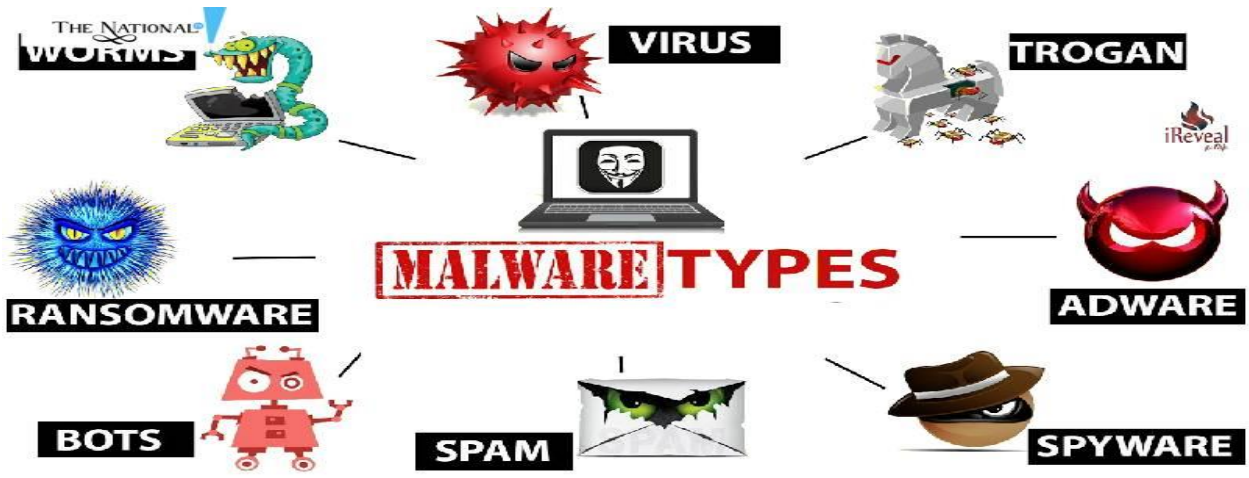
1. Giới thiệu về IcedID:

a/ IcedID là gì?

IcedID, hay còn được biết đến là BOKBOT, là một phần mềm độc hại được phát hiện lần đầu tiên vào tháng 9 năm 2017. Đây là một Trojan banking hay còn được hiểu là một loại phần mềm mã độc được thiết kế để đánh cắp thông tin tài khoản ngân hàng và thông tin đăng nhập của người dung có liên quan đến tài khoản trực tuyến của họ, điển hình như tài khoản VISA hoặc tài khoản Momo,…. Với sự trở lại của môt phần mềm mã độc khác mang tên Emotet với mục đích hoạt động khá tương tự, kể từ khi xuất hiện, IcedID đã trải qua rất nhiều phiên bản và được cập nhật liên tục nhằm tránh sự phát hiện và khiến cho chúng trở nên nguy hiểm hơn.

b/ Phương thức hoạt động:

IcedID luôn được xem là một trong những phần mềm độc hại vô cùng nguy hiểm và có sức ảnh hưởng vô cùng mạnh mẽ. Chúng nó những phương thức hoạt động và những cách thức tưởng chừng vô cùng đơn giản nhưng cũng rất dễ dàng để có thể tiếp cận đến thông tin người dùng.



Hình 1. Một số malware và phần mềm độc hại phổ biến

Phising: đây là một kỹ thuật tấn công mà kẻ tấn công giả mạo một thực thể đáng tin cậy để lừa dối người dùng và thu thập thông tin nhạy cảm và mật như tên đăng nhập người dùng, mật khẩu, hoặc thông tin tài khoản ngân hàng. Có rất nhiều biến thể của hình thức tấn công này, điển hình trong số đó là:

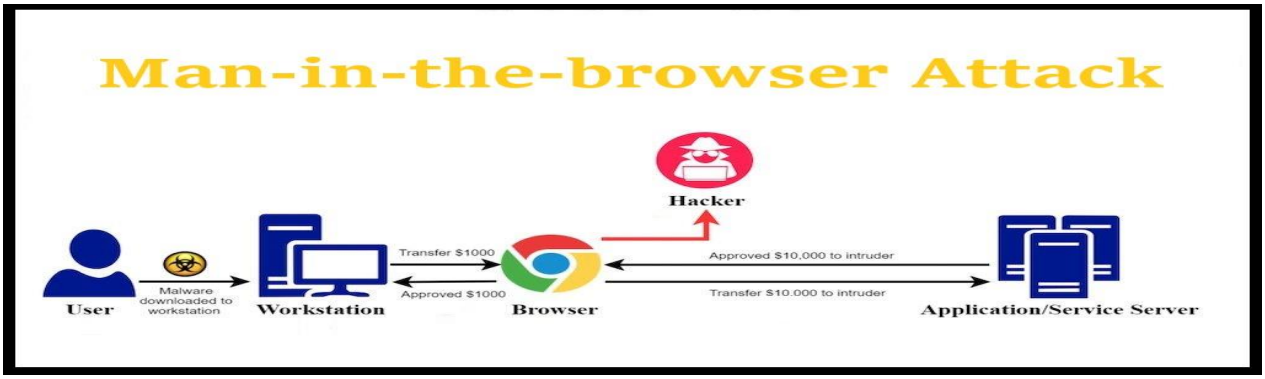
- Email phising: kẻ tấn công sẽ thiết lập một tài khoản email giả mạo và gửi mail đến cho mục tiêu là người dùng. Người dùng sẽ nhận được mail có thông tin và thông điệp vô cùng hấp dẫn hoặc những thông điệp cảm kích nhằm tạo nên độ tin cậy và trong mail sẽ chứa nhưng file hoặc tệp có chứa một malware IcedID để từ đó, kẻ tấn công sẽ dễ dàng đánh cắp thông tin. Chúng cũng có thể thay thế file đính kèm bằng những đường link dẫn đến những trang web có mã độc và mục đích tương tự.
- Spear phising: phương thức này nhắm đến một cá nhân cụ thể hoặc một nhóm nhỏ người dùng. Kẻ tấn công thường nghiên cứu về đối tượng để tạo ra thông điệp và liên kết giả mạo có tính cá nhân cao. Các email spear phishing thường chứa thông tin cá nhân, ví dụ như tên đăng nhập, tên người nhận, hoặc dự án cụ thể để làm cho nó trở nên thuyết phục hơn.
- Vishing (Voice Phising): thay vì sử dụng email, kẻ tấn công sẽ sử dụng điện thoại để giả mạo bản thân là một đại diện của tổ chức đáng tin cậy, yêu cầu người dùng cung cấp thông tin cá nhân hoặc thực hiện các hành động nhất định. Hiện nay phương thức này khó có thể được áp dụng một cách thường xuyên bởi hệ thống quản lý các số điện thoại giả mạo hiện nay đang hoạt động thường xuyên và rất hiệu quả trong việc ngăn chặn những số điện thoại rác.

- Smishing (SMS Phishing): phương pháp này sẽ sử dụng đến việc gửi các tin nhắn SMS trên điện thoại và sau đó yêu cầu mục tiêu cung cấp thông tin nhạy cảm cho kẻ tấn công. Phương thức này cũng dần bị hạn chế như Vishing.

Phương thức phishing ngày càng trở nên phức tạp và nguy hiểm và người dùng cần duy trì sự cảnh báo cao và thực hiện biện pháp bảo mật như không nhấp vào liên kết hoặc mở tệp đính kèm từ các nguồn không rõ. Các công ty và tổ chức cũng cần đào tạo nhân viên về cách nhận diện và phòng tránh các cuộc tấn công phishing. Với sự phát triển của công nghệ và sự bảo mật an ninh được hoạt động ngày một hiệu quả, cũng không thể không đề phòng bởi những kẻ tấn công với mục đích xấu cũng dễ dàng tiếp thu và thay đổi phương thức hoạt động của chúng.

