

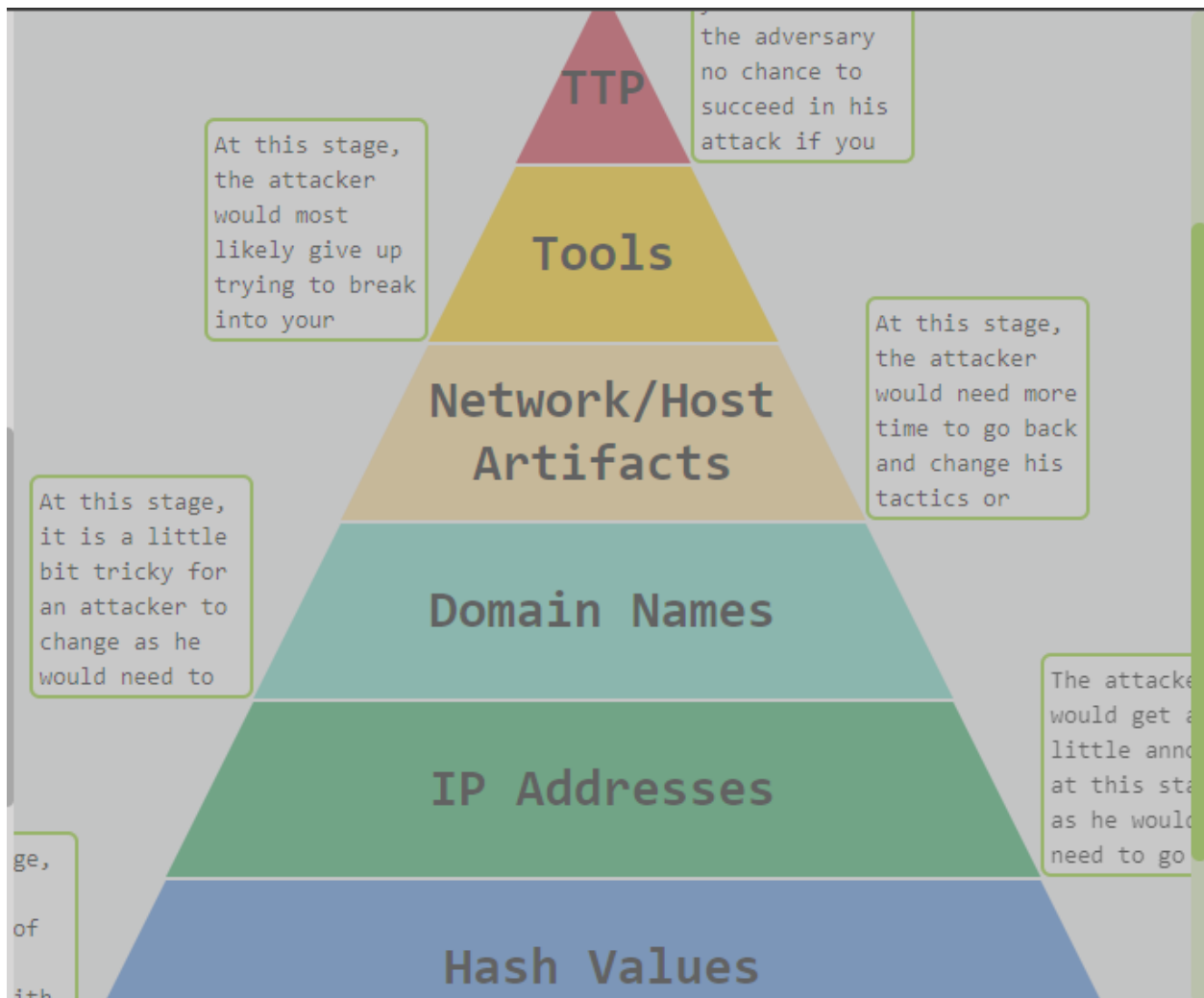


Pyramid Of Pain

-Để Tọa-

I. Over view

Understanding the Pyramid of Pain concept as a Threat Hunter, Incident Responder, or SOC Analyst is important.



II. Theory

1.Hash Values (Trivial)

Theo Microsoft, giá trị băm là giá trị số có độ dài cố định , giúp xác định duy nhất dữ liệu. Giá trị băm là kết quả của thuật toán băm. Sau đây là một số thuật toán băm phổ biến nhất:

- **MD5 (Message Digest, được xác định bởi RFC 1321)** - được thiết kế bởi Ron Rivest vào năm 1992 và là hàm băm mật mã được sử dụng rộng rãi với giá trị băm 128 bit. BămMD5 **KHÔNG** được coi là **an toàn về mặt mật mã**. Vào năm 2011,IETF đã xuất bản RFC 6151, "Cân nhắc bảo mật được cập nhật cho Thông báo MD5 và Thuật toán HMAC-MD5", trong đó đề cập đến một số cuộc tấn công chống lại MD5, bao gồm cả xung đột băm.

- **SHA-1 (Thuật toán băm an toàn 1, được xác định bởi RFC 3174)** - được Cơ quan An ninh Quốc gia Hoa Kỳ phát minh vào năm 1995. Khi dữ liệu được đưa vào Thuật toán băm SHA-1, SHA-1 nhận đầu vào và tạo ra hàm băm 160 bit chuỗi giá trị dưới dạng số thập lục phân gồm 40 chữ số. NIST đã không chấp nhận việc sử dụng SHA-1 vào năm 2011 và cấm sử dụng nó cho chữ ký số vào cuối năm 2013 do nó dễ bị brute-force attacks. Thay vào đó, NIST khuyên bạn nên chuyển từ SHA-1 sang các thuật toán băm mạnh hơn trong nhóm SHA-2 và SHA-3.
- **The SHA-2 (Secure Hash Algorithm 2)** - Thuật toán băm SHA-2 được Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) và Cơ quan An ninh Quốc gia (NSA) thiết kế vào năm 2001 để thay thế SHA-1. SHA-2 có nhiều biến thể và được cho là phổ biến nhất là SHA-256. Thuật toán SHA-256 trả về giá trị băm 256 bit dưới dạng số thập lục phân gồm 64 chữ số.

Hàm băm không được coi là an toàn về mặt mật mã nếu hai tệp có cùng giá trị băm hoặc thông báo.

- Các chuyên gia bảo mật thường sử dụng các giá trị băm để hiểu rõ hơn về một mẫu phần mềm độc hại cụ thể, một tệp độc hại hoặc đáng ngờ, đồng thời như một cách để xác định và tham chiếu duy nhất đến tạo phẩm độc hại.

