## Signature-based Detection Using Network Timing

Josh Pyorre, Nov, 2022



TIMECOP

# JOSH PYORR TALOS Senior Security Researcher

## DEEPSEC



NASA

## A few things first

l'm not a scientist Also not a mathematician More like an artist who likes to brute force through a problem using Python (Security Researcher)



# Finding Bad Things in the Network

## DEEPSEC



Time	Source	Destination	Protocol	gtr   Info	
2022-11-09 15.50.57.255040	3.237.73.239	192.100.1.79	ICP	00 445 - 57655 [ACK] 5eq-10114	Z ACK-0939 WIN-30704 LEN-1440 13
2022-11-09 15:38:57.233047	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16258	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.233047	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16402	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.233048	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16546	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.233049	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16690	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.233102	192.168.1.79	3.237.73.239	TCP	66 57853 → 443 [ACK] Seq=8959	Ack=168342 Win=122432 Len=0 TSva
2022-11-09 15:38:57.233118	192.168.1.79	3.237.73.239	TCP	66 [TCP Window Update] 57853 →	443 [ACK] Seq=8959 Ack=168342 W
2022-11-09 15:38:57.308865	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16834	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.308866	3.237.73.239	192.168.1.79	TCP	06 443 → 57853 [ACK] Seq=16978	2 Ack=8959 Win=56704 Len=1440 TS
2022-11-09 15:38:57.309201	192.168.1.79	3.237.73.239	TCP	66 57853 → 443 [ACK] Seq=8959	Ack=171222 Win=316800 Len=0 TSva
2022-11-09 15:38:57.311057	3.237.73.239	192.168.1.79	TLSv1	07 Application Data, Applicati	on Data
202					
<sup>202</sup> (Slide contains a	video of stream	ning traffic)			

 202
 202
 202
 202
 202
 202
 202
 202
 202
 203
 204
 205
 205
 206
 206
 207
 208
 208
 209
 209
 200
 200
 201
 202
 203
 204
 205
 206
 206
 207
 208
 209
 209
 209
 200
 200
 200
 201
 202
 203
 204
 205
 206
 206
 207
 208
 208
 209
 209
 209
 200
 200
 201
 202
 203
 204
 205
 205
 206
 206
 207
 208
 208
 209
 209
 209
 200
 200
 200
 201
 202
 202
 203
 204
 205
 206
 207
 208
 208
 209
 209
 209
 200
 200
 200
 200
 201
 202
 203
 204
 205
 206
 206
 207
 208
 208
 209
 209
 209
 200
 200
 200
 200
 200
 201
 201
 202
 203
 204
 204
 205
 206
 206
 207
 208
 208
 208
 208
 208
 209
 However, we have tools to reduce that - IDS, various network analysis tools.

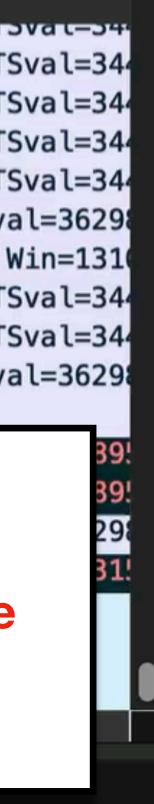
byte

Src: SonyInte\_6b:06:97 (00:e4:21:6b ocol Version 4, Src: 192.168.1.9, D Protocol, Src Port: 5353, Dst Port ain Name System (response)

00 68 97 4e 00 00 ff 11 81 0010 00 fb 14 e9 14 e9 00 54 0020 62 00 01 00 00 00 00 09 5f 73 0030 07 5f 64 6e 73 2d 73 64 0040 -04 63 61 6c 00 00 0c 00 01 0050 00 73 70 6f 74 69 66 79 2d 0060 63 5f 74 63 70 c0 23 0070

## DEEPSEC

89	c0	a8	01	09	e0	00	$\cdot h \cdot N \cdot \cdot$
db	00	00	84	00	00	00	•••••T b•••••
65	72	76	69	63	65	73	•••••_ services
5f	75	64	70	05	6c	6f	∙_dns-sd ·_udp·lo
00	11	94	00	18	10	5f	cal · · · · · · · · · · · · · · · · _
6f	6e	6e	65	63	74	04	spotify- connect
							_tcp #



POST /wp-includes/fonts/Review/Home/ HTTP/1.1

application, application/vnd.ms-excel, application/msword, \*/\*
Referer: http://triangularllc.com/wp-includes/fonts/Review/Home/
Accept-Language: en-us

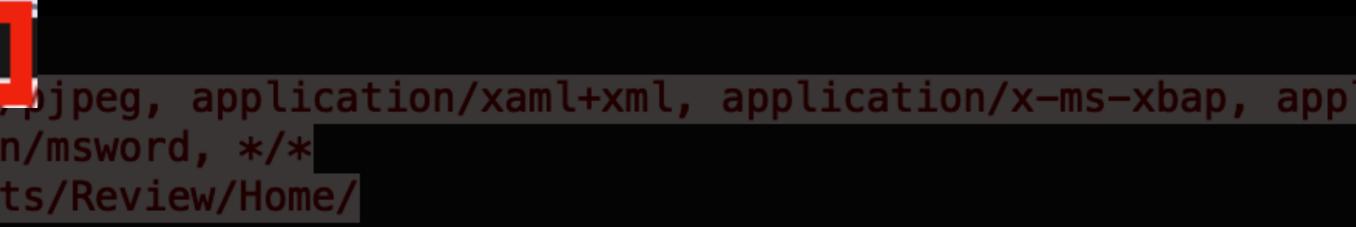
Connection: Keep-Alive Cache-Control: no-cache

hidCflag=&Email=johnharmathon&Passwd=%2544q439%26%26&signIn=Sign+in&rmShown=1HTTP/1.1 200 OK

Date: Mon, zo sep zoio iz sonsz om

X-Powered-By: PHP/5.4.45 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html





Notes for the viewer: How do you find the one bad thing in all that traffic?

Server: Apache/2.2.31 (Unix) mod\_ssl/2.2.31 OpenSSL/1.0.1e-fips mod\_bwlimited/1.4



### Notes for the viewer: Building context while leading into the topic. Let's talk about Attribution



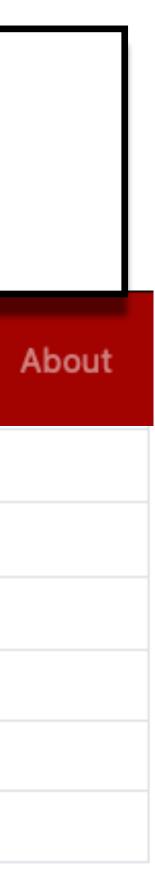


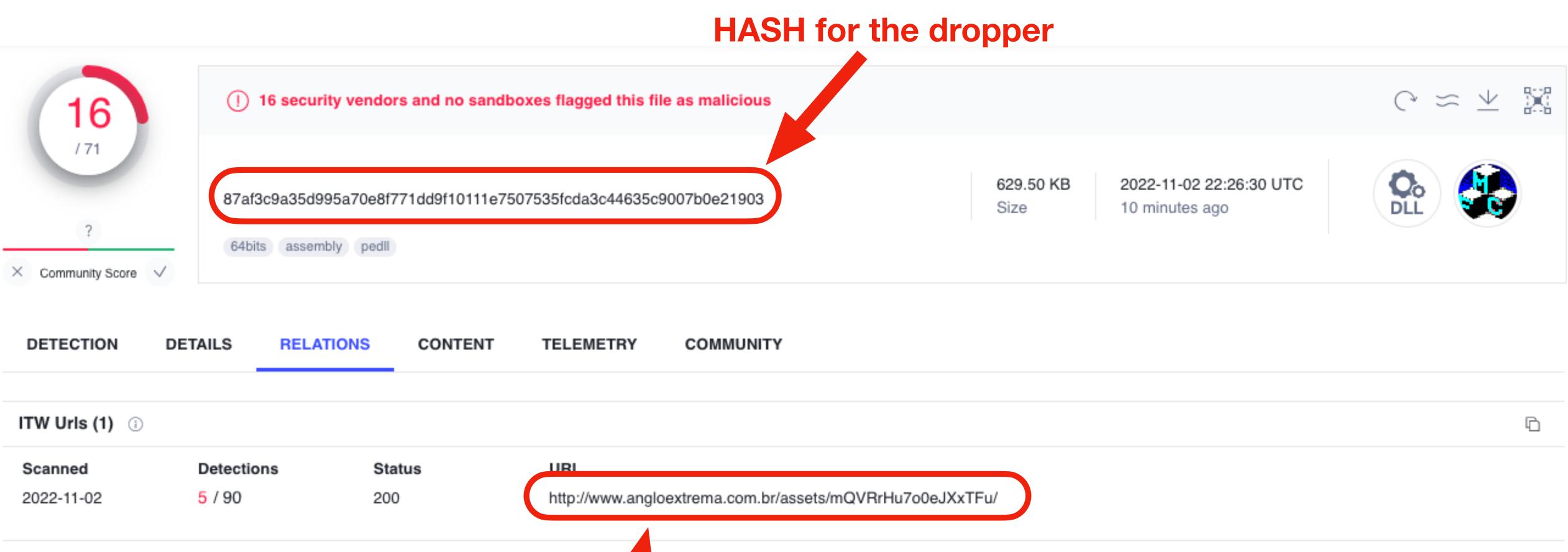
# Attribution

Notes for the viewer: If we see a suspicious URL in our network, what does it mean?					
		Browse	API	Feeds	Statistics
URL:	http://www.angloextrema.com.br/assets/mQVRrHu7o0eJXxTFu/				
URL Status:	A Online				
Host:	C www.angloextrema.com.br				
Date added:	2022-11-02 22:03:12 UTC				
Threat:	j≨ Malware download				
Tags:	dll emotet 🖻 epoch4 heodo 🖻				
Emotet					