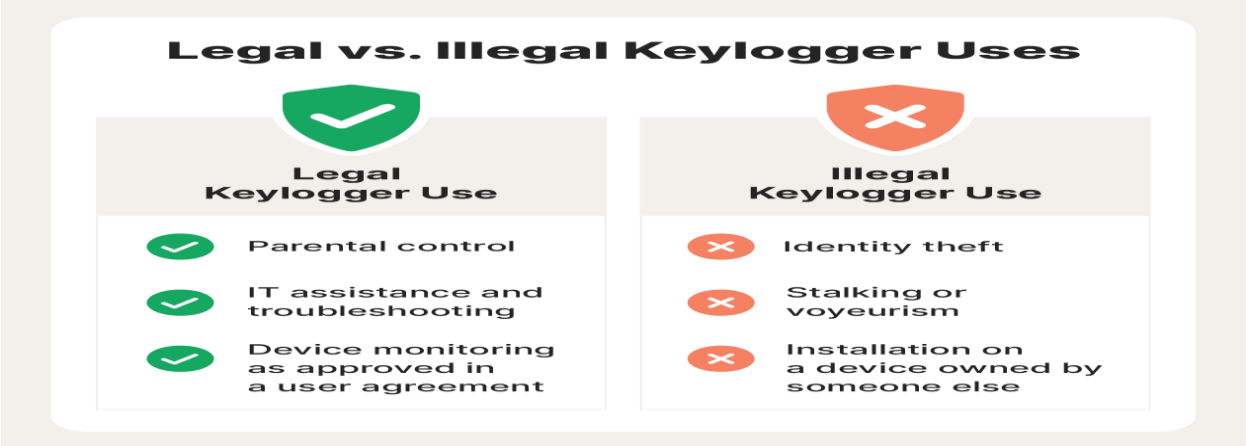
Hình 2. Hình ảnh tượng trưng nói về vấn nạn các tin tặc luôn tìm mọi thủ thuật để đánh cắp thông tin người dùng

Man-in-the-Browser Attacks (MITB): đây là một kỹ thuật tấn công mà kẻ tấn công can thiệp vào quá trình truyền thông giữa người dùng và trình duyệt web trên máy tính của họ. Thông thường, MITB cho phép kẻ tấn công theo dõi và thậm chí thay đổi dữ liệu giao dịch mà người dùng thực hiện trực tuyến mà không sự nhận thức của họ. Chúng thường can thiệp trực tiếp vào quá trình giao tiếp giữa người dùng với trình duyệt, có khả năng tương thích cao và được cập nhật liên tục.



Hình 3. Phương thức Man-in-the-browser Attack, một trong những phương thức hoạt động vô cùng nổi tiếng để tấn công vào trình duyệt người dùng

Triển Khai Ransomware/ Keylogger: IcedID có thể chấp nhận và triển khai các payloads khác nhau, bao gồm ransomware để mã hóa dữ liệu người dùng hoặc keylogger để ghi lại các phím được nhấn.



Hình 4. Sự khác biệt giữ Keylogger hợp lệ và Keylogger không hợp lệ

c/ Mối nguy hiểm:

IcedID mang lại nhiều bất lợi về mặt an ninh bảo mật cho các tổ chức, doanh nghiệp nói riêng cũng như người dùng mạng máy tính nói chung. Về tổng quan, sau đây là những mối nguy mà chúng mang lại:

- Đánh cắp thông tin mật của người dùng, những thông tin có liên quan đến vấn đề ngân hàng tài chính của họ
- Rủi ro về việc mất tiền trong chính tài khoản ngân hàng của họ
- Sử dụng chứng nhận SSL giả mạo khiến cho việc truy tìm và phát hiện chúng ngày càng khó khăn hơn, từ đó khiến cho chúng ngày càng nguy hiểm hơn
- Khả năng mở rộng và liên kết với những phần mềm mã độc khác, tạo ra một loạt phương thức hoạt động có sự gắn kết, ảnh hưởng và tấn công vô cùng mạnh mẽ khiến cho việc ngăn chặn dường như là không thể
- Việc những kẻ tấn công sử dụng VPN trong quá trình tấn công cũng góp phần không nhỏ khiến cho công cuộc điều tra về địa chỉ thực của chúng trở nên khó khăn hơn, càng làm cho việc ngăn chặn IcedID trở nên dai dẳng hơn

Hình 5. Hình ảnh tượng trưng cho malware IcedID luôn là malware ưa thích của các tin tặc

CHƯƠNG III: TRIỂN KHAI ĐỒ ÁN

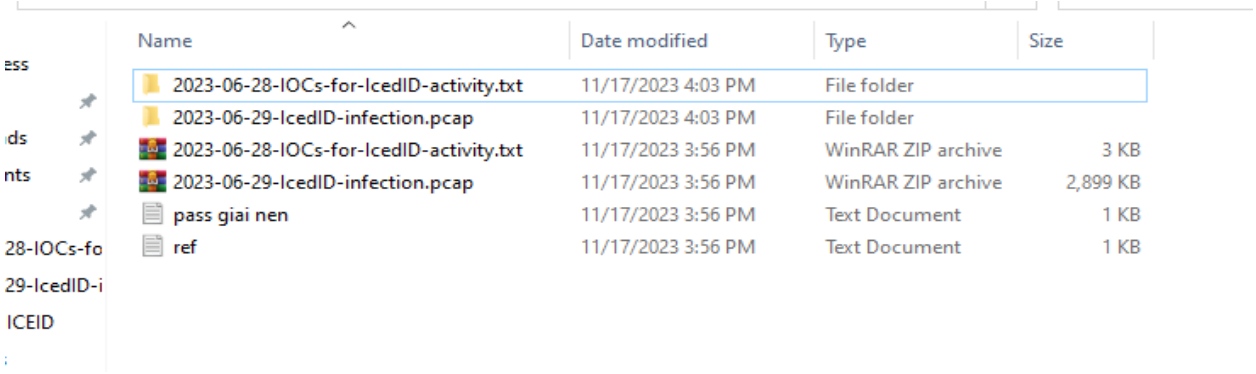
3.1/ Yêu cầu về chuyên môn:

Nhóm chúng em sẽ sử dụng phần mềm WireShark và một vài trang web phát hiện, đánh giá dựa vào trải nghiệm của nhiều người dùng để lại

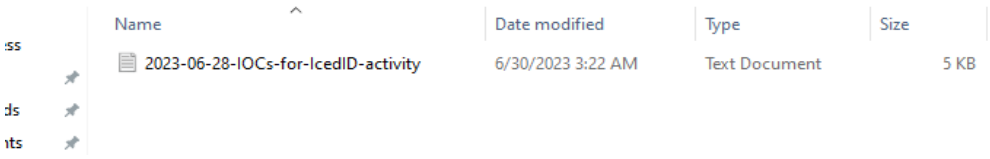
3.2/ Triển khai:

Sử dụng những tài liệu mà giảng viên đã cung cấp sẵn để giúp cho việc đồ án trở nên dễ dàng hơn, nhóm chung em sẽ báo cáo tình hình và phân tích activity về file infection ngày 29/06/2023. Phần mềm chúng em quyết định sử dụng để hiển thị những hoạt động sẽ là phần mềm WireShark.