Questions And Answers

Analyse the report associated with the hash

"b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d" [here](#). What is the filename of the sample?

Sales_Receipt 5606.xls

2. IP Address (Easy)

Bạn có thể đã biết được tầm quan trọng của Địa chỉ IP từ phần "Mạng là gì?" Phòng_.

Tầm quan trọng của Địa chỉ IP. Địa chỉ IP được sử dụng để xác định bất kỳ thiết bị nào được kết nối với mạng. Những thiết bị này bao gồm từ máy tính để bàn, máy chủ và thậm chí cả camera quan sát! Chúng ta dựa vào địa chỉ IP để gửi và nhận thông tin qua mạng. Nhưng chúng ta sẽ không đi sâu vào cấu trúc và chức năng của địa chỉ IP. Là một phần của Pyramid of Pain, chúng ta sẽ đánh giá cách sử dụng địa chỉ IP làm chỉ báo.

Trong Pyramid of Pain, địa chỉ IP được biểu thị bằng màu xanh lục. Bạn có thể hỏi tại sao và bạn có thể kết hợp màu xanh lá cây với cái gì?

Từ quan điểm quốc phòng, kiến thức về địa chỉ IP mà đối thủ sử dụng có thể có giá trị. Một chiến thuật phòng thủ phổ biến là **chặn, loại bỏ** hoặc **từ chối** các yêu cầu gửi đến từ các địa chỉ IP trên thông số hoặc tường lửa bên ngoài của bạn. Chiến thuật này thường không có khả năng chống đạn vì đối thủ có kinh nghiệm có thể phục hồi chỉ bằng cách sử dụng địa chỉ IP công cộng mới là điều tầm thường.

Kết nối IP độc hại ([app.any.run](#)):

HTTP Requests 0		Connections 4		DNS Requests 4		Threats 0	
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port
85528 ms	TCP	⚠	1632	some_malicious_file.bi...		50.87.136.52	443
144.95 s	TCP	?	1632	some_malicious_file.bi...		78.46.1.42	443
205.35 s	TCP	⚠	1632	some_malicious_file.bi...		134.119.253.108	443
264.76 s	TCP	⚠	1632	some_malicious_file.bi...		104.21.87.185	443

GHI CHÚ! Đừng cố gắng tương tác với các địa chỉ IP được hiển thị ở trên.

Một trong những cách mà kẻ thù có thể gây khó khăn cho việc thực hiện chặn IP thành công là sử dụng **Fast Flux** .

Theo [Akamai](#) , Fast Flux là một kỹ thuật DNS được các botnet sử dụng để ẩn các hoạt động lừa đảo, proxy web, phân phối phần mềm độc hại và các hoạt động giao tiếp phần mềm độc hại đằng sau các máy chủ bị xâm nhập hoạt động như proxy. Mục đích của việc sử dụng mạng Fast Flux là khiến việc liên lạc giữa phần mềm độc hại và máy chủ chỉ huy và kiểm soát (C&C) của nó trở nên khó bị các chuyên gia bảo mật phát hiện.

Vì vậy, khái niệm chính của mạng Fast Flux là có nhiều địa chỉ IP được liên kết với một tên miền và địa chỉ này liên tục thay đổi. Palo Alto đã tạo ra một kịch bản hư cấu tuyệt vời để giải thích Fast Flux: "[Fast Flux 101: Cách tội phạm mạng cải thiện khả năng phục hồi của cơ sở hạ tầng của chúng để trốn tránh sự phát hiện và triệt phá của cơ quan thực thi pháp luật](#)"

Questions And Answers

Read the following [report](#) to answer this question. What is the first IP address the malicious process (PID 1632) attempts to communicate with?

50.87.136.52

Read the following [report](#) to answer this question. What is the first domain name the malicious process ((PID 1632) attempts to communicate with?

[craftingalegacy.com](#)






























3. Domain Names (Simple)

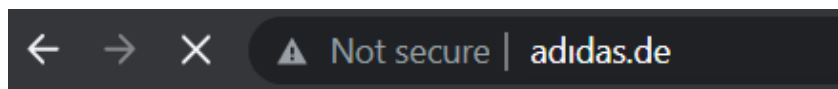
Hãy bước lên Pyramid of Pain và chuyển sang Domain. Bạn có thể thấy sự chuyển đổi màu sắc - từ xanh lục sang xanh mòng kết.

Domain có thể được coi đơn giản là ánh xạ địa chỉ IP thành một chuỗi văn bản. Domain có thể chứa một miền và một miền cấp cao nhất (evilcorp.com) hoặc một miền phụ theo sau là một miền và miền cấp cao nhất (tryhackme.evilcorp.com). Nhưng chúng ta sẽ không đi sâu vào chi tiết cách thức hoạt động của Hệ thống tên miền (DNS). Bạn có thể tìm hiểu thêm về DNS trong [Phòng "Chi tiết về DNS"](#) này .

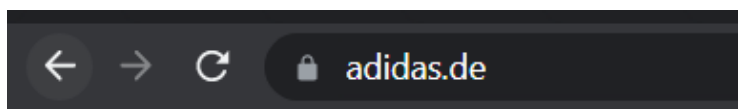
Tên miền có thể gây khó khăn hơn một chút cho kẻ tấn công khi thay đổi vì rất có thể **chúng sẽ cần mua miền, đăng ký và sửa đổi bản ghi DNS** . Thật không may cho những người bảo vệ, nhiều nhà cung cấp DNS có các tiêu chuẩn lỏng lẻo và cung cấp API để giúp kẻ tấn công thay đổi tên miền dễ dàng hơn.

Các miền Sodinokibi **C2 (Cơ sở hạ tầng chỉ huy và kiểm soát) độc hại** :

Campaign		8254	
C2	boisehosting.net	 fotoideaymedia.es	
	dubnew.com	 stallbyggen.se	
	koken-voor-baby.nl	 juneauopioidworkgroup.org	
	vancouver-print.ca	 zewatchers.com	
	bouquet-de-roses.com	 seevilla-dr-sturm.at	
	olejack.ru	 i-trust.dk	
	wasmachtmeinfonds.at	 appsformacpc.com	
	friendsandbrgrs.com	 thenewrejuveme.com	
	xn--singlebrsen-vergleich-nec.com	 sabel-bf.com	
	seminoc.com	 ceres.org.au	
	cursoporcelanatoliquido.online	 mariettearnoudts.nl	
	tastewilliamsburg.com	 charlottepoudroux-photographie.fr	
	aselbermachen.com	 klimt2012.info	
	accountancywijchen.nl	 creamery201.com	
	nerekatu.com	 makeurvoiceheard.com	



Bạn có thể phát hiện ra điều gì độc hại trong ảnh chụp màn hình ở trên không? Bây giờ, hãy so sánh nó với chế độ xem trang web hợp pháp bên dưới:



Đây là một trong những ví dụ về cuộc tấn công **Punycode** được những kẻ tấn công sử dụng để chuyển hướng người dùng đến một miền độc hại thoát nhìn có vẻ hợp pháp.