DEEPSEC







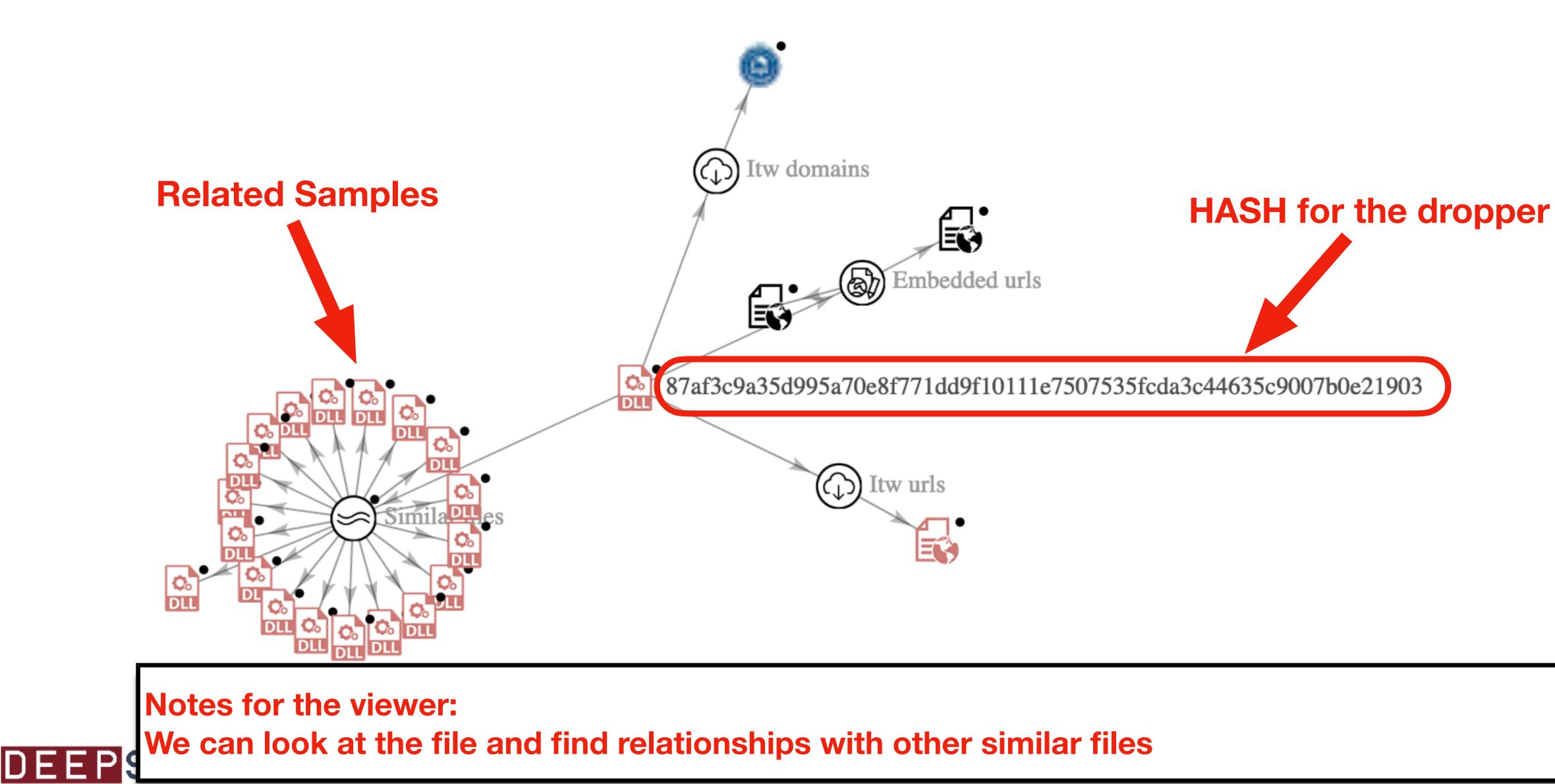
DETECTION	DETAILS	RELATIONS	CONTENT	TELEMETRY	сомми
ITW Urls (1)	D				
Scanned	Detectio	ons Sta	atus	LIRI	
2022-11-02	5 / 90	20	0	http://www.angle	oextrema.co

### **Notes for the viewer:**

When that URL leads to a suspicious file, what is that file? DEEP

URL







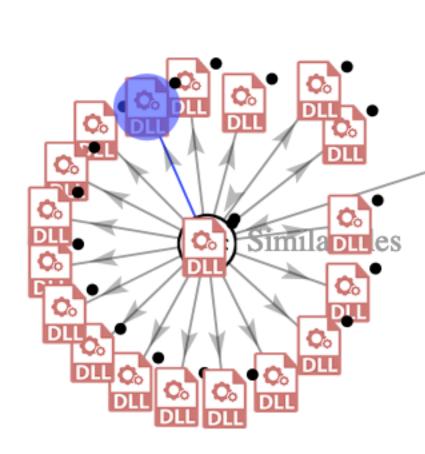
Basic Properties	L
Type Size	Win32 DLL 629.50 kB 2022-11-02 22:22:52
First Seen Last Seen Submissions	2022-11-02 22:22:52 2022-11-02 22:22:52 1
File Name	payload_1.bin

Relations	<i>?</i> * <sup>8</sup>
Embedded urls 2	ß
Similar files 168	ß
Expand using new intelligence search	

Basic Properties	
Туре	Win32 DLL
Size	629.50 kB
First Seen	2022-11-02 22:25:11
Last Seen	2022-11-02 22:25:11
Submissions	1
File Name	49d1ac29fa559b4b9c 6a54c700beaba9.viru
	S
Polationa	0.9

Relations		<i>~</i> \$
Embedded urls	2	ß
Similar files	168	ß
Expand using new intellige	anco soarch	9.2





DLL

**C**\_

C.

Q<sub>o</sub>

•

DL

Ç,

0.

0.

۱ů

#### **Basic Properties**

T	Wi-00 DI
Туре	Win32 DL
Size	629.50 kB
First Seen	2022-11-0
Last Seen	2022-11-0
Submissions	1
File Name	5728b804
	30432a57
	us

#### Relations

Embedded urls

Similar files

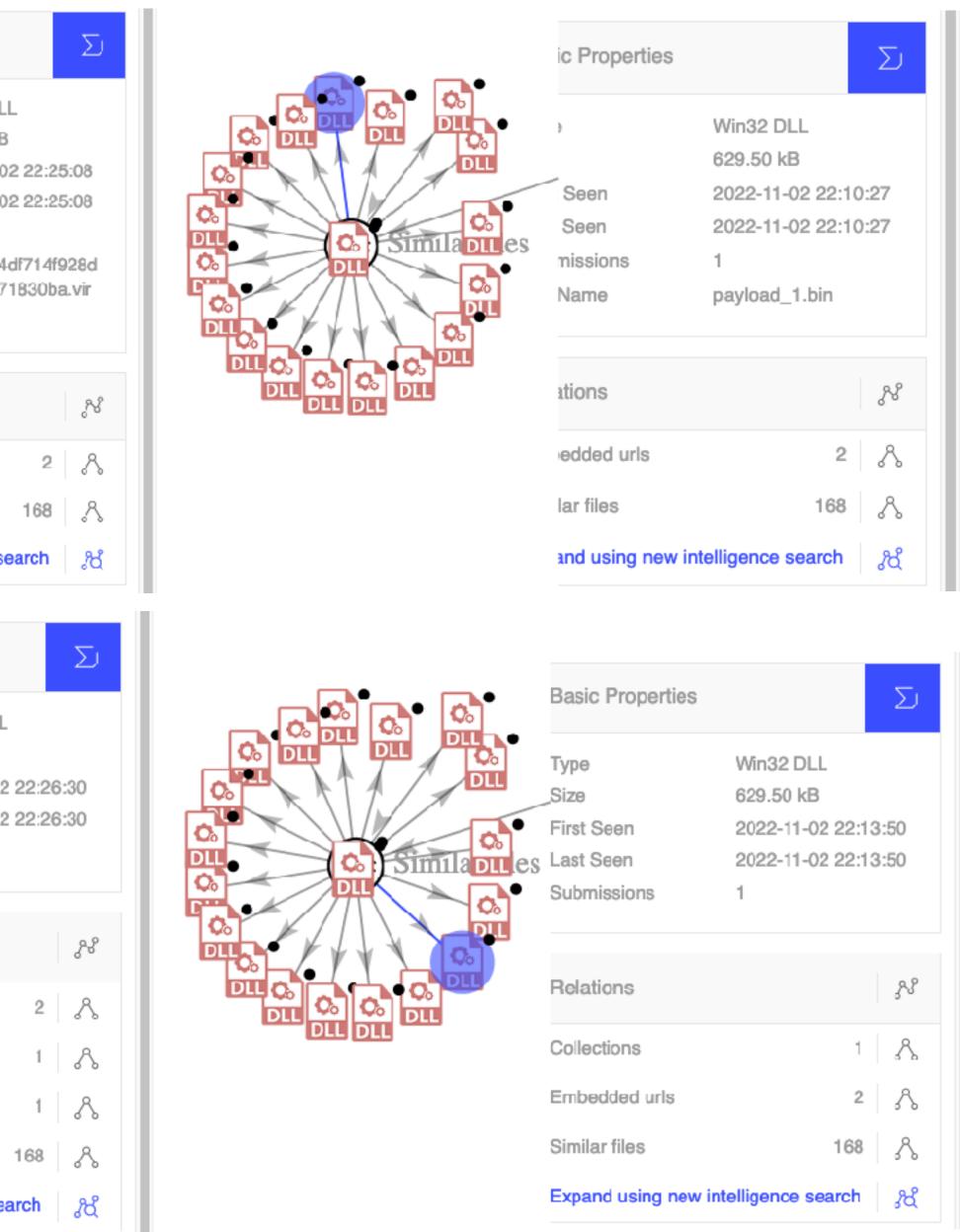
Expand using new intelligence search

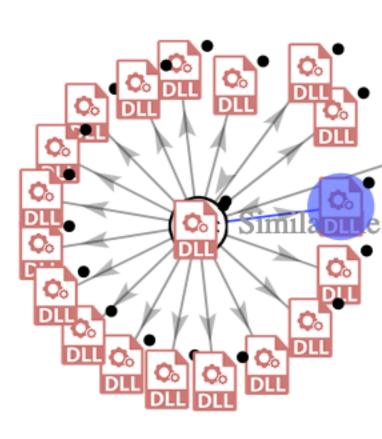
#### **Basic Properties**

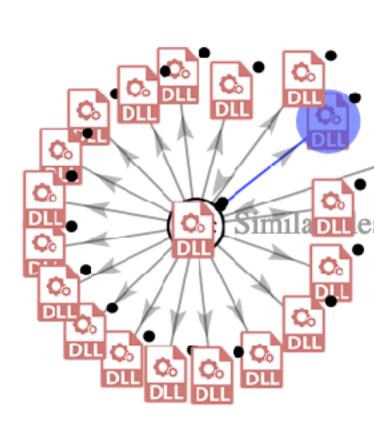
	Type Size First Seen Last Seen Submissions	Win32 DLL 629.50 kB 2022-11-02 2 2022-11-02 2 1
Simila Diles	Relations	
	Embedded urls Itw domains	
	ltw urls Similar files	1
	Expand using new in	telligence sear