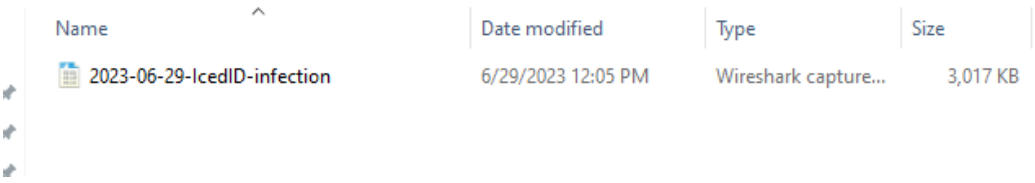
Dựa vào tài liệu, sau đây là những file để chúng em phân tích đồ án:



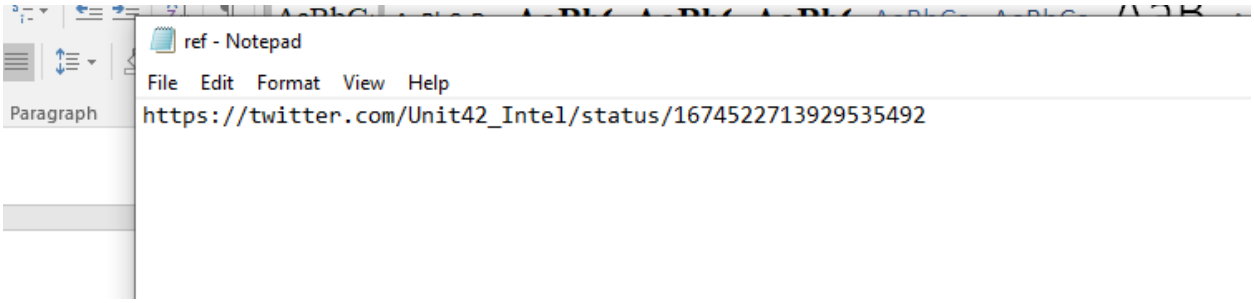
Hình 6. Tài liệu và file báo cáo về phương thức và lịch sử hoạt động của IcedID ngày 28/06/2023



Hình 7. 2023-06-28-IOCs-for-IcedID-activity.txt:



Hinh 8. 2023-06-29-IcedID-infection.pcap:



Hinh 9. File ref dẫn đến đường link Twitter, về bài viết thông báo dấu hiệu về hoạt động của IcedID trong ngày 28/06/2023

Infection chain đã được thống kê tổng hợp trong file activity.txt cho những hoạt động ngày 28/06/2023:

INFECTION CHAIN:

- email --> PDF attachment --> link from PDF --> TDS redirect --> password-protected zip archive --> EXE installer for IcedID --> gzip binary --> persistent IcedID infection established --> IcedID C2

Ta có thể dựa vào lịch sử hoạt động của file pcap trên và đưa ra kết luận về toàn bộ quá trình lây nhiễm của phần mềm độc hại này như sau:

Trước tiên, kẻ tấn công sẽ sử dụng nhiều phương thức lừa đảo khiến người dùng sẽ tải về một tập tin PDF

-> Tập tin PDF chứa đường link để tải xuống một tệp file zip

-> File zip sau khi được giải nén sẽ chứa một phần mềm con với đuôi là EXE, đây chính là phần mềm mã độc IcedID

-> Mã độc này sẽ bắt đầu xuất hiện dạng tệp tin gzip nhị phân

-> Mã độc IcedID giờ đây là mã hóa vào máy tính của nạn nhân, kẻ tấn công giờ đây đã có quyền kiểm soát và đánh cắp thông tin mật tùy vào mục đích của chúng.

Tiếp đến, chúng ta sẽ cùng phân tích những hoạt động của malware này vào ngày sớm hơn trước đó, ngày 28/06/2023

Đầu tiên, ta dựa vào 8 file ví dụ PDF đã được cho sẵn chi tiết, khi kiểm tra mã Hash của chúng trên những trang web scan malware ở trên trình duyệt như virustotal.com, đây là những kết quả của chúng:

ALYac	Trojan.GenericKD.67845515	Arcabit	Trojan.Generic.D40B3D8B
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
BitDefender	Trojan.GenericKD.67845515	Cyren	PDF/ABRisk.CMNQ-6
Emsisoft	Trojan.GenericKD.67845515 (B)	eScan	Trojan.GenericKD.67845515
GData	Trojan.GenericKD.67845515	Google	Detected
Ikarus	Trojan.Win32.Leonem	Kaspersky	HEUR:Hoax.PDF.Phish.gen
Lionic	Hacktool.PDF.Phish.3!c	MAX	Malware (ai Score=89)
McAfee	Artemis!00877F107576	McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win32/Leonem	Symantec	Trojan.Pidief
Trellix (FireEye)	Trojan.GenericKD.67845515	TrendMicro	Trojan.PDF.ICEDID.YXDF3Z
TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z	VIPRE	Trojan.GenericKD.67845515
ViRobot	PDF.Z.Agent.109894.D	ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen

Hình 10. Document_06-28_82.pdf 1

AhnLab-V3	Phishing/PDF.Agent.SC190268	Avast	PDF:PhishingX-gen [Phish]
AVG	PDF:PhishingX-gen [Phish]	Cyren	PDF/ABRisk.QDHH-5
Google	Detected	Kaspersky	HEUR:Hoax.PDF.Phish.gen
Lionic	Hacktool.PDF.Phish.3!c	McAfee	RDN/Generic.cf
McAfee-GW-Edition	RDN/Generic.cf	Microsoft	Trojan:Win32/Leonem
TrendMicro	Trojan.PDF.ICEDID.YXDF3Z	TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z
ViRobot	PDF.Z.Agent.142732	ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen

Hình 11. Document_06-28_110.pdf 2

ALYac	Trojan.GenericKD.67843956	Arcabit	Trojan.Generic.D40B3774
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
BitDefender	Trojan.GenericKD.67843956	Cyren	PDF/ABRisk.KODW-2
Emsisoft	Trojan.GenericKD.67843956 (B)	eScan	Trojan.GenericKD.67843956
GData	Trojan.GenericKD.67843956	Google	Detected
Kaspersky	HEUR:Hoax.PDF.Phish.gen	Lionic	Hacktool.PDF.Phish.3!c
MAX	Malware (ai Score=80)	McAfee	RDN/Generic.cf
McAfee-GW-Edition	RDN/Generic.cf	Microsoft	Trojan:Win32/Leonem
Symantec	Trojan.Pidief	Trellix (FireEye)	Trojan.GenericKD.67843956
TrendMicro	Trojan.PDF.ICEDID.YXDF3Z	TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z
VIPRE	Trojan.GenericKD.67843956	ViRobot	PDF.Z.Agent.138578.A
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

Hình 12. Document_06-28_179.pdf 3

Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
Avira (no cloud)	EXP/Pidief.kmnpa	Cynet	Malicious (score: 99)
Cyren	PDF/ABRisk.XAUR-2	F-Secure	Exploit.EXP/Pidief.kmnpa
GData	PDF.Trojan.Agent.9KRUMJ	Google	Detected
Kaspersky	HEUR:Hoax.PDF.Phish.gen	Lionic	Hacktool.PDF.Phish.3!c
McAfee	RDN/Generic.cf	McAfee-GW-Edition	RDN/Generic.cf
Microsoft	Trojan:Script/Sabsik.FL.A!ml	TrendMicro	Trojan.PDF.ICEDID.YXDF3Z
TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z	ViRobot	PDF.Z.Agent.139813.A
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

Hình 13. Document_06-28_250.pdf 4

ALYac	Trojan.GenericKD.67866547	Arcabit	Trojan.Generic.D40B8FB3
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
Avira (no cloud)	PHISH/KAB.Talu.qoacb	BitDefender	Trojan.GenericKD.67866547
Cynet	Malicious (score: 99)	Cyren	PDF/ABRisk.QSUF-0
Emsisoft	Trojan.GenericKD.67866547 (B)	eScan	Trojan.GenericKD.67866547
F-Secure	Phishing.PHISH/KAB.Talu.qoacb	GData	Trojan.GenericKD.67866547
Google	Detected	Ikarus	Trojan.PDF.Phish
Kaspersky	HEUR:Hoax.PDF.Phish.gen	Lionic	Hacktool.PDF.Phish.3!c
MAX	Malware (ai Score=80)	McAfee	RDN/Generic.dx
McAfee-GW-Edition	RDN/Generic.dx	Microsoft	Trojan:PDF/Phish!MSR
QuickHeal	Pdf.Trojan.A7880061	Symantec	Trojan.Gen.NPE
Tencent	Pdf.Trojan-PSW.Phish.Ocnw	Trellix (FireEye)	Trojan.GenericKD.67866547
TrendMicro	Trojan.PDF.ICEDID.YXDF3Z	TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z
VIPRE	Trojan.GenericKD.67866547	ViRobot	PDF.Z.Agent.146995
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