Punycode là gì? Theo Wandera , "Punycode là một cách chuyển đổi các từ không thể viết bằng ASCII thành mã hóa Unicode ASCII."

Những gì bạn thấy trong URL ở trên `adidas.de` có mã Punycode là `http://xn--addas-04a.de/`

Internet Explorer, Google Chrome, Microsoft Edge và Apple Safari hiện khá giỏi trong việc dịch các ký tự bị xáo trộn thành tên miền Punycode đầy đủ.

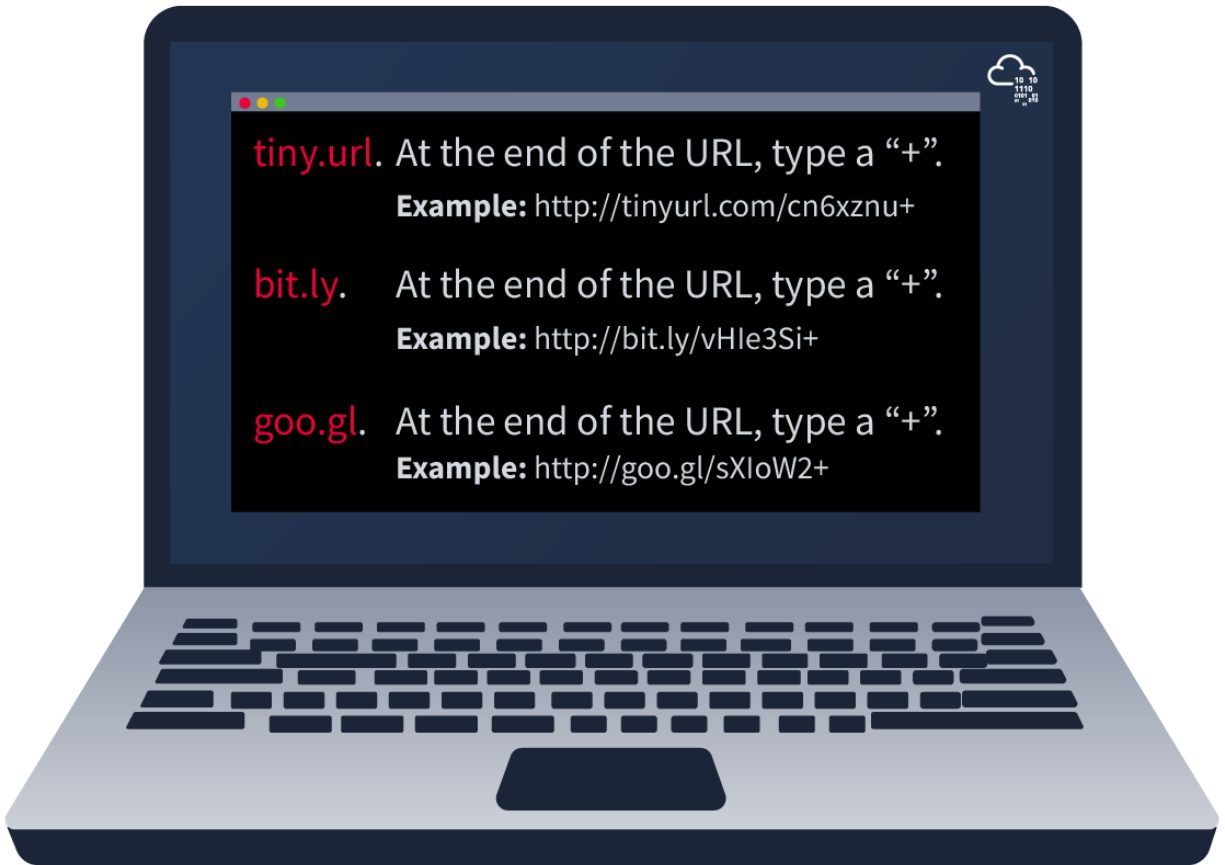
Để phát hiện các miền độc hại, có thể sử dụng nhật ký proxy hoặc nhật ký máy chủ web.

Những kẻ tấn công thường ẩn các miền độc hại trong **Công cụ rút ngắn URL**. URL Shortener là một công cụ tạo một URL ngắn và duy nhất sẽ chuyển hướng đến trang web cụ thể được chỉ định trong bước đầu tiên thiết lập liên kết URL Shortener. Theo Cofense , kẻ tấn công sử dụng các dịch vụ Rút ngắn URL sau để tạo liên kết độc hại:

- bit.ly
- goo.gl
- ow.ly
- s.id
- smarturl.it
- tiny.pl
- tinyurl.com
- x.co

Bạn có thể xem trang web thực tế mà liên kết rút gọn đang chuyển hướng bạn đến bằng cách thêm dấu "+" vào đó (xem ví dụ bên dưới). Nhập URL rút gọn vào thanh địa chỉ của trình duyệt web và thêm các ký tự trên để xem URL chuyển hướng.

LƯU Ý: Các ví dụ về các liên kết rút gọn bên dưới không tồn tại.



Xem kết nối trong Any.run:

Vì Any.run là dịch vụ hộp cát thực thi mẫu nên chúng tôi có thể xem xét mọi kết nối như yêu cầu HTTP , yêu cầu DNS hoặc các quy trình giao tiếp với địa chỉ IP. Để làm như vậy, chúng ta có thể xem tab "kết nối mạng" nằm ngay bên dưới ảnh chụp nhanh của máy.

HTTP Request:

Tab này hiển thị các yêu cầu HTTP được ghi lại kể từ khi mẫu được phát hiện. Điều này có thể hữu ích để xem tài nguyên nào đang được truy xuất từ máy chủ web, chẳng hạn như trình nhả giọt hoặc lệnh gọi lại.