#### **Notes for the viewer:**

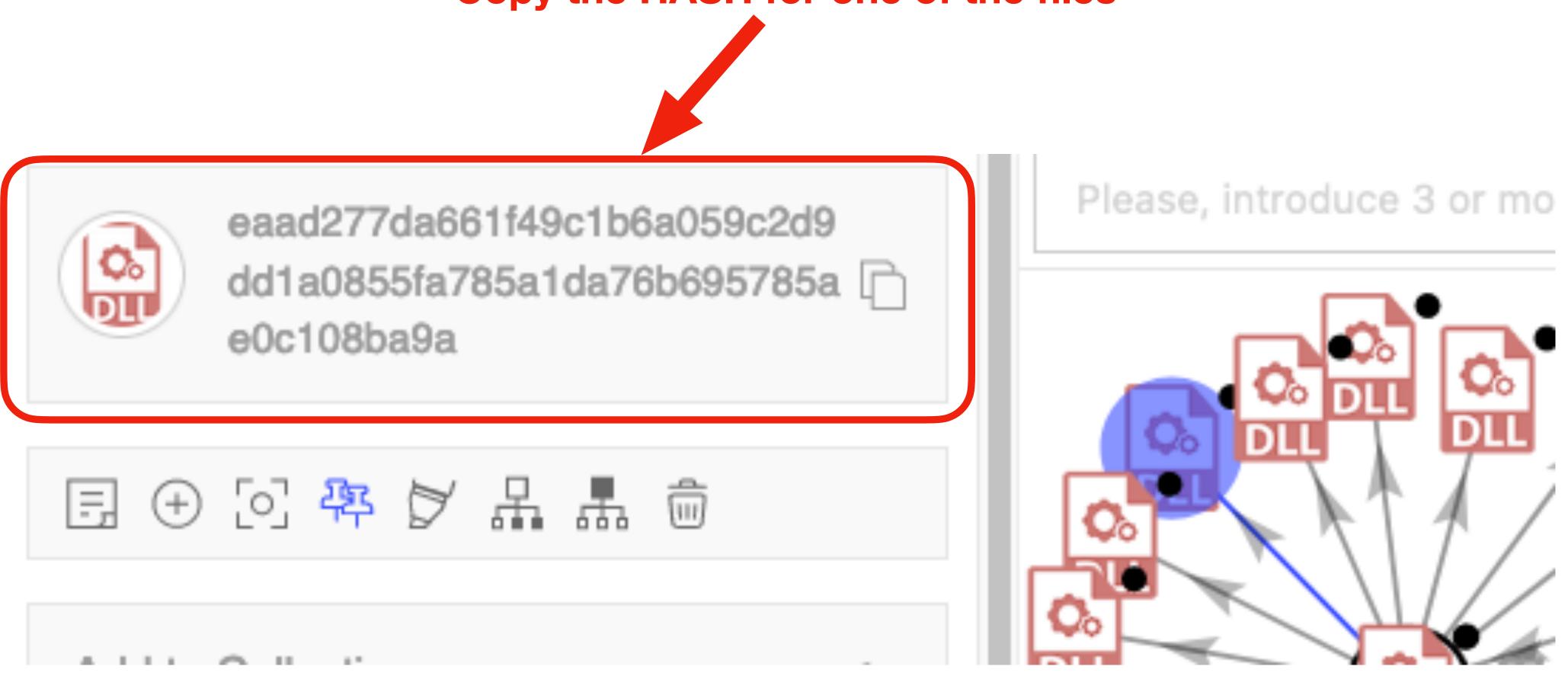
We can look at the file and find relationships with other similar files DEEPS











Notes for the viewer: We can continue looking using various thir campaign



## **Copy the HASH for one of the files**

#### We can continue looking using various third party tools to find other relationships, attributing to a



#### Associated Artifacts

The following artifacts may have been incomplete or missing information about behavioral indicators and network connections.

SHA256 Signature	Magic Type
b5a9530302ceab6a1193dcda7a6b68e9e32ae90513285b38	PE32+ executable (GUI) x86
ac3f645023b0a826a8dfdf01610cc9ebd6dfcec6a06ba8f3151	MS Windows Vista Event Lo
bbb7404419f91f82cedfec915931a9339f04165b27d8878d63	PE32+ executable (GUI) x86
9b7ac0309609983d0cc06a7d4872d68f0c33d865b4abf8e29	data
9117986e2928133190cbaa2ab698d6280ff9bffd0e17e43ca7	PE32+ executable (GUI) x86
3b633bb92eb56e06c8d60d8f6328aa835be63a5a8e1abf2d3	MS Windows Vista Event Lo
b0bc89e94585c3bf6e1123ac27c4e66c04f6400487b3fe57d9	data
d03e31bf532aadfa780081cd2f387ac2519543379de231b5d	MS Windows Vista Event Lo
cda618f08b4bf7099206ff6cc85156a69e2744c1bb7157c798	MS Windows Vista Event Lo
d03e31bf532aadfa780081cd2f387ac2519543379de231b5d	MS Windows Vista Event Lo

**Notes for the viewer:** 

We can continue looking using various this campaign



	AV Result
6-64	
og	
6-64	
6-64	
og	
og	
og	
	$1 - 0$ of $\ell$

#### We can continue looking using various third party tools to find other relationships, attributing to a



## **Compromised websites**

http://www.angloextrema.com.br/assets/mQVRrHu7o0eJXxTFu/

http://alvaovillagecamping.pt/wp-content/Ra9iwOPb6uLf/

2022-11-02 22:03:11	http://alvaovillagecamping.pt/wp-content /Ra9iwOPb6uLf/	Online	dll emotet 🕑 epoch4 heodo 🕑
2022-11-02 21:51:07	http://wordpress.xinmoshiwang.com /list/cRIH9Bd/	Online	dll emotet 🕑 epoch5 heodo 🖻
2022-11-02 21:50:20	http://ruitaiwz.com/wp- admin/sV1NeVxLDiHJ1xm/	Online	dll emotet 🖻 epoch5 heodo 🖻
2022-11-02 21:50:15	http://voinet.ca/cgi-bin/RXDWHpi8dHHZf8/	Offline	dll emotet 🕑 epoch5 heodo 🕑
2022-11-02 21:50:15	http://cultura.educad.pe/wp-content /A86I7QxwuEZV/	Online	dll emotet 🕑 epoch5 heodo 💌
2022-11-02 17:35:41	https://atlantia.sca.org/php_fragments /D8Nwm2F80BL4s/	Offline	dll emotet 🕑 epoch4 heodo 🕑
2022-11-02 17:35:13	https://amorecuidados.com.br/wp- admin/t3D/	Offline	dll emotet 🕑 epoch4 heodo 💌
2022-11-02 17:35:13	http://thuybaohuy.com/wp-content /u3MJwXSP9tmiaTCyZD/	Online	dll emotet 🖻 epoch4 heodo 🖻

**Notes for the viewer:** 

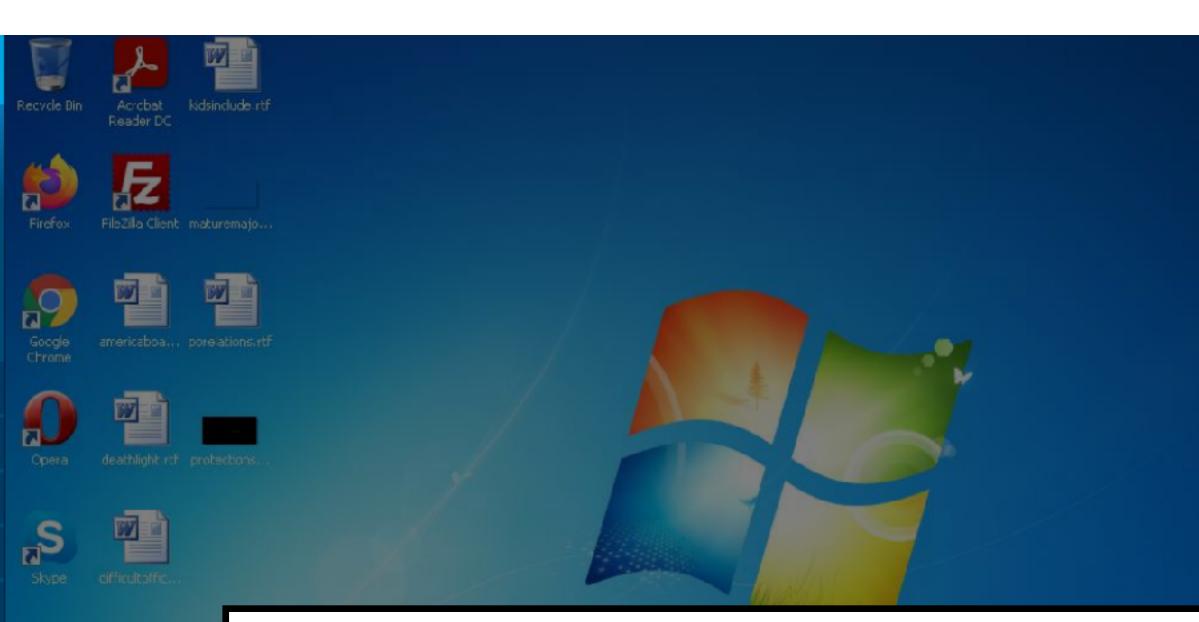
DEEPSEC

case), attributing to a campaign

2022-11-02	http://sat/ate.com/wordpress
09:53:06	/ZAf5j4MG8Hwnig/

## We can continue looking using various third party tools to find other relationships (URLs in this





# CCeaner Hields.pnc

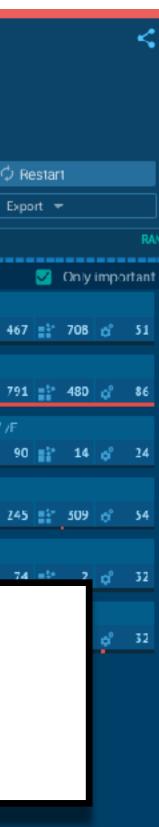
DEEPSEC

### Notes for the viewer: We can also follow, in more detail, the hosting infrastructure to gain attribution - or ownership based off that infrastructure use. In this case, I found a sample that calls out to an IP address.

#### Start 6 7 0 0 4 Connections DNS Requests HTTP Requests 0 Threats Headers Fimeshift Rep PID POST + 200: 0K 👌 2480 rowwer.exe POST + 200: 0K 👌 2480 rovwer.exe http://31.41.244.15/Mp1sDv3/index.php?scr=1 57512 ms CET | 200: OK 🤣 2480 rovwer.exe http://31.41.244.15/Mb1aDv3/Plugins/cred.dll 57521 ms POST | 200: 0K Ð

file         MD5: 4DD5F34C943BE0         Start: C2.11 2022, 15.05         Win7 32 bit         Complete         Indicators: 10	5 Total time: 120 s		
🛓 Get sample	E 10C	🗶 MalConf	
Text report	Process graph	ATT&CK <sup>™</sup> matrix	
Processes Filter by PID or name	CPU		
▼ 1124 file exe PF			
- ▼ 2480 rovwel.exe PE ·ᢓ· ←→			ama dey
2146 schtasks.exe /Create /	/SC MINUTE /MO 1 /TN rovwer.exe /TR "D:\Use	rs\admin\AppData\Locel\Temp\e94c2b2i	8f2\rovwer.exe
3936 nundil32 exe_Cr\Users\ ← <sub>→</sub>	admin\AppData\Roaming\80b59841e5c623\c	red dll, Main	E
2452 SCH rovwer.exe PE			

* ()) 🖬	P	11 05 PM 📰
Filter by PID, name or un		± PCAP
	Conte	ent
8	57b 🕈	text
	6ს 🔸	text
61.6	а КБ 👍	binary
61.6	i Kb 🔺	binary
120	а КБ 🔸	executable
7	786 🕈	text



**Notes for the viewer:** 

We can also follow, in more detail, the hosting infrastructure to gain attribution - or ownership based off that infrastructure use. In this case, I found a sample that calls out to an IP address.