Hình 14. Document_06-28_425.pdf 5

ALYac	Trojan.GenericKD.68018755	Arcabit	Trojan.Generic.D40DE243
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
BitDefender	Trojan.GenericKD.68018755	Cyren	PDF/ABRisk.GLFJ-5
Emsisoft	Trojan.GenericKD.68018755 (B)	eScan	Trojan.GenericKD.68018755
GData	Trojan.GenericKD.68018755	Google	Detected
Kaspersky	HEUR:Hoax.PDF.Phish.gen	MAX	Malware (ai Score=84)
McAfee	Artemis!96AA4101C6C3	McAfee-GW-Edition	Artemis
Trellix (FireEye)	Trojan.GenericKD.68018755	TrendMicro	Trojan.PDF.ICEDID.YXDF3Z
TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z	VIPRE	Trojan.GenericKD.68018755
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

Hình 15. Document_06-28_452.pdf 6

ALYac	Trojan.GenericKD.68018486	Arcabit	Trojan.Generic.D40DE136
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
BitDefender	Trojan.GenericKD.68018486	Cyren	PDF/ABRisk.BWEB-2
Emsisoft	Trojan.GenericKD.68018486 (B)	eScan	Trojan.GenericKD.68018486
GData	Trojan.GenericKD.68018486	Google	Detected
Kaspersky	HEUR:Hoax.PDF.Phish.gen	MAX	Malware (ai Score=87)
McAfee	Artemis!BF209549D128	McAfee-GW-Edition	Artemis
Trellix (FireEye)	Trojan.GenericKD.68018486	TrendMicro	Trojan.PDF.ICEDID.YXDF3Z
TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z	VIPRE	Trojan.GenericKD.68018486
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

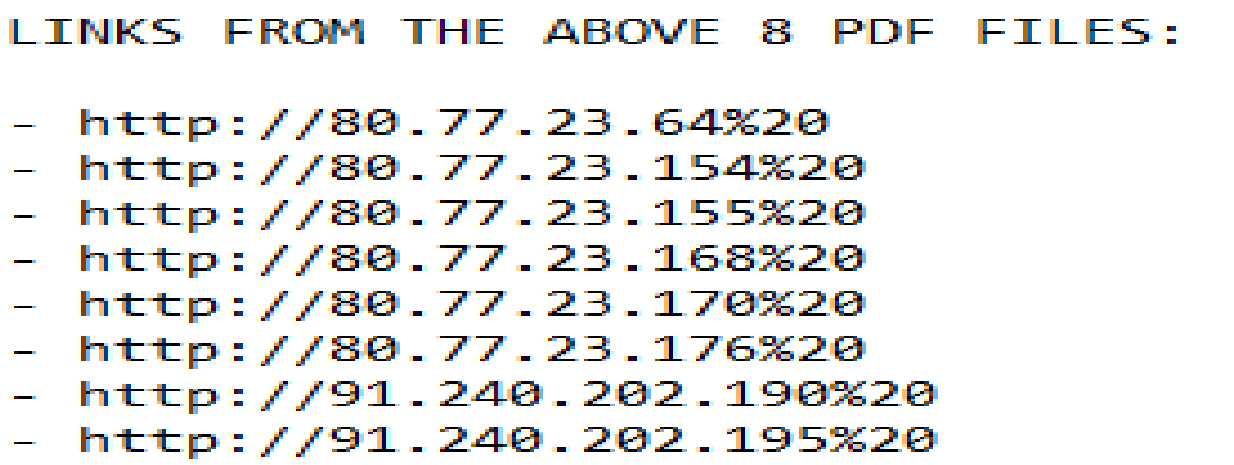
Hình 16. Document_06-28_475.pdf 7

ALYac	Trojan.GenericKD.68018485	Arcabit	Trojan.Generic.D40DE135
Avast	PDF:PhishingX-gen [Phish]	AVG	PDF:PhishingX-gen [Phish]
Avira (no cloud)	PHISH/KAB.Talu.ehwis	BitDefender	Trojan.GenericKD.68018485
Cynet	Malicious (score: 99)	Cyren	PDF/ABRisk.RZFI-6
Emsisoft	Trojan.GenericKD.68018485 (B)	eScan	Trojan.GenericKD.68018485
F-Secure	Phishing.PHISH/KAB.Talu.ehwis	GData	Trojan.GenericKD.68018485
Google	Detected	Kaspersky	HEUR:Hoax.PDF.Phish.gen
Lionic	Hacktool.PDF.Phish.3!c	MAX	Malware (ai Score=88)
McAfee	RDN/Generic.cf	McAfee-GW-Edition	RDN/Generic.cf
Trellix (FireEye)	Trojan.GenericKD.68018485	TrendMicro	Trojan.PDF.ICEDID.YXDF3Z
TrendMicro-HouseCall	Trojan.PDF.ICEDID.YXDF3Z	VIPRE	Trojan.GenericKD.68018485
ZoneAlarm by Check Point	HEUR:Hoax.PDF.Phish.gen	Acronis (Static ML)	Undetected

Hình 17. Document_06-28_494.pdf 8

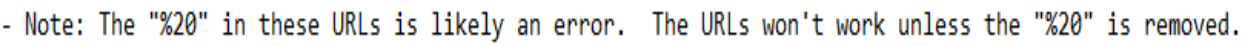
Khi nhìn chung qua đánh giá và vấn đề an toàn trong việc bảo mật của trang web, có một điều rất dễ để nhận biết rằng chúng đều sử dụng chung phương thức Phising – một phương thức rất phổ biến được những tin tặc, hacker sử dụng trong quá trình lây nhiễm phần mềm mã độc IcedID.

Dựa vào Infection Chain mà bản báo cáo ngày 28/06/2023 đã tổng kết lại, những file PDF ấy đều tồn tại một đường link dẫn đến file zip chứa IcedID để triển khai. Những đường link ấy được xếp theo thứ tự như sau:



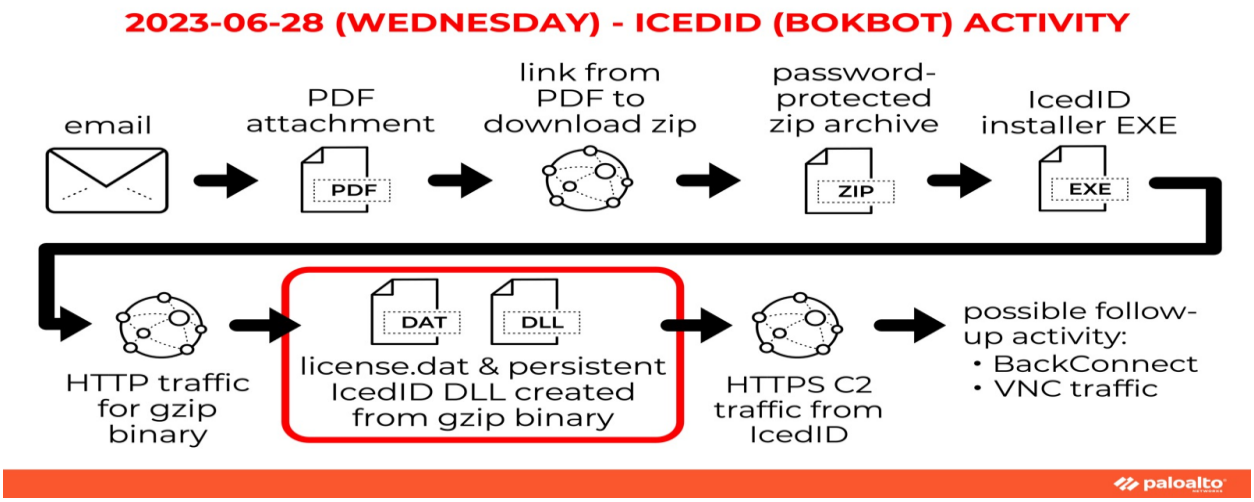
Hình 18. Đường link được đính kèm trong 8 file PDF, dẫn đến trang web tải xuống tệp zip có malware IcedID