HTTP Requests 7 Connections 51 DNS Requests 20 Threats 0									
Filter by PID, name or url									
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content	PCAP
NETWORK	25853 ms	GET 204: No Content	✓	2572	chrome.exe		http://www.gstatic.com/generate_204	–	
	44576 ms	GET 200: OK	✓	2572	chrome.exe		http://cldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl cab...	62.3 Kb ↓ compressed	
FILES	76052 ms	HEAD 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERYWQY...	–	
	81155 ms	GET 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/YGkwa4MXjfWSuERYWQY...	3.72 Kb ↓ binary	
	105.77 s	HEAD 200: OK	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zfhpi3roq46nymxtbz...	3.72 Kb ↓ crx	
	105.77 s	GET 206: Partial Con...	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zfhpi3roq46nymxtbz...	7.13 Kb ↓ binary	
DEBUG	110.88 s	GET 206: Partial Con...	✓	852	svchost.exe		http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/eua6zfhpi3roq46nymxtbz...	3.11 Kb ↓ binary	

Kết nối:

Tab này hiển thị mọi thông tin liên lạc được thực hiện kể từ khi mẫu được phát hiện. Điều này có thể hữu ích để xem liệu một tiến trình có giao tiếp với một máy chủ khác hay không. Ví dụ: đây có thể là lưu lượng truy cập C2, tải lên/tải xuống tệp qua FTP, v.v.

HTTP Requests 7 Connections 51 DNS Requests 20 Threats 0									
Filter by PID, domain, name or ip									
	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Traffic
NETWORK	1309 ms	UDP	✓	4	System		192.168.100.255	138	↑ 2.21 Kb ↓
	1312 ms	UDP	✓	1076	svchost.exe		224.0.0.252	5355	↑ 48 b ↓
	1314 ms	UDP	✓	3740	svchost.exe		239.255.255.250	1900	↑ 1.41 Kb ↓
FILES	1315 ms	UDP	✓	4	System		192.168.100.255	137	↑ 1.70 Kb ↓
	4397 ms	UDP	✓	1076	svchost.exe		224.0.0.252	5355	↑ 44 b ↓
	4399 ms	UDP	✓	1076	svchost.exe		224.0.0.252	5355	↑ 48 b ↓
	4405 ms	UDP	✓	2044	chrome.exe		239.255.255.250	1900	↑ 696 b ↓
DEBUG	4408 ms	UDP	✓	1076	svchost.exe		224.0.0.252	5355	↑ 44 b ↓
	5412 ms	TCP	✗	2572	chrome.exe		142.250.185.173	443	No Data
	5573 ms	TCP	✓	2572	chrome.exe		142.250.186.142	443	↑ 1.02 Kb ↓ 8.64 Kb

DNS Request:

Tab này hiển thị các yêu cầu DNS được thực hiện kể từ khi mẫu được phát hiện. Phần mềm độc hại thường thực hiện các yêu cầu DNS để kiểm tra kết nối internet (Tức là nếu Nó không thể truy cập internet/gọi về nhà thì có thể nó đã bị sandbox hoặc vô dụng).

HTTP Requests 7 Connections 51 DNS Requests 20 Threats 0				
Filter by IP or domain				
	Timeshift	Status	Rep	Domain
NETWORK	5371 ms	Responded	?	ice-eng.app.box.com
	5373 ms	Responded	✓	accounts.google.com
FILES	5373 ms	Responded	✓	clients2.google.com
	5374 ms	Responded	✓	clients2.googleusercontent.com
	11478 ms	Responded	✓	ssl.gstatic.com
DEBUG	25794 ms	Responded	✓	www.gstatic.com
	27799 ms	Responded	✓	cdn01.boxcdn.net
	29500 ms	Responded	✓	cdn.amplitude.com

Questions And Answers

Go to [this report on app.any.run](#) and provide the first suspicious URL request you are seeing, you will be using this report to answer the remaining questions of this task.

[craftingalegacy.com](#)

What term refers to an address used to access websites?

Domain Name

What type of attack uses Unicode characters in the domain name to imitate the a known domain?

Punycode attack

Provide the redirected website for the shortened URL using a preview: <https://tinyurl.com/bw7t8p4u>

<https://tryhackme.com/>



4. Host Artifacts (Annoying)

Hãy tiến thêm một bước nữa tới vùng màu vàng.

Ở cấp độ này, kẻ tấn công sẽ cảm thấy khó chịu và bức bối hơn một chút nếu chúng ta có thể phát hiện ra cuộc tấn công. Kẻ tấn công sẽ cần phải quay lại mức phát hiện này và thay đổi các công cụ cũng như phương pháp tấn công của mình. Điều này rất tốn thời gian đối với kẻ tấn công và có lẽ anh ta sẽ cần phải dành nhiều tài nguyên hơn cho các công cụ của đối thủ.

Các thao tác trên máy chủ là các dấu vết hoặc có thể quan sát được mà kẻ tấn công để lại trên hệ thống, chẳng hạn như giá trị registry, quá trình thực thi quy trình đáng ngờ, kiểu tấn công hoặc IOC (Indicators of Compromise), các tệp do ứng dụng độc hại đánh rơi hoặc bất kỳ thứ gì độc quyền đối với mối đe dọa hiện tại.

Suspicious process execution from Word:

 WINWORD.EXE	0.01	51,500 K	134,300 K	3640 Microsoft Word	Microsoft Corporation
 api-ms-win-downlevel-user32-l1-...		4,632 K	11,192 K	3300 EffectDemo MFC Application	

Suspicious events followed by opening a malicious application:

Time o...	Process Name	PID	Operation	Path	Result
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3/24/26...	Powershell.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14f\G_jugk.exe	SUCCESS
3/24/26...	Powershell.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS

The files modified/dropped by the malicious actor:

2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exe	MD5: CC11BFD14D6ECC83477B69FF06C6C587	SHA256: A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AEF01A6DA	tlb
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~\$O-100120 CDW-102220.doc	MD5: 2E7A3442236F2D50C669BC79188BBD69	SHA256: BF007001BACF8F6ABF371B0B2797B7D13B741879E1E5B76FB616A934318418A9	pgc
3828	Powershell.exe	C:\Users\admin\Jehhzda\Ben14f\G_jugk.exe	MD5: 92F58C4E2F524EC53EBE10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAAAF140B98B64329BD05878BC13671FA916F423710	executable
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe	MD5: 92F58C4E2F524EC53EBE10D914D96CCB	SHA256: 4A9E32BC5348265C43945ADAAAF140B98B64329BD05878BC13671FA916F423710	executable

Question and Answers:

1. A process named regidle.exe makes a POST request to an IP address based in the United States (US) on port 8080. What is the IP address?