## http://31.41.244.15/Mb1sDv3/index.php

## http://31.41.244.15/Mb1sDv3/index.php?scr=1

## http://31.41.244.15/Mb1sDv3/Plugins/cred.dll

## http://31.41.244.15/Mb1sDv3/index.php



	31.41.2	244.15					INVESTIGATE	ВАСК ТО ТОР
DNS Resolution	Autonomous Sys	stems Associate	d Samples Rece	ent Detections				
Threat Score	SHA256 Signa	ture			AV Result	File Type		First Seen
95	18dc2f7943	15142579f1e66b13	dea4e23ff1c51589	2b8d079b	malicious, (RDML:ZHvxJU985AcNY gen,(high,[Trj],win /malicious_confidence_1 Downloader.Win32.Deym [Trj],ML.Attribute.HighCon gen,Trojan.Malware.3009 /GenKryptik.ETEM!tr,Dete /Kryptik.HUW.gen!Eldorad Downloader.Win32.Deym /PE- A,Trojan.Win32.Save.a,Su (W),Generic.Malware,W3 (score:,Trojan.MalPack.G	PE32 exec	cutable (GUI) Intel 8038	6 11/02/2022
95	cb31e10b92	90209208fe012f4e	3e48348efbe31f9e	46c4b073	[Trj], suspicious,Trojan.Malwar QV,PWSX-gen,W32 /Kryptik.HWT.gen!Eldorad Cryptor.2LA.gen,Static,Tr /Sabsik.FL.B!ml, (W),Generic.Malware,W3 (score:,Mal/Generic- S,Trojan.MalPack.GS,Mali /GenKryptik_EBYOltr.malic	PE32 exec	cutable (GUI) Intel 8038	6 11/02/2022

#### **Notes for the viewer:**

relationships.



	EST		
_		_	

### We can then look at that IP using third party services or other intelligence to find additional

Generic.Malware,W32.Al. (score:,Trojan.MalPack.G... 9976466, confidence), mal... (high,[Trj],win /malicious\_confidence\_1... gen,Al,100),Malicious,VH...



#### 18dc2f794315142579f1e66b13dea4e23ff1c515892b8d079b7

Destination	URLs
31.41.244.15	3^
Destination http://31.41.244.15/Mb1sDv3/Plugins/cred64.dll http://31.41.244.15/Mb1sDv3/index.php http://31.41.244.15/Mb1sDv3/index.php?scr=1	

cb31e10b9290209208fe012f4e3e48348efbe31f9e46c4b0739e

#### Network Connections

Destination	URLs
31.41.244.15	3^
Destination http://31.41.244.15/Mb1sDv3/Plugins/cred64.dll http://31.41.244.15/Mb1sDv3/index.php http://31.41.244.15/Mb1sDv3/index.php?scr=1	

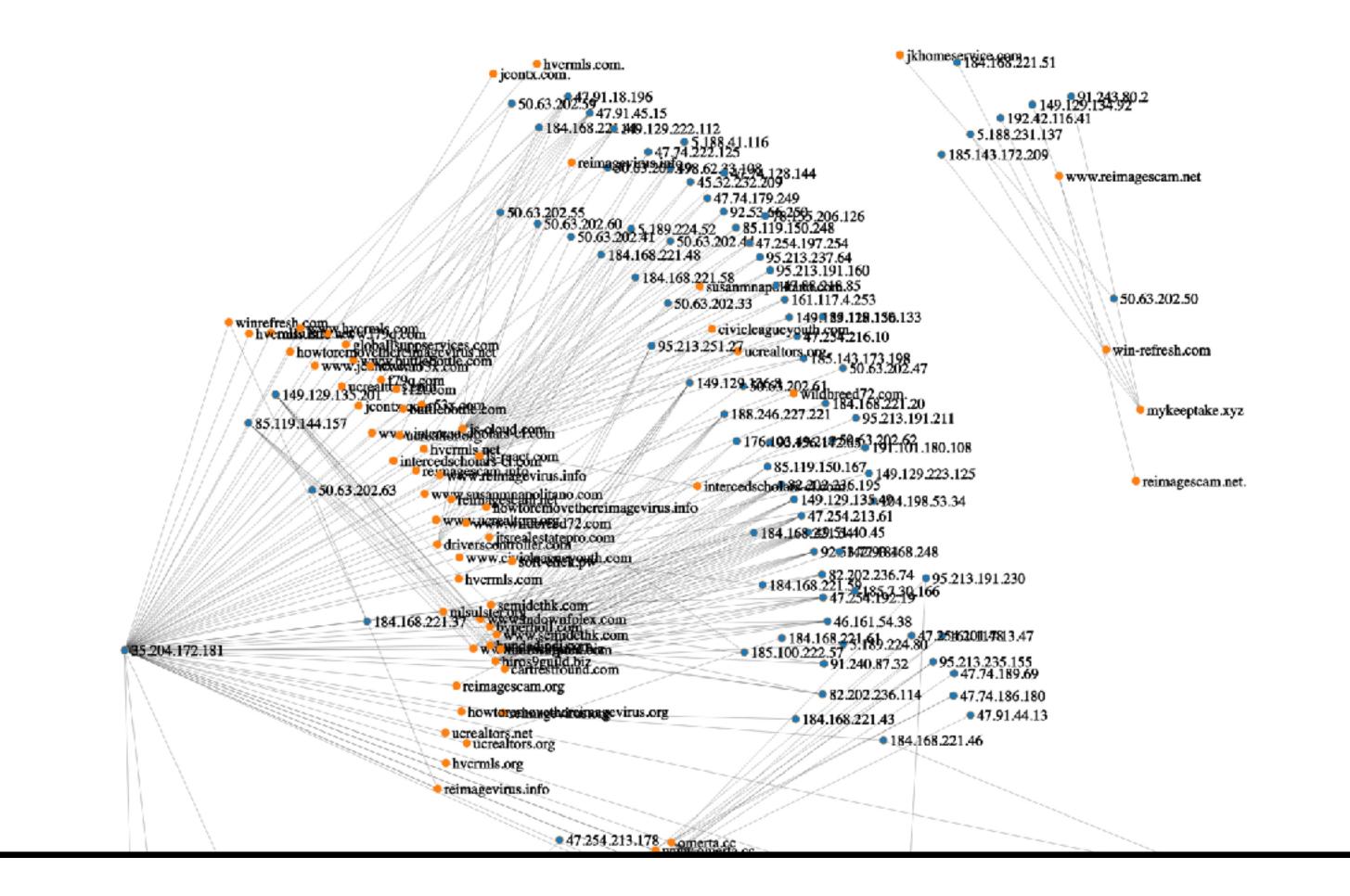
Notes for the viewer: We can then look at that IP using third par relationships.

0149dca9db0b625	INVESTIGATE	BACK TO TOP
	Security Categories	
		1 - 1 of 1
e4b92af2ea206	INVESTIGATE	BACK TO TOP
	Security Categories	

#### We can then look at that IP using third party services or other intelligence to find additional







## **Notes for the viewer:**

bankieren-rabobank.net www.nwolb-security.com

howtoremovethereimagevirus.com

## DEEPSEC

### And we can map those relationships if needed to get an even clearer picture of attribution.

	· 3. 10 10 10 10 10 10 10 10 10 10 10 10 10
	35.204.54.118
11	• 35.204.54.118 • 35.228.109.88
N	
N N	
92.53.91.54	



## MITRE | ATT&CK°

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (B)	Account Manipulation (5)	Abuse Elevation Control	Abuse Elevation Control Mechanism (4)	H Adversary-in-the- Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the- Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public- Facing Application	Container Administration	BITS Jobs	Mechanism (4) Access Token	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data <sub>(3)</sub>	Communication Through Removable	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (/)	External Remote Services	Command Deploy Container	Boot or Logon Autostart Execution (14)	II Boot or Logon	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Media Data Encoding (2)	Exfiltration Over Alternative	Data Encrypted for Impact
Gather Victim Network II	Develop	Hardware Additions	Exploitation for Client	Boot or Logon	Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service	Automated Collection	Data Obfuscation (2)	Protocol (3)	Data Manipulation (3)
Gather Victim Org	Capabilities (2) Establish	Phishing (3)	Execution Inter-Process	Initialization Scripts <sub>(5)</sub>	Boot or Logon Initialization	Debugger Evasion Deobfuscate/Decode Files	Forced Authentication	Cloud Service Dashboard	Session Hijacking (2)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Defacement (7) Disk Wipe (2)
Phishing for Information (3)	Accounts (3) Obtain	Replication Through Removable Media	Communication (3) Native API	Browser Extensions Compromise Client	Scripts (5) Create or Modify	or Information Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery Cloud Storage Object	Remote Services (6)	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Capabilities (6) Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	System Process (4) Domain Policy	Direct Volume Access	Input Capture (4)	Discovery Container and Resource	Through Removable Media	Data from Cloud Storage	Fallback Channels	Exfiltration Over Physical	Firmware Corruption
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Serverless Execution Shared Modules	Create or Modify	Modification (7)	Domain Policy Modification (2)	Modify Authentication	Discovery	Software Deployment Tools	Data from Configuration	Ingress Tool Transfer	Medium (1) Exfiltration Over	Inhibit System Recovery
Search Open Websites/Domains (3)		Valid Accounts (4)	Software Deployment	System Process (4) Event Triggered	Escape to Host	Execution Guardrails (1)	Multi-Factor	Debugger Evasion Domain Trust Discovery	Taint Shared Content	Repository (2) Data from	Multi-Stage Channels	Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			System Services (2)	Execution (16) External Remote	Execution (16) Exploitation for	Exploitation for Defense Evasion	Authentication Interception	File and Directory Discovery	Use Alternate Authentication	Information Repositories <sub>(3)</sub>	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			User Execution (3)	Services Hijack Execution	Privilege Escalation Hijack Execution	File and Directory Permissions Modification (2)	Multi-Factor     Authentication     Request	Group Policy Discovery Network Service Discovery	Material (4)	Data from Local System	Non-Standard Port	Transfer Data to Cloud Account	Service Stop System
			Windows Management Instrumentation	Flow (12) Implant Internal	Flow (12)	Hide Artifacts (10)	Generation     Network Sniffing	Network Share Discovery		Data from Network Shared Drive	Protocol Tunneling		Shutdown/Reboot
				Image	Process Injection (12)	Hijack Execution Flow (12)	OS Credential	Network Sniffing		Data from Removable Media	Proxy (4) Remote Access		
				Modify Authentication Process (7)	III Task/Job (5)	Impair Defenses (9) Indicator Removal (9)	Dumping (8)     Steal Application	Password Policy Discovery Peripheral Device Discovery		Data Staged (2)	I Traffic Signaling (2)		
				Office Application Startup (6)	Valid Accounts (4)	Indirect Command Execution	Access Token Steal or Forge	Permission Groups Discovery (3)		Email Collection (3)	Web Service (3)		
				Pre-OS Boot (5)		Masquerading (7)	Authentication     Certificates	Process Discovery		Screen Capture			
				Scheduled Task/Job (5)		Modify Authentication Process (7)	Steal or Forge Kerberos Tickets (4)	Query Registry		Video Capture			
				Server Software Component (5)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookle	Remote System Discovery Software Discovery (1)					
				Traffic Signaling <sub>(2)</sub>		Modify Registry	Unsecured Credentials (7)	System Information Discovery					

#### **Notes for the viewer:**

levels of a malware or attack campaign.