Và cũng thông qua đánh giá của virustotal.com, những đường link này cũng đã được xếp hạng và đánh giá là những đường link có độ nguy hiểm cao và chứa malware. Nên lưu ý rằng, những đường link này sẽ thật sự hoạt động khi và chỉ khi ở cuối mỗi đường link, đuôi "%20" phải được loại bỏ để đường link có thể hoạt động thành công:

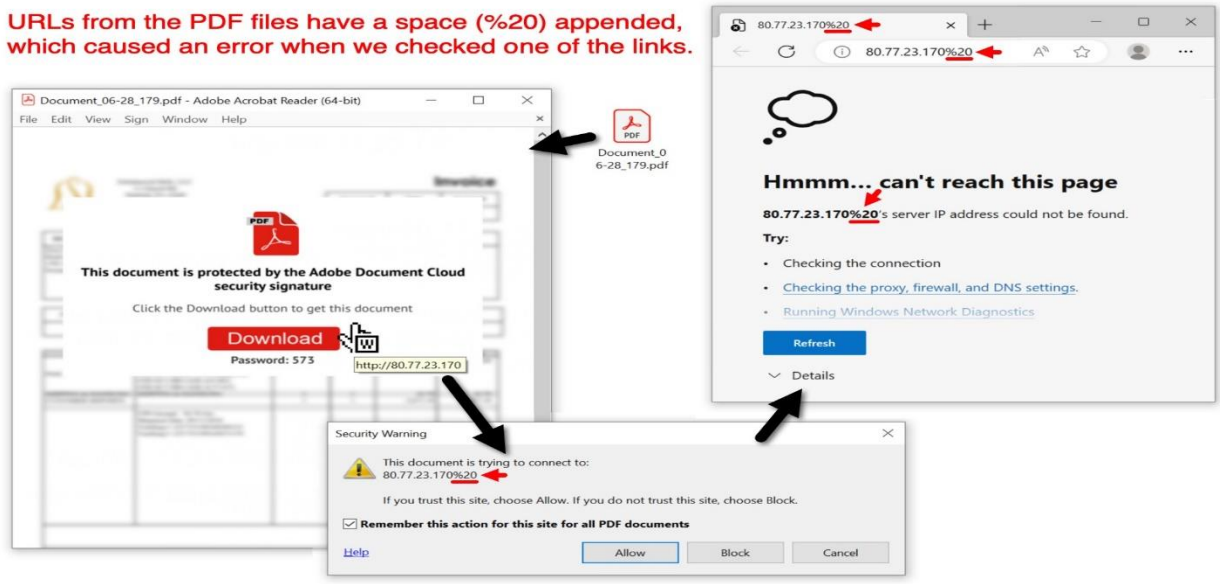


Hình 19. Lưu ý về đường dẫn để tải về file zip

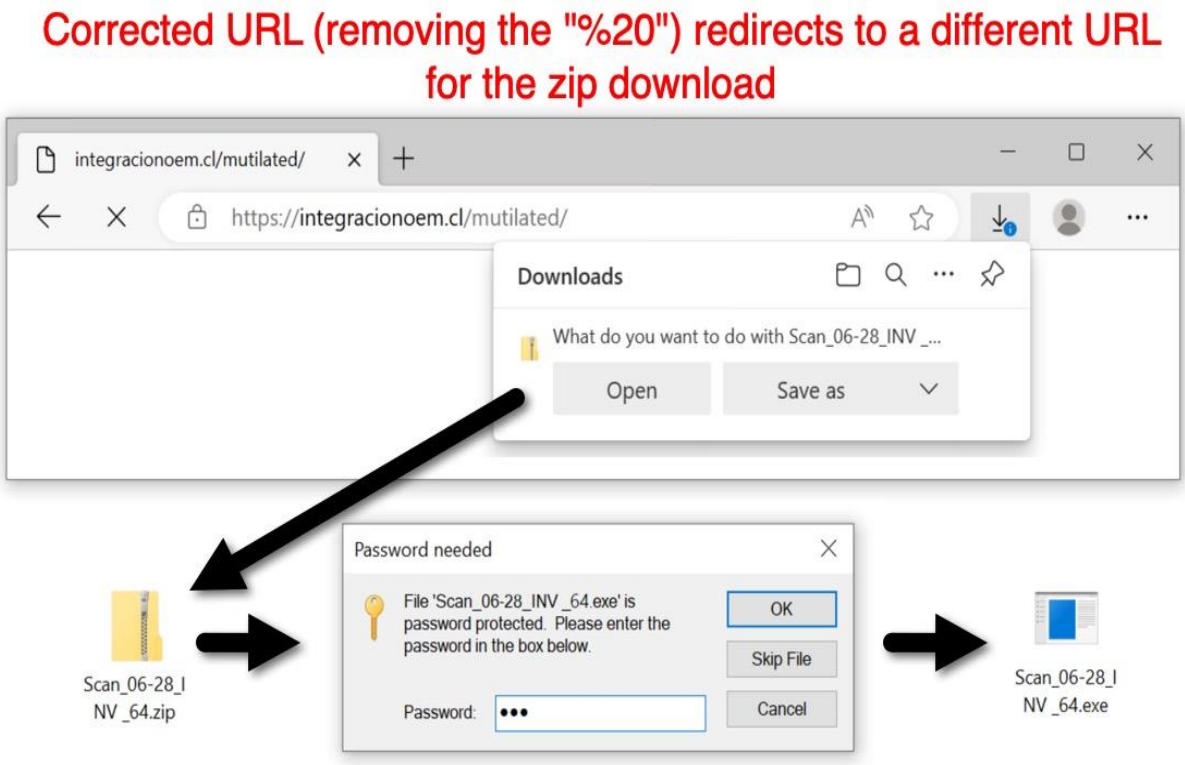
Sau đây là một vài hình ảnh chi tiết hơn về việc IcedID được gán vào những file PDF thông qua những phương thức hoạt động lừa đảo mà hacker đã khiến cho người dùng không may tải về và cài đặt trên máy của mình (nguồn từ bài viết trên Twitter của Unit42 với nội dung báo cáo về hình thức và quá trình hoạt động của IcedID):



Hình 20. Qúa trình hoạt động của tin tặc nhằm đưa malware IcedID vào bên trong thiết bị của nạn nhân



Hình 21. Như lưu ý của Unit42, đường lin dẫn đến mục tải về file zip chỉ thực sự thành công khi đuôi "%20" bị loại bỏ



Hình 22. Tệp file zip sẽ được bảo mật bởi mật khẩu mà những tin tặc đã cung cấp sẵn trong file PDF

Tiếp đến , nhóm chúng em sẽ bắt đầu quá trình phân tích và báo cáo quá trình hoạt động của IcedID thông qua file gói tin infection.pcap. Đây là DNS và các tên miền đã xuất hiện có dấu hiệu liên quan hoặc chứa malware IcedID khi mở file pcap bằng phần mềm WireShark:

→	4 0.175739	10.6.29.101	91.240.202.195	HTTP	738 GET / HTTP/1.1
←	6 0.655266	91.240.202.195	10.6.29.101	HTTP	532 HTTP/1.1 302 Moved Temporarily
	1597 100.976569	10.6.29.101	193.149.129.12	HTTP	345 GET / HTTP/1.1
	2667 102.442757	193.149.129.12	10.6.29.101	HTTP	432 HTTP/1.1 200 OK (application/gzip)