96.126.101.6

- Đi đến địa chỉ: <https://assets.tryhackme.com/additional/pyramidofpain/task5-report.pdf>
- Tìm process có tên là regidle, có thể tìm nhanh bằng cách sử dụng ctrl+ F

task5-report.pdf 39 / 51 125% +

regidle.exe 36/109

HTTP(S) requests: 18 TCP/UDP connections: 25 DNS requests: 4 Threats: 27

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3164	regidle.exe	POST	--	200.116.145.225	http://200.116.145.225:443/x4VtVzvRbVfYB/kqQ2AK6eEV	CO	--	--	malicious
3164	regidle.exe	POST	--	96.126.101.6	http://96.126.101.6:8080/VdPvH/OUmWdFVBXpU7L/vvWud	US	--	--	malicious
3828	Powershell.exe	GET	404	69.65.3.162	http://eubanks7.com/administrator/ubd08/	US	html	315 b	suspicious
3828	Powershell.exe	GET	200	35.214.215.33	http://ldoraggodisole.it/cg-bin/zL6879/	US	executable	368 Kb	malicious
3164	regidle.exe	POST	404	5.196.108.185	http://5.196.108.185:8080/VznUAWLqIqARcFNv/EWHCK	FR	html	564 b	malicious
3164	regidle.exe	POST	--	167.114.153.111	http://167.114.153.111:8080/OxYV/Bzg2soY5SR/jk8008e/	CA	--	--	malicious
3164	regidle.exe	POST	--	194.187.133.160	http://194.187.133.160:443/Nqdlz/w2BG/	BG	--	--	malicious
3164	regidle.exe	POST	--	103.86.49.11	http://103.86.49.11:8080/VdQpXmgEhauu/AfEp/Q9Qn2/	TH	--	--	malicious
3164	regidle.exe	POST	--	98.174.164.72	http://98.174.164.72:ghMuzyNcNWN/kMmYdVthaeVj/c2fe	US	--	--	malicious

2. The actor drops a malicious executable (EXE). What is the name of this executable?

G_jugk.exe

- Tiếp tục sử dụng filter: drop + tìm kiếm nhanh: ctrl + F:

MALICIOUS	SUSPICIOUS	INFO
<p>Application was dropped or rewritten from another process</p> <ul style="list-style-type: none"> • regidle.exe (PID: 3164) • G_jugk.exe (PID: 1640) <p>EMOTET was detected</p> <ul style="list-style-type: none"> • regidle.exe (PID: 3164) <p>Drops executable file immediately after starts</p> <ul style="list-style-type: none"> • G_jugk.exe (PID: 1640) <p>Connects to CnC server</p> <ul style="list-style-type: none"> • regidle.exe (PID: 3164) 	<p>Checks supported languages</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) • regidle.exe (PID: 3164) • G_jugk.exe (PID: 1640) <p>Reads the computer name</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) • regidle.exe (PID: 3164) • G_jugk.exe (PID: 1640) <p>Reads the date of Windows installation</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) <p>PowerShell script executed</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) <p>Creates files in the user directory</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) <p>Reads Environment values</p> <ul style="list-style-type: none"> • Powershell.exe (PID: 3828) <p>Executed via WMI</p>	<p>Reads the computer name</p> <ul style="list-style-type: none"> • WINWORD.EXE (PID: 2728) <p>Creates files in the user directory</p> <ul style="list-style-type: none"> • WINWORD.EXE (PID: 2728) <p>Checks supported languages</p> <ul style="list-style-type: none"> • WINWORD.EXE (PID: 2728) <p>Reads mouse settings</p> <ul style="list-style-type: none"> • WINWORD.EXE (PID: 2728) <p>Reads Microsoft Office registry keys</p> <ul style="list-style-type: none"> • WINWORD.EXE (PID: 2728)

3. Look at this report by Virustotal. How many vendors determine this host to be malicious?

9

Đây là các chuỗi Tác nhân người dùng phổ biến nhất được tìm thấy cho Trojan Emotet Downloader

Nếu bạn có thể phát hiện các chuỗi Tác nhân người dùng tùy chỉnh mà kẻ tấn công đang sử dụng, bạn có thể chặn chúng, tạo ra nhiều trở ngại hơn và khiến nỗ lực xâm phạm mạng của chúng trở nên khó chịu hơn.

Question and Answer:

What browser uses the User-Agent string shown in the screenshot above?

- Copy chuỗi trên rồi search xem nó sử dụng browser nào
Internet Explorer

How many POST requests are in the screenshot from the pcap file?