Matrices

Tactics -

Techniques -

Data Sources

Mitigations -

Software

Groups

#### The MITRE ATT&CK Framework is a well-known method of tracking attribution across multiple

Impact 13 techniques ount Access ioval Destruction Encrypted for act Manipulation (3) cement (2) «Wipe (2) point Denial of ice (4) ware Corruption oit System very work Denial of rice (7) ource Hijacking rice Stop

Campaigns



## APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).<sup>[1][2]</sup> They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.<sup>[3][4][5][6]</sup>

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.<sup>[7][8]</sup> Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.<sup>[9][10][11][12][13]</sup>

Notes for the viewer: The MITRE ATT&CK Framework can be use threat actors.



#### ID: G0016

 Associated Groups: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary

Version: 3.1

Created: 31 May 2017

Last Modified: 11 July 2022

Version Permalink

#### The MITRE ATT&CK Framework can be used to trace tactics and techniques to various known







#### Techniques Used

Domain	ID		Name	Use												
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has l												
Enterprise	T1087		Account Discovery	APT29 obta												
		.002	Domain Account	APT29 has												
		.004	Cloud Account	APT29 has												
Enterprise	T1098	T1098	.001	Account Manipulation: Additional Cloud Credentials	APT29 has											
															.002	Account Manipulation: Additional Email Delegate Permissions
		.003	Account Manipulation: Additional Cloud Roles	APT29 has												
		.005	Account Manipulation: Device Registration	APT29 regis												
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT29 has												
		.006	Acquire Infrastructure: Web Services	APT29 has												

## Notes for the viewer: The MITRE ATT&CK Framework can be used to trace tactics and techniques to various known threat actors.

Registry Run Keys / Startup Folder





bypassed UAC.<sup>[24]</sup>

tained a list of users and their roles from an Exchange server using Get-ManagementRoleAssignment.<sup>[12]</sup>

used PowerShell to discover domain accounts by executing Get-ADUser and Get-DGroupMember.<sup>[17][14]</sup>

conducted enumeration of Azure AD accounts.<sup>[25]</sup>

added credentials to OAuth Applications and Service Principals.<sup>[26][17]</sup>

ded their own devices as allowed IDs for active sync using <u>Set-CASMailbox</u>, allowing it to obtain copies of permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.<sup>[12]</sup>

granted company administrator privileges to a newly created service principal.<sup>[17]</sup>

istered devices in order to enable mailbox syncing via the Set-CASMailbox command.<sup>[12]</sup>

acquired C2 domains, sometimes through resellers.<sup>[10][27][18]</sup>

registered algorithmically generated Twitter handles that are used for C2 by malware, such as HAMMERT



-

# There are books about doing this kind of thing



**Copyrighted Material** 

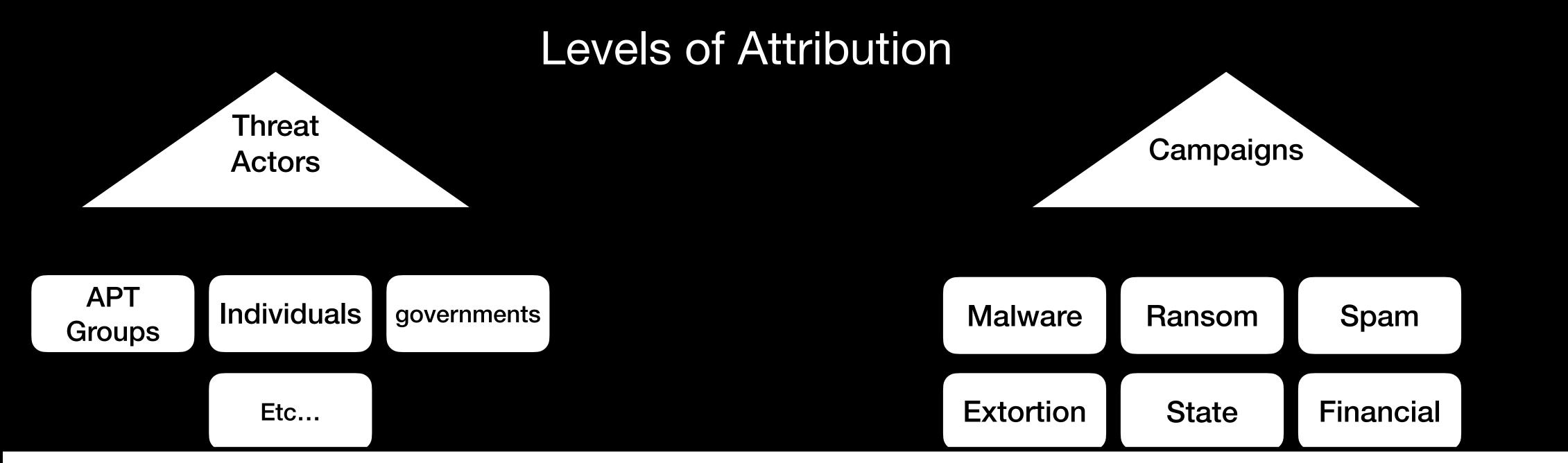
# Malware Data Science

**Attack Detection and Attribution** 

Joshua Saxe with Hillary Sanders

Foreword by Anup Ghosh, PhD Copyrighted Material





#### **Notes for the viewer:**

Attribution is up to you. Are you interested in what group is targeting your network? Or maybe you just want to know if that URL is related to some malware family. Or maybe you simply want to know what is happening in your network and that's enough.



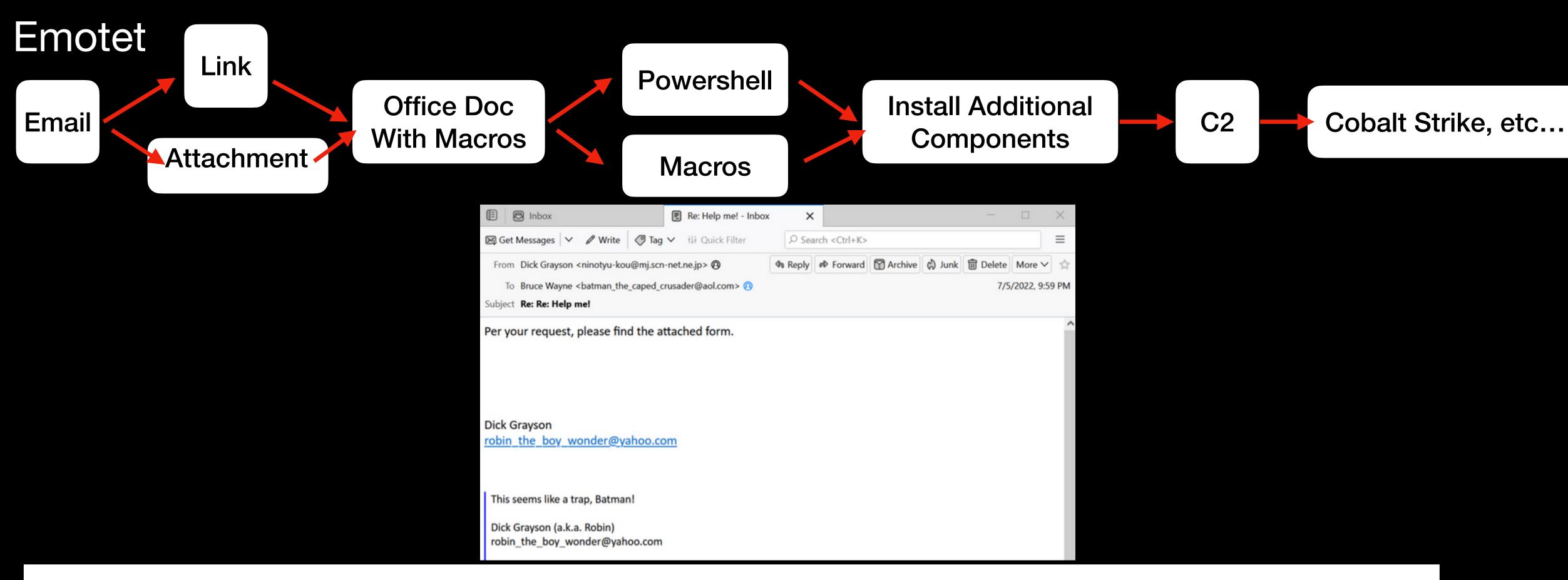


's in your	Or just		
	's in your		
	etwork		

**Notes for the viewer:** A quick summary of the common path of infection on a system, before we get into a bunch of **PCAP** analysis.

# The Infection Chain





Notes for the viewer: Using Emotet as an example: Comes in as email, leading to a URL to download additional components, and typically ending up in Cobalt Strike and Ransomware infection.