Hình 23. Báo cáo về hoạt động của gói tin với filter là http

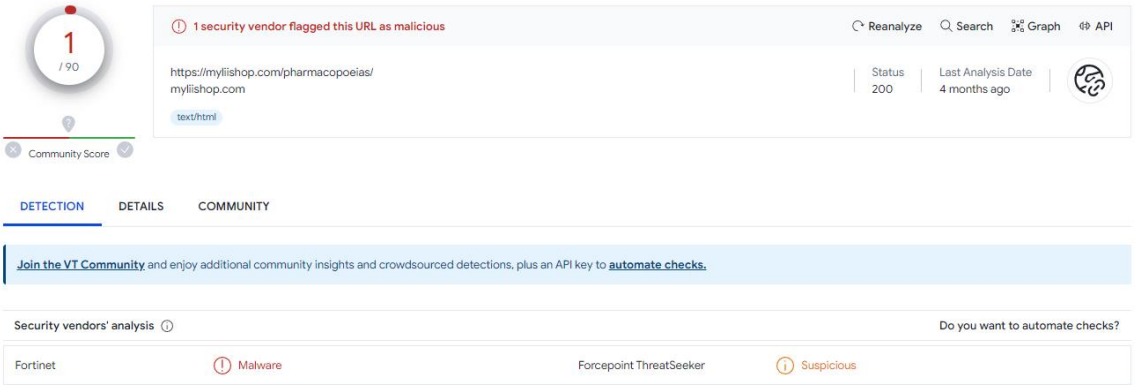
Có một điều ta cần lưu ý rằng những hoạt động này đều sử dụng port mạng là 80 thay vì 443, vì port mạng 443 là cổng hỗ trợ mã hóa kết nối từ máy tính client đến server, nhằm bảo vệ gói dữ liệu đang được truyền đi, từ đó có thể hiểu rằng port 80 đang là port mạng có sự bảo vệ yếu kém hơn so với 443 và ít phổ biến hơn.

Tiếp đến, ta sẽ tìm hiểu chi tiết về thông tin đến từ nguồn IP 91.240.202.19 tiếp theo:

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50059, Seq: 1, Ack: 685, Len: 478
v Hypertext Transfer Protocol
  > HTTP/1.1 302 Moved Temporarily\r\n
    Server: nginx\r\n
    Date: Thu, 29 Jun 2023 04:44:16 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  > Content-Length: 0\r\n
    Connection: keep-alive\r\n
    Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
    Cache-Control: no-store, no-cache, must-revalidate\r\n
    Pragma: no-cache\r\n
    Set-Cookie: PHPSESSID=bnkvs03vg77bm7m78ovdavmlq9; path=/\r\n
    Set-Cookie: _subid=ukiaandutv; expires=Fri, 30-Jun-2023 04:44:16 GMT; Max-Age=86400; path=/\r\n
    Location: https://myliishop.com/pharmacopoeias\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.479527000 seconds]
    [Request in frame: 4]
    [Request URI: http://91.240.202.195/]
```

Hình 24. Thông tin về hoạt động của nguồn IP 91.240.202.19

Có thể thấy rằng địa điểm mà nguồn IP này cung cấp là một địa chỉ URL: https//myliishop.com/pharmacopoeias. Sau khi tiếp tục sử dụng trang web scan malware virustotal.com để đánh giá hoạt động, sau đây là kết quả:



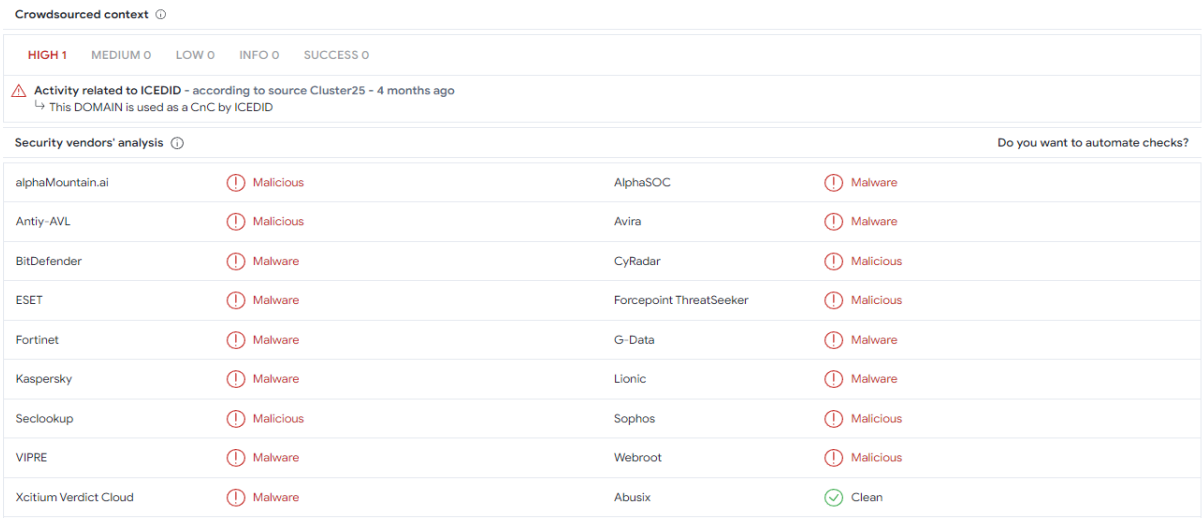
Hình 25. Đánh giá malware của đường link URL: myliishop.com/pharmacopeias

Tuy rằng một đánh giá là thực sự chưa đủ để kết luận rằng đường link này có thật sụ độc hại hay không, nhưng nó cũng phần nào cảnh báo cho mọi người dùng internet cần phải thật sự đề phòng.

Sau phân tích đầu, ta sẽ đến với thông tin đến từ nguồn IP 193.149.129.12:

Hình 26. Thông tin về hoạt động của nguồn IP 193.149.129.12

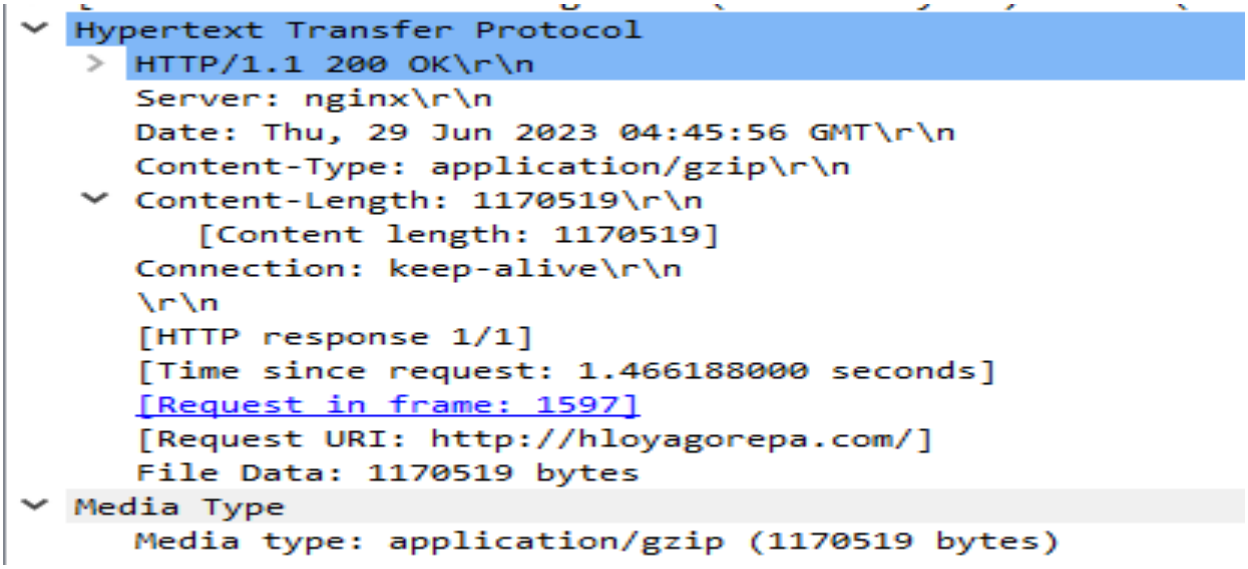
Lần này, nguồn IP lại cho ra một địa chỉ URL khác với host là http://hloyagorepa.com. Ta tiếp tục đánh giá đường link URL này để tìm hiểu về sự an toàn của nó:



Hình 27. Đánh giá malware của đường link URL: http.hloyagorepa.com

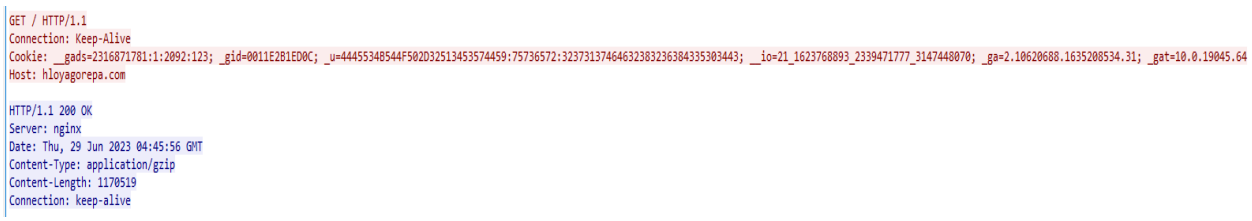
Lần này, đã có rất nhiều đánh giá cảnh báo về sự xuất hiện của malware được đính kèm hoặc có liên quan đến đường link này, thậm chí nó còn được đánh giá nguy hiểm ở mức độ HIGH và có thể hiện rõ sự liên quan của malware IcedID.

Ở thông tin cuối cùng dựa vào filter http, ta thấy được sự xuất hiện của tệp tin gzip binary hay còn được gọi là gzip nhị phân thông qua nguồn IP 10.6.29.101:



Hình 28. Thông tin về hoạt động của nguồn IP 10.6.29.101

Theo như Unit42 đã tổng hợp về quá trình tin tặc sử dụng nhiều phương thức hoạt động để đưa nạn nhân cài đặt file zip, ta nhận biết rằng họ đã cảnh báo về sự xuất hiện của http traffic hay còn được gọi là lưu lượng truy cập http của tệp gzip binary này. Ta tiếp tục dựa vào nguồn IP này cung cấp thông tin và đi thep TCP Stream, ta sẽ nhận được những thông tin tiếp theo:



Hình 29. Thông tin về hoạt động của nguồn IP 10.6.20.101 thông qua việc đi theo TCP Stream

Cookie mà nguồn IP cung cấp có dạng như sau:

__gads=2316871781:1:2092:123;_gid=0011E2B1ED0C;
_u=4445534B544F502D32513453574459:75736572:3237313746463238323638433530344 3;__io=21_1623768893_2339471777_3147448070;
_ga=2.10620688.1635208534.31; _gat=10.0.19045.64

Sau khi cài đặt IcedID có đuôi .exe, gói tin đã tiếp nhận những thông tin mới hơn. Ta sẽ nhập filter mới với dạng (http.request or tls.handshake.type eq 1) and !(ssdp) and ip.addr eq 10.6.29.101 vì tệp file gzip binary giờ đây đã gửi đường truyền đến với một máy chủ server tên gọi là C2:

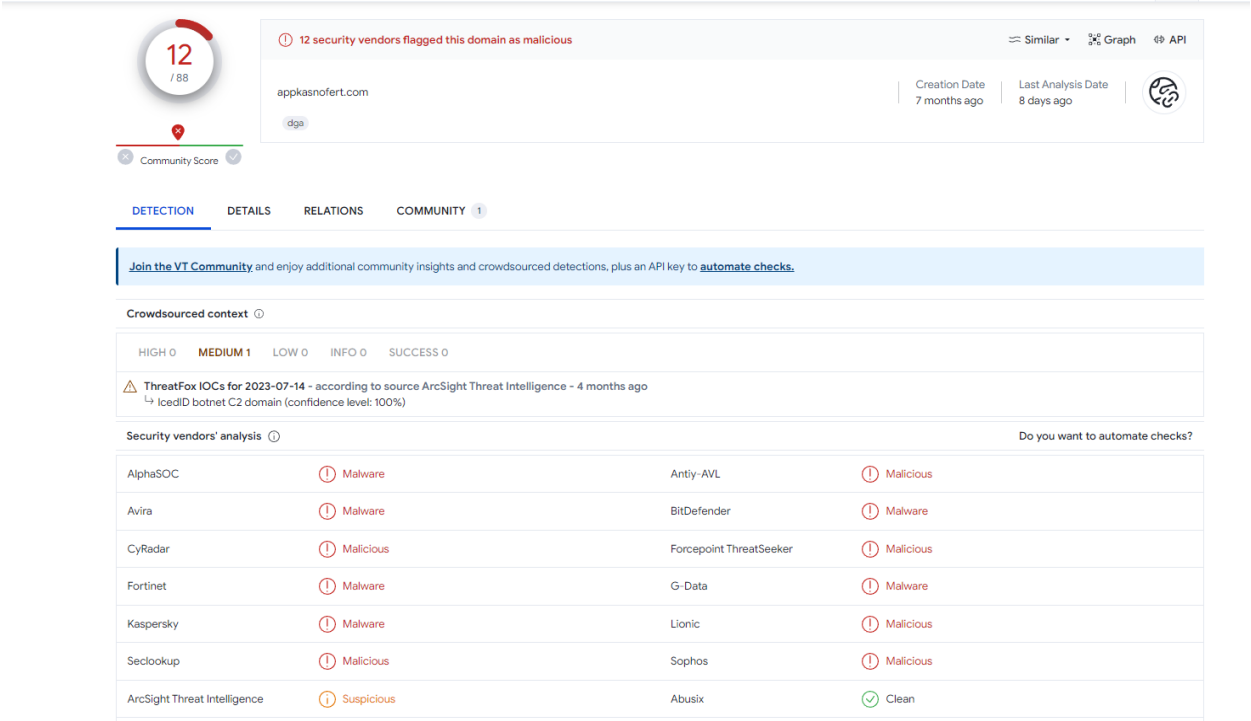
No.	Time	Source	Destination	Protocol	Length	Info
4	0.175739	10.6.29.101	91.240.202.195	HTTP	738	GET / HTTP/1.1
14	1.008613	10.6.29.101	109.234.161.246	TLSv1.3	571	Client Hello
18	1.068759	10.6.29.101	109.234.161.246	TLSv1.3	571	Client Hello
1597	100.976569	10.6.29.101	193.149.129.12	HTTP	345	GET / HTTP/1.1
2678	162.592815	10.6.29.101	192.3.76.146	TLSv1.2	237	Client Hello
2702	464.414973	10.6.29.101	192.3.76.146	TLSv1.2	237	Client Hello

Hình 30. Gzip nhị phân đã gửi và ping đến server C2 của tin tặc