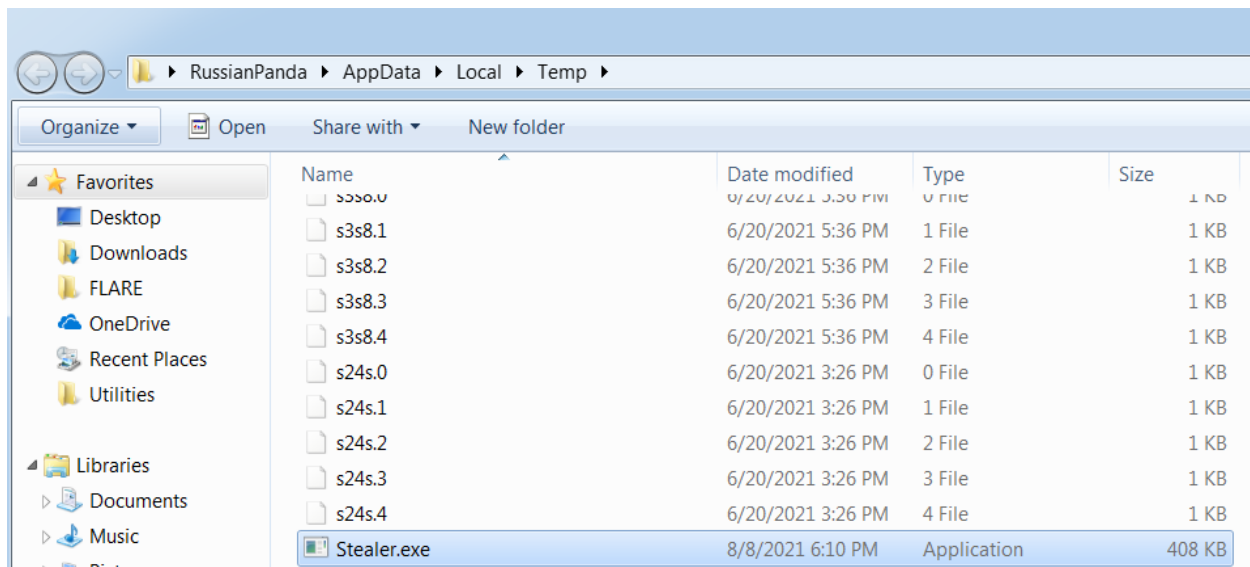
6

6. Tools (Challenging)

Ở giai đoạn này, chúng ta đã nâng cao khả năng phát hiện của mình đối với các hiện vật. Kẻ tấn công rất có thể sẽ từ bỏ việc cố gắng đột nhập vào mạng của bạn hoặc quay lại và cố gắng tạo một công cụ mới phục vụ cùng mục đích. Đây sẽ là end game đối với những kẻ tấn công vì chúng cần đầu tư một số tiền vào việc xây dựng một công cụ mới (nếu chúng có khả năng làm như vậy), tìm công cụ có cùng tiềm năng hoặc thậm chí được đào tạo để học cách sử dụng. thành thạo một công cụ nào đó.

Những kẻ tấn công sẽ sử dụng các tiện ích này để tạo tài liệu macro độc hại (maldocs) cho các nỗ lực lừa đảo, một backdoor có thể được sử dụng để thiết lập C2 (Cơ sở hạ tầng chỉ huy và kiểm soát), mọi tệp .EXE tùy chỉnh và . Tệp DLL , tải trọng hoặc trình bẻ khóa mật khẩu.

Một Trojan đã thả "Stealer.exe" đáng ngờ vào thư mục Temp:



Việc thực thi nhĩ phân đáng ngờ:

payload.exe	1356	12.09 MB	WIN-31...\RussianPanda
Stealer.exe	2928	11.63 MB	WIN-31...\RussianPanda Galactus

Chữ ký chống vi-rút, quy tắc phát hiện và quy tắc YARA có thể là vũ khí tuyệt vời để bạn sử dụng để chống lại những kẻ tấn công ở giai đoạn này.

MalwareBazaar và Malshare là những tài nguyên tốt để cung cấp cho bạn quyền truy cập vào các mẫu, nguồn cấp dữ liệu độc hại và kết quả YARA - tất cả những thứ này đều có thể rất hữu ích khi tìm kiếm mối đe dọa và ứng phó sự cố.

Đối với các quy tắc phát hiện, Thị trường phát hiện mối đe dọa SOC Prime là một nền tảng tuyệt vời, nơi các chuyên gia bảo mật chia sẻ các quy tắc phát hiện của họ đối với các loại mối đe dọa khác nhau, bao gồm cả CVE mới nhất đang bị kẻ thù khai thác một cách tự nhiên.

Băm mờ cũng là một vũ khí mạnh chống lại các công cụ của kẻ tấn công. Băm mờ giúp bạn thực hiện phân tích sự giống nhau - khớp hai tệp có khác biệt nhỏ dựa trên giá trị băm mờ. Một trong những ví dụ về băm mờ là việc sử dụng SSDeep; trên trang web chính thức của SSDeep, bạn cũng có thể tìm thấy lời giải thích đầy đủ về hàm băm mờ.

Ví dụ về SSDeep từ VirusTotal:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 13+
Basic Properties ⓘ				
MD5	9498ff82a64ff445398c8426ed63ea5b			
SHA-1	36f9ca40b3ce96fcee1cf1d4a7222935536fd25b			
SHA-256	8b2e701e91101955c73865589a4c72999aeabc11043f712e05fdb1c17c4ab19a			
Vhash	025056657d755510804011z9005b9z25z12z3afz			
Authentihash	ad56160b465f7bd1e7568640397f01fc4f8819ce6f0c1415690ecee646464cec			
Imphash	d7584447a5c5ca9b4a55946317137951			
Rich PE header hash	fa4dbca9180170710b3c245464efa483			
SSDEEP	6144:Gz90qLc1zR98hUb4UdjzEwG+vgAWiR4EXePbix67CNzjX:Gz90qLc1WhUbhVqJPbiQ7CNzb			
TLSH	T1DB44CF267660D833D0DF94316C75C3F9673BFC2123215A6B6A4417699E307E0AE7839E			
File type	Win32 EXE			
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit			
TrID	Win32 Executable MS Visual C++ (generic) (48.8%)			
TrID	Win64 Executable (generic) (16.4%)			
TrID	Win32 Dynamic Link Library (generic) (10.2%)			
TrID	Win16 NE executable (generic) (7.8%)			
TrID	Win32 Executable (generic) (7%)			
File size	249.00 KB (254976 bytes)			

Question and Answer

Provide the method used to determine similarity between the files

Fuzzy hashing

Provide the alternative name for fuzzy hashes without the abbreviation

- Vào trang của SSDeep, ta có thể tìm thấy được tên của nó

ssdeep Project | ssdeep - Fuzzy hashing program

Home Download Quick Start Demo Documentation Go to GitHub

Introduction

ssdeep is a program for computing [context triggered piecewise hashes](#) (CTPH). Also called fuzzy hashes, CTPH can match inputs that have homologies. Such inputs have sequences of identical bytes in the same order, although bytes in between these sequences may be different in both content and length.

A complete explanation of CTPH can be found in [Identifying almost identical files using context triggered piecewise hashing](#) from the journal Digital Investigation. There is a free version of this paper available through the Digital Forensic Research Workshop conference, [free version of Identifying almost identical files using context triggered piecewise hashing](#).

It also provides a library (libfuzzy) to generate/compare fuzzy hashes.

ssdeep hashes are now widely used for simple identification purposes. (e.g. Basic Properties section in [VirusTotal](#)) Although "better fuzzy hashes" are available, ssdeep is still one of the primary choices because of its speed (now about twice as fast as TLSH) and being a de facto standard.

Platforms

context triggered piecewise hashes

7. TTPs (Tough)

Nó vẫn chưa hết. Nhưng tin tốt là chúng tôi đã đến được giai đoạn cuối cùng hoặc đỉnh của Pyramid of Pain!

TTP (Tactics, Techniques & Procedures) là viết tắt của Chiến thuật, Kỹ thuật & Thủ tục. Điều này bao gồm toàn bộ Ma trận MITER ATT&CK , có nghĩa là tất cả các bước mà kẻ thù thực hiện để đạt được mục tiêu của mình, bắt đầu từ các nỗ lực lừa đảo đến kiên trì và đánh cắp dữ liệu.