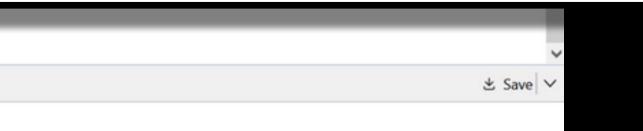
Help me, Batman and Robin! ?- Samantha

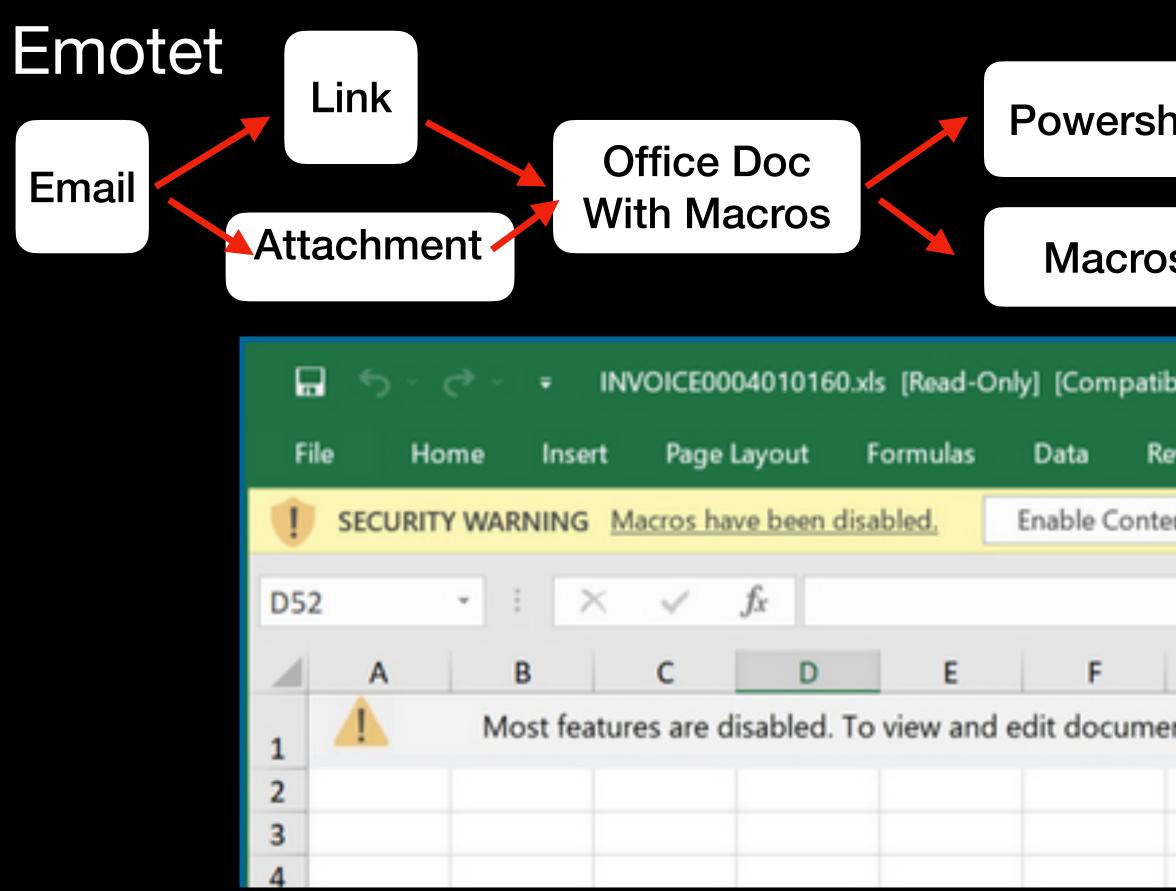
Il 1 attachment: INVOICE0004010160.xls 95.0 KB

INVOICE0004010160.xls 95.0 KB



Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/





#### Notes for the viewer:

Using Emotet as an example: Comes in as email, leading to a URL to download additional components, and typically ending up in Cobalt Strike and Ransomware infection.

Ready



Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/

nell s		tall Add ompon			C2	C	obalt Strike
bility Mode]	- Excel B	ruce Wayne	BW	<b>•</b> -	- 0	×	
eview Vie	w Help	🖓 Tel	l me what y	ou want to	do Q	Share	
nt						×	
						~	
G	н	1	J	к	L		
nt click Ena	ble Editing a	nd click En	able Cont	ent.			



#### e, etc...

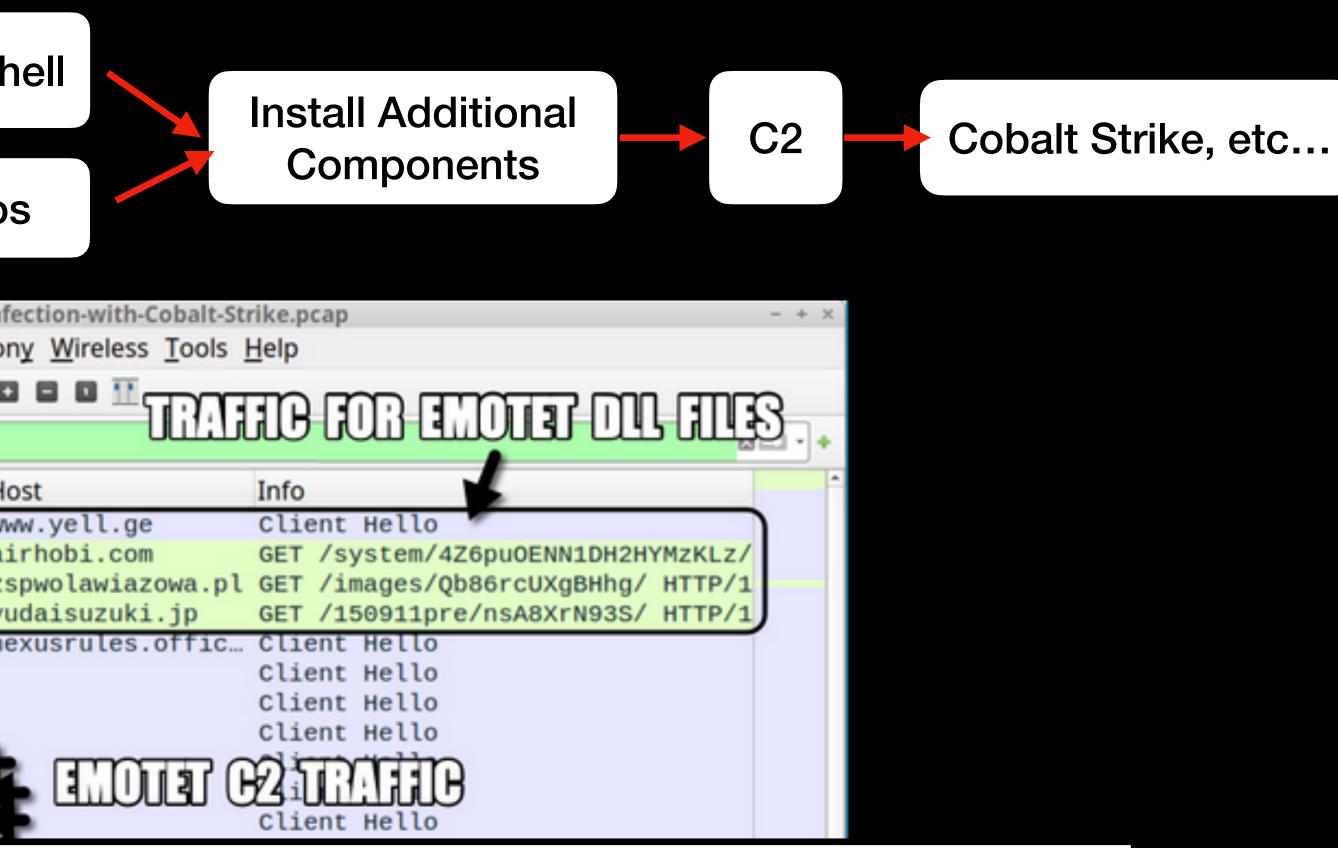
Email	owersh
Attachment With Macros	Macro
-       2022-07-01         File Edit View Go Capture Analyze Statistic         ▲       ▲         ▲       ●         ●       ●<	
(http.request or tls.handshake.type eq 1) and	!(ssdp)
Time Dst	port Ho
2022-07-07 18:18:50 91.239.206.239	443 W
2022-07-07 18:18:59 193.53.245.52	80 ai
2022-07-07 18:19:01 178.255.41.17 2022-07-07 18:19:02 112.78.112.34	80 ZS 80 yt
2022-07-07 18:19:23 52.109.8.21	443 ne
2022-07-07 18:19:28 164.90.222.65	443
2022-07-07 18:19:28 164.90.222.65	443
2022-07-07 18:19:29 164.90.222.65	443
2022-07-07 18:19:30 164.90.222.65 2022-07-07 18:19:30 144.202.108.11	443 6 8080
2022-07-07 18:19:30 144.202.108.11	8080

Notes for the viewer: Once traffic starts, you typically see a second-stage download over HTTP (although it might be over SSL), and then C2 communication over SSL

> 443 2022-07-07 18:21:47 20.189.173.5 443 18:21:47 20.189.173.5 2022-07-07 2022-07-07 18:22:01 144.202.108.116 8080 2022-07-07 18:22:11 52.191.219.104 443 S

## DEEPSEC

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/



			P.	
settings-win.dat	Client	Hello		-
	Client	Hello		
/20.events.data	Client	Hello		
10.events.uata	CTTent	Hello		

## Emotet

Link

Attachment -

#### Email

Office Doc With Macros



Macros

2022-07-07-Emotet-infection-with-Cobalt-Strike.pcap ony Wireless Tools Help • • • • • •

									dia 10 dia 3		07 L	1110.04	
Fi	le <u>E</u>	dit	Viev	<u>м G</u> o	<u>C</u> ap	oture	<u>A</u> r	nalyz	e <u>S</u> t	tatis	tics	Tele	pho
4		đ	۲	<b>•</b>	X	3	9	÷ >	3	₩	≯[		
	(http	o.re	ques	t or t	ls.ha	ndsh	ake.	.type	eq	1) ar	nd !(s	ssdp	)
ïr	ne						Dst					port	t H
	202	2-0	97-0	7 18	:31	:04	164	1.90	. 222	2.6	5	443	
	202	22-0	97-0	7 18	:32	:34	164	1.90	. 222	2.6	5	443	6
	202	2-0	97-0	7 18	:32	:36	164	1.90	. 222	2.6	5	443	G
	202	2-0	97-6	7 18	:32	:36	146	6.59	.15	1.2	50	443	ŀ
	202	22-0	97-0	7 18	:33	:46	164	1.90	. 222	2.6	5	443	
	202	2-0	97-0	7 18	:33	:52	164	1.90	. 222	2.6	5	443	6
	202	22-0	97-6	7 18	:34	:14	52.	18.	235	.51		443	d
	202	22-0	97-0	7 18	:35	:11	52.	18.3	235	.51		443	d:
	202	22-0	97-0	7 18	:35	:16	164	.90	. 222	2.6	5	443	1
	202	22-0	97-6	7 18	:35	:54	52.	18.3	235	.51		443	d
	202	22-0	97-0	7 18	:36	:37	52.	18.	235	.51		443	d:
	202	2-0	97-0	7 18	:37	:14	20.	189	.173	3.5		443	v:
	202	22-0	97-0	7 18	:37	:17	52.	18.3	235	.51		443	d:
	202	22-0	97-0	7 18	:37	:20	52.	18.	235	.51		443	d:
	202	2-0	97-0	7 18	:37	:52	52.	18.	235	.51		443	d
	202	22-0	97-0	7 18	:38	:34	52.	18.3	235	.51		443	d:
	202	22-0	97-0	07 18	:39	:10	52.	18.	235	.51		443	d:
	202	2-0	97-0	7 18	:39	:51	52.	18.	235	.51		443	d:
	202	2-0	97-6	7 18	:40	:34	52.	18.3	235	.51		443	d:
	202	22-0	97-0	07 18	:40	:53	40.	83.	240	.146	5	443	c
	202	2-0	97-0	7 18	:41	:14	52.	18.	235	.51		443	d:
	202	2-0	97-6	7 18	:41	:55	52.	18.3	235	.51		443	d
	202	2-0	97-0	7 18	:42	:40	52.	18.	235	.51		443	d:
	202	2-0	97-0	07 18	:43	:27	52.	18.	235	.51		443	d
	202	2-0	97-6	7 18	:44	:21	52.	18.	235	.51		443	d