```
▼ Handshake Protocol: Client Hello
0000  00 50 73 7f 18 1c 00 21  5a 33 b9 7c 08 00 45 00   ·Ps····! Z3·|··E·
0010  00 df 49 f7 40 00 80 06  7c 21 0a 06 1d 65 c0 03   ··I·@··· |!···e··
0020  4c 92 c3 94 01 bb 90 87  9c d1 0f d0 6c 6d 50 18   L····... ····lmP·
0030  fa f0 51 a2 00 00 16 03  03 00 b2 01 00 00 ae 03   ··Q····· ········
0040  03 64 9d 0c c2 f9 e2 4f  c6 a9 29 1e 6c 90 74 76   ·d·····O ··)·l·tv
0050  be c7 c6 32 80 f6 a3 e8  28 90 df 22 5d ac 14 4d   ···2···· (··"]··M
0060  47 00 00 26 c0 2c c0 2b  c0 30 c0 2f c0 24 c0 23   G··&·,·+ ·0·/·$·#
0070  c0 28 c0 27 c0 0a c0 09  c0 14 c0 13 00 9d 00 9c   ·('····· ········
0080  00 3d 00 3c 00 35 00 2f  00 0a 01 00 00 5f 00 00   ·=·<·5·/ ·····_··
0090  00 15 00 13 00 00 10 61  70 70 6b 61 73 6e 6f 66   ·······a ppkasnof
00a0  65 72 74 2e 63 6f 6d 00  05 00 05 01 00 00 00 00   ert.com· ········
00b0  00 0a 00 08 00 06 00 1d  00 17 00 18 00 0b 00 02   ········ ········
00c0  01 00 00 0d 00 1a 00 18  08 04 08 05 08 06 04 01   ········ ········
00d0  05 01 02 01 04 03 05 03  02 03 02 02 06 01 06 03   ········ ········
00e0  00 23 00 00 00 17 00 00  ff 01 00 01 00           ·#····· ·····
```

Hình 31. C2 có server là appkasnofert.com

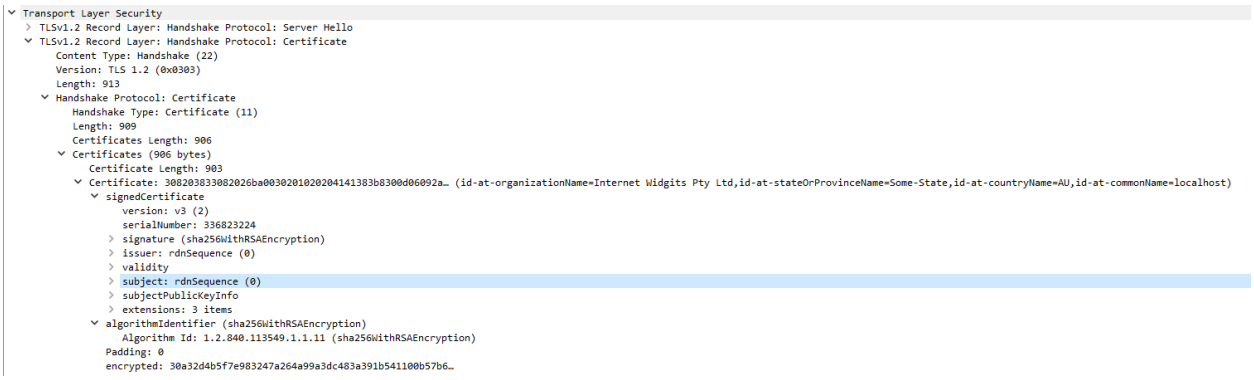
Ta kiểm tra tên miền server này thêm một lần nữa trên virustotal.com, kết quả cho ra là như sau:



Hình 32. Đánh giá malware của tên miền URL: appkasnofert.com

Như vậy có thể thây rằng, IcedID C2 có tên miền domain chính là appkasnofert.com và điều này đã được khẳng định 100%. Không những thế, tên miền này còn chứa rất nhiều đánh giá đến việc sở hữu hoặc có liên quan đến vấn đề bị lây nhiễm hoặc chứa những phần mềm mã độc khác.

Tuy vậy vẫn là chưa đủ so với những gì nhóm chúng em đã tìm hiểu. Để một trang web hợp pháp hoạt động cần bao gồm đầy đủ những yếu tố như domain, thông tin hợp pháp, …. Tên miền domain appkasnofert.com vẫn đầy đủ những yếu tố trên nhưng có một thứ cần được kiểm tra kỹ càng hơn, đó là chứng chỉ của trang web. Để kiểm tra chứng chỉ của tên miền, ta sẽ kiểm tra trong gói tin bằng cách nhập filter là x509sat.uTF8String eq "Internet Widgits Pty Ltd":



Hinh 33. Thông tin về chứng chỉ của tên miền này đã được tin tặc tự tạo ra để luồn lách khỏi các luật lệ, ràng buộc về yêu cầu cần có của một trang web

Tổng quan lại quá trình phân tích gói tin pcap ngày 29/06/2023 thông qua phần mềm WireShark, nhóm chúng em đưa ra kết luận như sau:

Dựa vào những báo cáo về khả năng bảo mật và an toàn của trang web virustotal.com , có thể thấy rằng đây là những trang web có xuất hiện hoặc liên quan trong quá trình thu thập dữ liệu gói tin đều chứa malware độc hại và đã bị đánh giá là liên quan đến những thủ thuật lừa đảo như phising

Tên của người dùng sử dụng thiết bị là user

IP của thiết bị bị ảnh hưởng bởi IcedID: 10.6.29.101

Tên của thiết bị bị ảnh hưởng bởi IcedID: DESKTOP-2Q4SWDY

CHƯƠNG IV: TỔNG QUAN ĐỒ ÁN

Thông qua việc kiểm tra và xác định hành vi của malware độc hại IcedID dựa trên file pcap ngày 29/06/2023, nhóm của chúng em rút ra được những vấn đề quan trọng sau đây:

- IcedID là một phần mềm mã độc vô cùng nguy hiểm đến người dùng bởi chúng luôn được cập nhật theo thời gian một cách liên tục
- Phương thức hoạt động nhằm phán tán malware này vào máy tính nạn nhân rất tinh vi và cần phải có kinh nghiệm và kĩ năng tin học chuyên sâu để nhận biết và phòng tránh những thông tin rác hoặc tập tin rác được gửi đến
- IcedID có thể được kết hợp phương thức hoạt động của chúng đồng thời với một số malware khác, khiến cho việc ngăn chặn và bảo vệ máy tính, dữ liệu, thông tin cá nhân ngày một khó khăn

Không chỉ riêng IcedID mà còn rất nhiều phần mềm mã độc khác còn nguy hiểm hơn, có thể gây ra được những tổn thất lớn hơn không chỉ về mặt tài chính và còn về mặt bảo mật, an ninh của quốc gia. Việc các hacker ngày một học hỏi được thêm nhiều thủ thuật mới cũng như sự phát triển vượt bậc của trí tuệ nhân tạo AI đã trở thành một rào cản không hề nhỏ về vấn đề bảo mật máy tính của người dùng đối với chúng. IcedID là một ví dụ điển hình và vẫn đang là một lời cảnh tỉnh cho những người sử dụng mạng máy tính nhưng hiếm khi hoặc không bao giờ kiểm tra kỹ những thông tin hoặc tin nhắn, mail, những cuộc điện thoại,... được nhận bởi những kẻ xấu với mục đích cá nhân quy mô nhỏ hoặc lớn. Chính vì vậy, người dùng cần phải có sự nhận thức rõ ràng và cần phải để ý, quan trọng việc nhận những thông tin từ người lạ khác hoặc đơn giản hơn là bắt đầu bảo mật, an ninh thiết bị của mình thông qua việc cài những ứng dụng, phần mềm antivirus như McAfee,... và backup, sao lưu dữ liệu của bản thân mình sang những thiết bị có thể cắm rời như ổ cứng.

KẾT LUẬN

Xuyên suốt quá trình học tập và làm đồ án bộ môn Điều tra tấn công, nhóm chúng em nhận thấy rằng bản thân đã học hỏi và tiếp thu được nhiều kiến thức không chỉ bởi giảng viên bộ môn là thầy Phạm Đình Thắng, mà chúng em còn được tìm hiểu nhiều hơn thông qua bạn bè cùng chuyên ngành và các nguồn thông tin khác tin cậy trên mạng. Nhóm chúng em cũng nhận thấy rằng bản thân cần phải cố gắng nhiều hơn trong môn học này, không chỉ để đạt được thành tích cao mà còn phát triển và áp dụng qua những môn học khác có liên quan đến An Ninh Mạng. Trong tương lai, chúng em sẽ cố gắng phát huy để có được bài báo cáo đồ án hoàn thiện nhất cũng như có thêm nhiều sự hiểu biết và kinh nghiệm trong việc thực hiện và thực hành đồ án một cách thực tế nhất.

BẢNG PHÂN CÔNG CÔNG VIỆC

HỌ VÀ TÊN	MSSV	CÔNG VIỆC
Trần Ngọc Vinh	21DH113413	Phân tích, đánh giá, báo cáo về toàn bộ lịch sử và quá trình hoạt động của IcedID thông qua pcap, hỗ trợ phần kết luận
Lê Thành Ân	21DH112304	Tìm hiểu và hoàn thành lý thuyết tổng quan, hỗ trợ phần kết luận
Nguyễn Hoàng Phúc	21DH114014	Tìm hiểu và hoàn thành tổng quan đồ án, hoàn thiện phần kết luận

TÀI LIỆU THAM KHẢO: REDDIT, YOUTUBE VÀ CÁC NGUỒN TIN CẬY TRÊN UNIT42 (KHÔNG BAO GỒM CÁC CÔNG CỤ AI)