Nếu bạn có thể phát hiện và phản hồi TTP một cách nhanh chóng, bạn sẽ khiến đối thủ gần như không có cơ hội chống trả. Ví dụ: nếu bạn có thể phát hiện một cuộc tấn công Pass-the-Hash bằng cách sử dụng tính năng Giám sát nhật ký sự kiện của Windows và khắc phục nó, thì bạn có thể nhanh chóng tìm thấy máy chủ bị xâm nhập và ngăn chặn chuyển động bên trong mạng của mình . Tại thời điểm này, kẻ tấn công sẽ có hai lựa chọn:

1. Quay lại, nghiên cứu và đào tạo thêm, cấu hình lại các công cụ tùy chỉnh của họ
2. Bỏ cuộc và tìm mục tiêu khác

Tùy chọn 2 chắc chắn có vẻ ít tốn thời gian và tài nguyên hơn.

Question and Answer

Navigate to ATT&CK Matrix webpage. How many techniques fall under the Exfiltration category?

9

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Account	Abuse	Abuse Elevation	Adversary-in-	Account Discovery	Exploitation of	Adversary-in-	Application	Automated	Account Access

Chimera is a China-based hacking group that has been active since 2018. What is the name of the commercial, remote access tool they use for C2 beacons and data exfiltration?

- Search trên att&ck :

MITRE | ATT&CK[®]

Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog

Search

GROUPS

Chimera
Cleaver
Cobalt Group
Confucius
CopyKittens
CURIUM
Dark Caracal
Darkhotel
DarkHydus
DarkVishnya

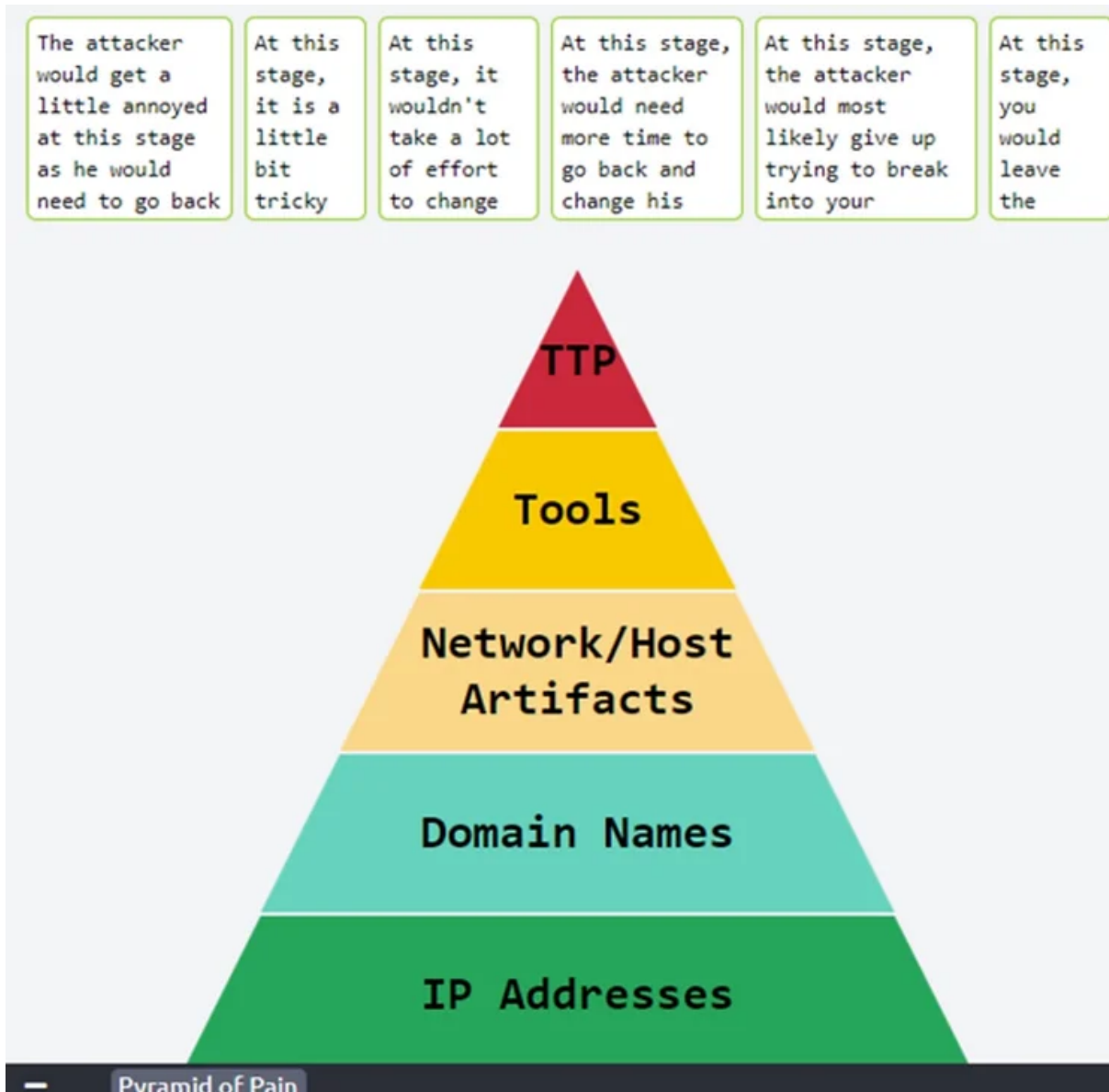
Techniques Used

ATT&CK[®] Navigator Layers

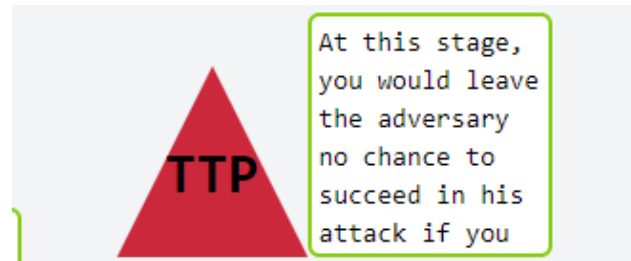
Domain	ID	Name	Use
Enterprise	T1087	.001 Account Discovery: Local Account	Chimera has used <code>net user</code> for account discovery. ^[2]
		.002 Account Discovery: Domain Account	Chimera has has used <code>net user /dom</code> and <code>net user Administrator</code> to enumerate domain accounts including administrator accounts. ^{[1][2]}
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	Chimera has used HTTPS for C2 communications. ^[2]
		.004 Application Layer Protocol: DNS	Chimera has used Cobalt Strike to encapsulate C2 in DNS traffic. ^[2]
Enterprise	T1560	.001 Archive Collected Data:	Chimera has used gzip for Linux OS and a modified RAR software to