Images from: https://isc.sans.edu/forums/diary/Emotet+infection+with+Cobalt+Strike/28824/





**Install Additional** Components



🖾 🗆 • 🔸

Info

Clie

Clie

Clie

Clie

Clie

Clie

Clie

Clie

Clie

Cobalt Strike, etc...

lost

## EDENT STELLE TELLE STELLS

istinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io

```
Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
10.events.data.microsoft.com
                                               Clie
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
lient.wns.windows.com
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
listinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io
                                               Clie
```

istinctive-obi-mgw.aws-euw1.cloud-ara.tyk.io Clie

# Common Signature Detection Methods

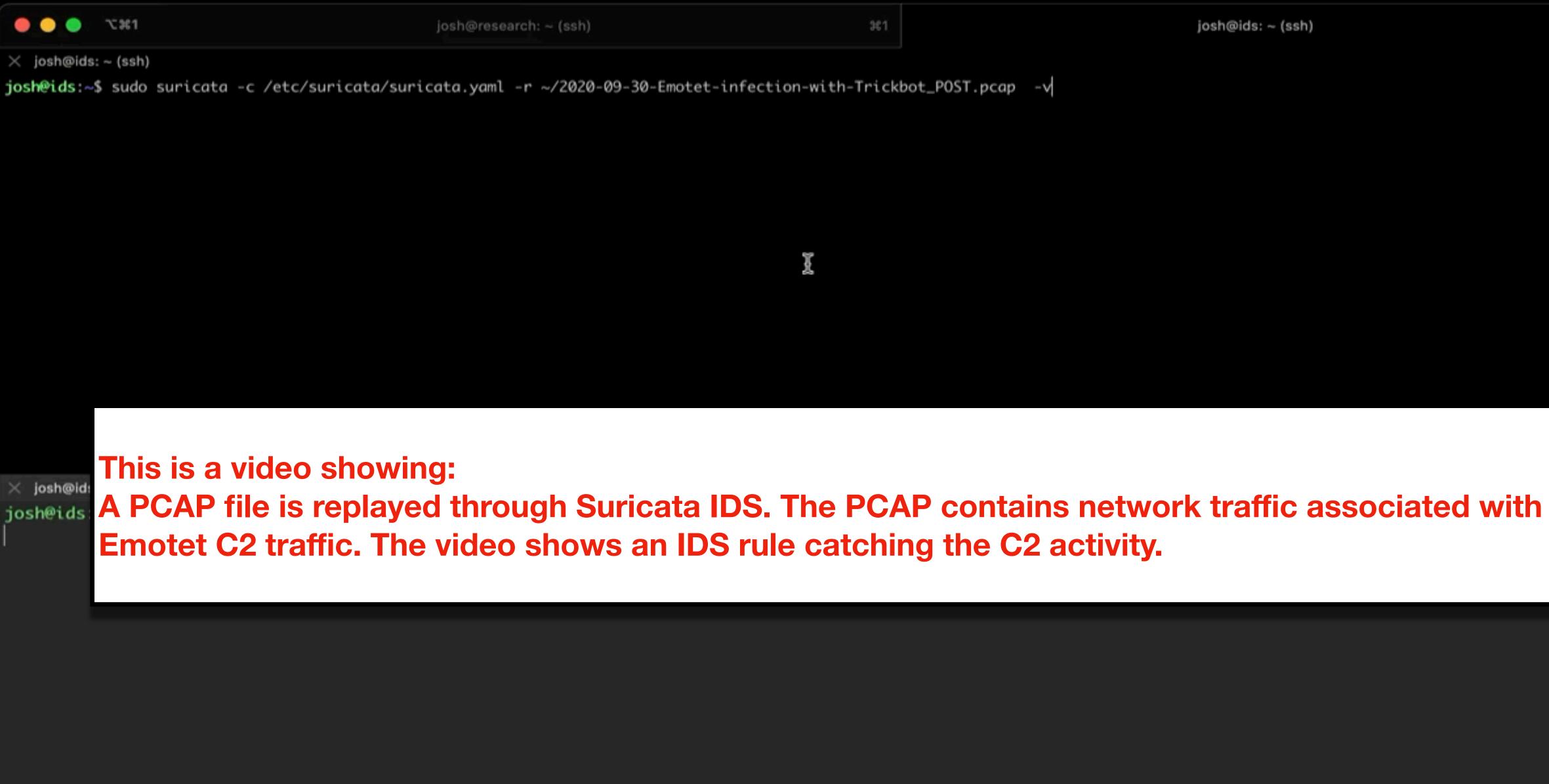
Notes for the viewer: Let's cover the most common signature-based detection methods







**DS Rules** 

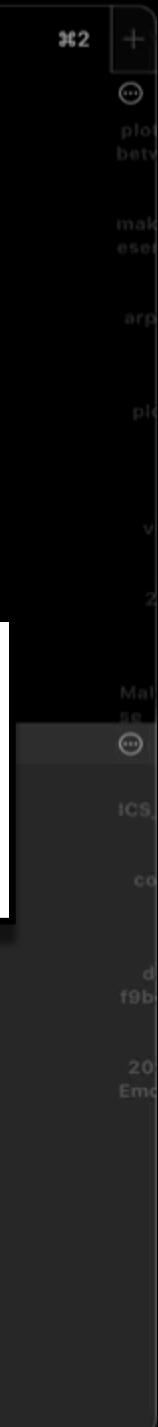




361

josh@ids: ~ (ssh)

I



58:34 - <Notice> - Signal Received. Stopping engine.

 $58:34 - \langle Info \rangle - time elapsed 0.080s$ 

58:34 - <Info> Alerts: 6

58:35 - <Info> - cleaning up signature grouping structure... complete

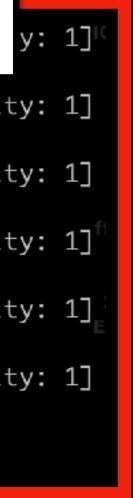
#### **Notes for the Viewer:** Here is a close up of Suricata running and catching the C2 activity.

09/30/ {TCP}

[]	
09/30/2020-16:50:21.950965	[**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priori
{TCP} 10.9.30.101:64263 ->	80.87.201.221:7080
09/30/2020-16:50:25.861050	[**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priori
{TCP} 10.9.30.101:64263 ->	80.87.201.221:7080
09/30/2020-16:50:28.057649	[**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priori
{TCP} 10.9.30.101:64263 ->	80.87.201.221:7080
09/30/2020-16:50:29.657596	[**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priori
{TCP} 10.9.30.101:64263 ->	
09/30/2020-16:50:34.181486	[**] [1:2030868:2] ET MALWARE Win32/Emotet CnC Activity (POST) M10 [**] [Classification: A Network Trojan was detected] [Priori
{TCP} 10.9.30.101:64263 ->	80.87.201.221:7080



## 58:34 - <Notice> - Pcap-file module read 1 files, 1527 packets, 1219373 bytes



alert http \$HOME\_NET any -> \$EXTERNAL\_NET [7080,8080,443,80,4143,995,21,50000,20,8090,8443,990,22] (msg:"ET MALWARE Win32/Emotet CnC Activity (POST) M10"; flow:established,to\_server; content:"POST"; http.uri; content:!"."; content:!"&"; content:!"""; http.user\_agent; content:"Mozilla/5.0 (Windows NT 6."; startswith; content:"|3b 20|"; distance:1; within:2; http.request\_body; content:!".zip"; content:!".png"; content:!".jp"; content:!".exe"; fast\_pattern; http.content\_len; byte\_test:0,<,8000,0,string,dec; byte\_test:0,>,500,0,string,dec; reference:md5,ba2e4a231652f8a492feb937b1e96e71; classtype:trojan-activity; sid:2030868; rev:2; 2020\_09\_14;)

ne 9, Column 1

<ul> <li>17 2</li> <li>18 2</li> <li>19 2</li> <li>20 2<th>t captured the C2 ac</th></li></ul>	t captured the C2 ac
26 2020-09-30 09:50:17.953918 10.9.30.101 27 2020-09-30 09:50:17.954608 trafcj.fvds.r 28 2020-09-30 09:50:17.954734 10.9.30.101 29 2020-09-30 09:50:17.958959 trafcj.fvds.r	Host: 80.87.201.221:7080 Content-Length: 4804 Cache-Control: no-cache
Frame 8: 478 bytes on wire (3824 bits), 478 by Ethernet II, Src: HewlettP_1c:47:ae (00:08:02: Internet Protocol Version 4, Src: 10.9.30.101 Transmission Control Protocol, Src Port: 64263 [5 Reassembled TCP Segments (5457 bytes): #3(6 Hypertext Transfer Protocol	UZ9rmC19 Content-Disposition: form-dat Content-Type: application/oct ?.VP.we.0.tn.)y ``.=\$xxV+ 5.ar
MIME Multipart Media Encapsulation, Type: mult	/y.MpFHF.5.%% V(.J9.Q*cC`0. %v.L@.L.{Z/ 2*g.&WdCH.).w z.q\.ao.`%z.c{C. kR".3*.N.'.2.H&
EEPSEC	UZ9rmC1SsoZVjPcS5Vu

```
http.header_names; content:"|0d 0a|User-Agent|0d 0a|Accept|0d 0a|Accept-Language|0d 0a|Accept-Encoding|0d 0a|"; startswith; content:"Referer|0d 0a|"; distance:0;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_09_14, deployment Perimeter, signature_severity Major
```