Cobalt Strike

8. Practical: The Pyramid of Pain



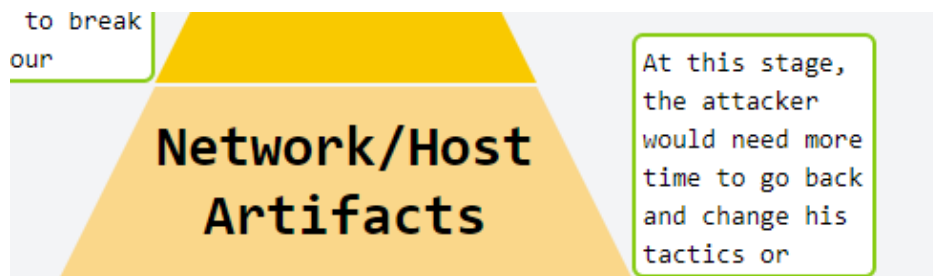
- Chúng ta sẽ đi theo từ trên xuống dưới
- Ở phần TTP: Đây không chỉ là đỉnh của kim tự tháp mà còn là khó khăn nhất đối với kẻ tấn công. Vì vậy, câu trả lời là: Ở giai đoạn này, bạn sẽ không để đối thủ có cơ hội thành công trong cuộc tấn công nếu bạn có thể phát hiện và phản ứng nhanh chóng với các mối đe dọa.



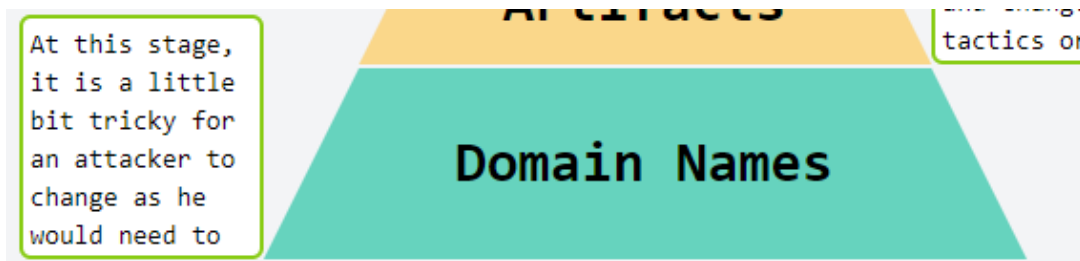
- Ở phần Tools: chúng ta đã phát hiện ra các công cụ, tệp và tài liệu có thể có trên PC của nạn nhân. Vì vậy, câu trả lời cho lớp này sẽ là câu lệnh; Ở giai đoạn này, kẻ tấn công rất có thể sẽ từ bỏ việc cố gắng đột nhập vào mạng của bạn hoặc quay lại và cố gắng tạo một công cụ mới có khả năng tương tự. Ở giai đoạn này, kẻ thù sẽ sử dụng cửa sau, tải trọng tùy chỉnh hoặc tài liệu độc hại.



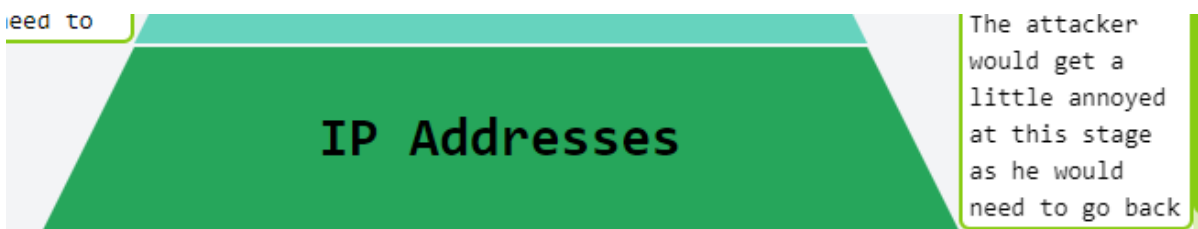
- Ở phần Network/Artifacts: Ở lớp này chúng ta tìm hiểu về HTTP POST và chuỗi tác nhân người dùng. Vì vậy, mô tả phù hợp nhất với lớp này là; Ở giai đoạn này, kẻ tấn công sẽ cần nhiều thời gian hơn để quay lại và thay đổi chiến thuật hoặc sửa đổi công cụ. Chuỗi tác nhân người dùng, thông tin C2 hoặc mẫu URI theo sau là các yêu cầu HTTP POST có thể là chỉ báo.



- Ở phần Domains: Trong lớp này chúng ta đã tìm hiểu về các URL rút ngắn và các tác nhân đe dọa có thể thay đổi tên miền. Vì vậy, câu trả lời mô tả sẽ là; Ở giai đoạn này, kẻ tấn công sẽ gặp một chút khó khăn khi thay đổi vì hần cần mua, đăng ký và lưu trữ nó ở đâu đó.



- Ở phần IP Address: Ở cấp độ này, chúng ta biết rằng chúng ta có thể khám phá địa chỉ IP của tác nhân đe dọa sau đó chặn nó thông qua tường lửa, do đó gây khó chịu cho tác nhân đe dọa. Vì vậy, câu trả lời mô tả sẽ là; Kẻ tấn công sẽ cảm thấy hơi khó chịu ở giai đoạn này vì hắn cần phải quay lại và cấu hình lại các công cụ của mình. Kẻ tấn công có xu hướng để lại các mẫu phổ biến như thay đổi khóa đăng ký, tệp bị mất và thực thi quy trình đáng ngờ.



- Ở phần Hash: Trong lớp này, chúng ta đã biết rằng hàm băm là các chuỗi chữ cái và số duy nhất. Khi chạy tệp độc hại thông qua thuật toán băm, kết quả đầu ra có thể được sử dụng để ký tên phần mềm độc hại. Vấn đề là một thay đổi nhỏ sẽ làm thay đổi giá trị băm. Mô tả phù hợp nhất với lớp này là; Ở giai đoạn này, sẽ không mất nhiều công sức để thay đổi nó chỉ bằng một chút sửa đổi tệp, nhưng hầu hết bạn vẫn có thể phát hiện ra nó bằng cách sử dụng hàm băm mở.