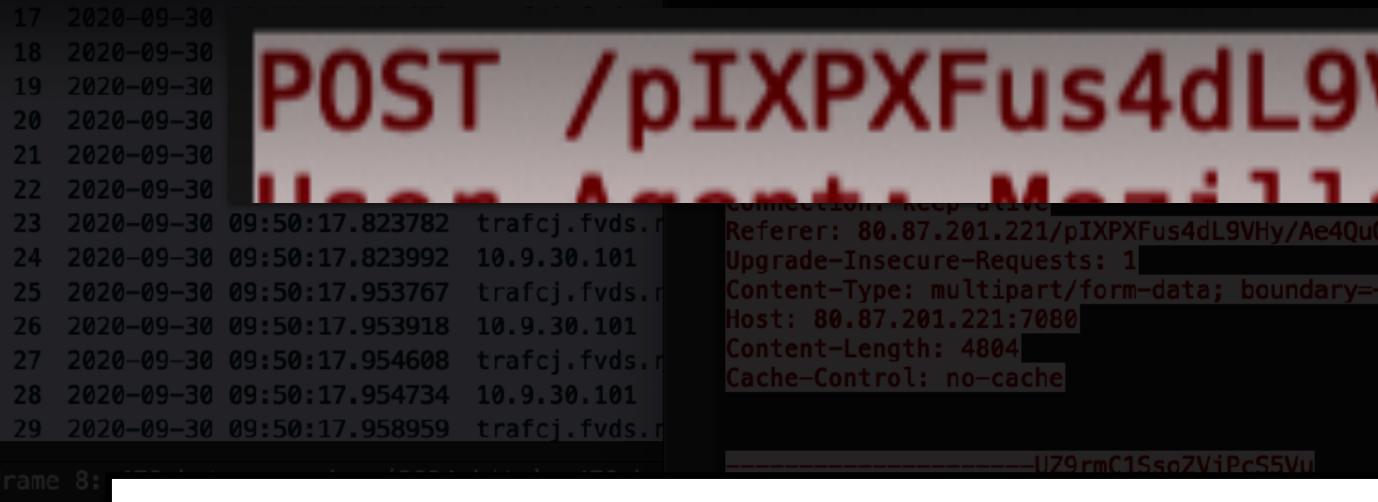
Tab Size: 4

#### ctivity, and the bottom is the PCAP.

1SsoZVjPcS5Vu ata; name="emdseqxxlbwpxzof"; filename="rhyjvabjbzq" ctet-stream
0c.
&F.%{.3<*5o0x S,[ 9&ia a:k.i <n!vcebc.e{.8=*0,.xt?dzz JE.v&amp;5L .]+.#5B.mQJC9v.E.7y.[.\$'</n!vcebc.e{.8=*0,.xt?dzz 
lZ.&.S3;V+x.R
/.//f.k.12!q.0v(gn.90R,CV 7.+T.Ra=."\T,; w:%bjE.b W~IdC.},.[Q.9\$%p3'P.+.3fb\ .2.k.KYi.E</td
H&0@M.:v_e.#z.\(.>



## content:"POST"



**Notes for the Viewer:** The IDS rule looks for POST



Z9rmC1SsoZVjPcS5Vu--.....

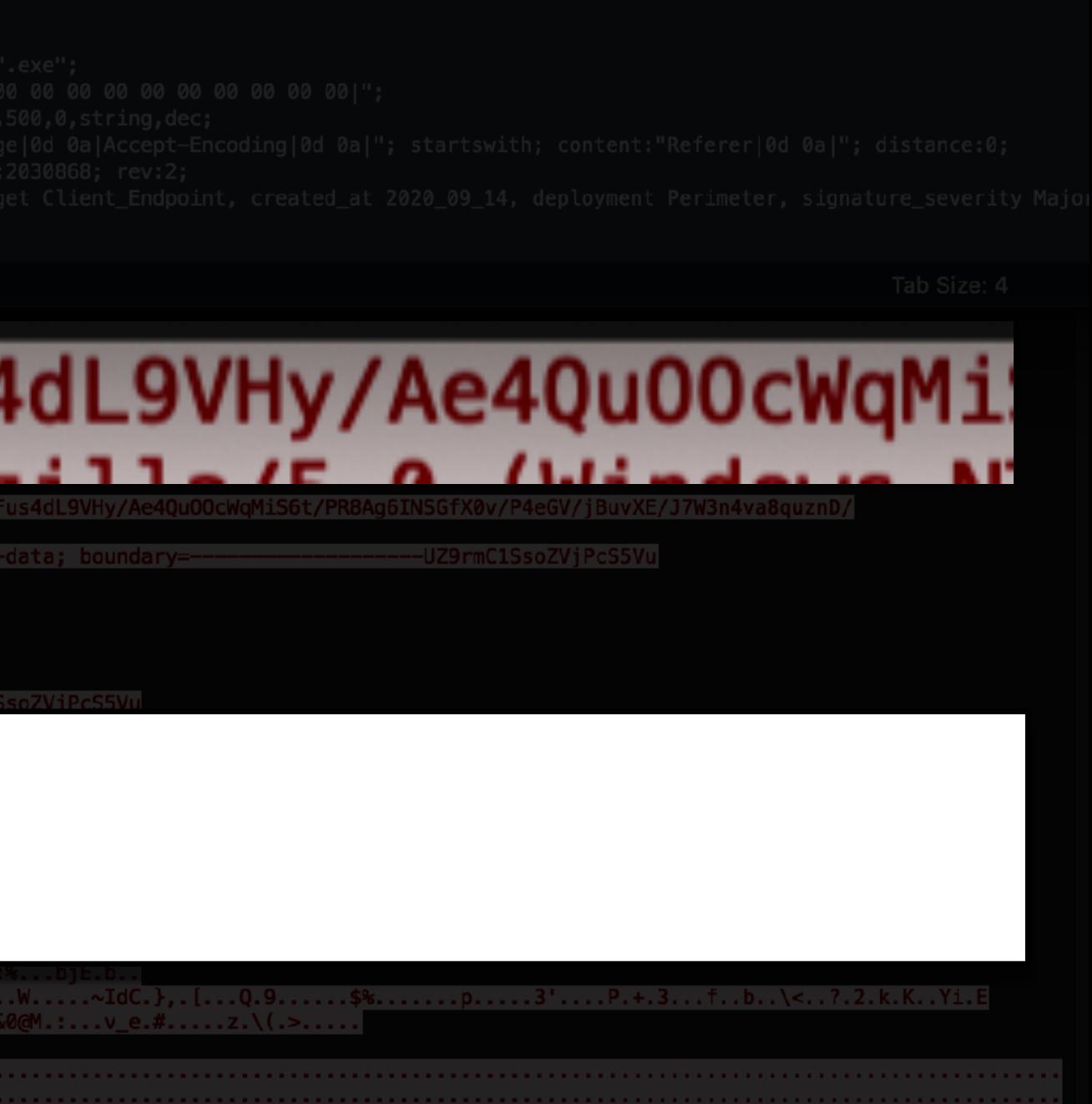
# POST /pIXPXFus4dL9VHy/Ae4Qu00cWqMi

221/pIXPXFus4dL9VHy/Ae4QuOOcWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/

-UZ9rmC1SsoZVjPcS5Vu

UZ9rmC1SsoZViPcS5Vu

r.q\.ao.`...%z..c{...C....W....~IdC.},.[...Q.9.....\$%.....p....3'....P.+.3...f..b..\<..?.2.k.K..Yi.E .....R".3.....\*..N.'.2.H&0@M.:...v\_e.#....z.\(.>....



http.user\_agent; content:"Mozilla/5.0 (Windows NT 6.";

19 2( <b>U</b> 21 22 23 24 25 26 27	2020-09-30 2020-09-30 2020-09-30 2020-09-30 2020-09-30 2020-09-30	<b>gent: Moz</b> 09:50:17.014500 09:50:17.614494 09:50:17.823782 09:50:17.823992 09:50:17.953767 09:50:17.953918 09:50:17.954608	<b>illa/5.</b> 10.9.30.101 trafcj.fvds.r 10.9.30.101 trafcj.fvds.r 10.9.30.101 trafcj.fvds.r 10.9.30.101	DNT: 1 Connection: keep-alive Referer: 80.87.201.221/pIXPXF Upgrade-Insecure-Requests: 1 Content-Type: multipart/form- Host: 80.87.201.221:7080 Content-Length: 4804
28 29 Frame Ether Inter Trans [5 Re	2020-09-30 8: net net	09:50:17.954734 09:50:17.958959	10.9.30.101 trafcj.fvds.r	Cache-Control: no-cache

And it looks for the user agent



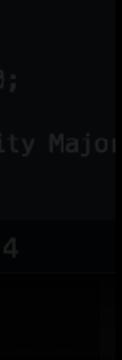
Z9rmC1SsoZVjPcS5Vu--.... 

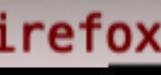
## 3; Win64; x64; rv:75.0) Gecko/20100101 Firefox

4dL9VHy/Ae4Qu00cWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/

ta; boundary=--UZ9rmC1SsoZVjPcS5Vu

z.q\.ao.`...%z..c{...C....W....~IdC.},.[...Q.9.....\$%.....p....3'....P.+.3...f..b..\<..?.2.k.K..Yi.E <.....R".3.....\*..N.'.2.H&0@M.:...v\_e.#....z.\(.>....









**Notes for the Viewer:** Another method of signature-based detection.





## {} YARA in a nutshell

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
    meta:
         description = "This is just an example"
         threat_level = 3
         in_the_wild = true
    strings:
         a = \{6A \ 40 \ 68 \ 00 \ 30 \ 00 \ 00 \ 6A \ 14 \ 8D \ 91\}
```

**Notes for the Viewer:** 



### The pattern matching swiss knife for malware researchers (and everyone else)

### YARA rules are typically used to find data within static files, like HTML or binaries

## yaraPCAP

Yara Scanner For IMAP Feeds and saved Streams

###What it does:

- Reads a PCAP File and Extracts Http Streams.
- gzip deflates any compressed streams
- Scans every file with yara
- writes a report.txt
- optionally saves matching files to a Dir

###Usage

## **Notes for the Viewer:** I found a project that uses YARA against network traffic.

## DEEPSEC

• Yara / PyYara

i yunon

- TCPFlow 1.3 https://github.com/simsong/tcpflow

• For windows edit the Script to point to your copy of the tcpflow binary. Line 29

## • Write a YARA rule:

```
rule emotet : post {
meta:
 author = "Josh Pyorre"
 date = "2022-09-21"
 description = "Emotet"
strings:
 $type="POST"
 $user_agent="Mozilla/5.0 (Windows NT 6."
 $referer="Referer|0d 0a|"
condition:
 ($user_agent) and ($type) and ($content) and ($referer)
}
```

**Notes for the Viewer:** I created a YARA rule based off the IDS rule to capture the Emotet C2 traffic shown in the Suricata example.

## DEEPSEC





jpyorre@evol YaraPcap %

This is a video showing: The same PCAP file is replayed through YARAPCAP. The video shows the YARA rule catching the C2 activity.



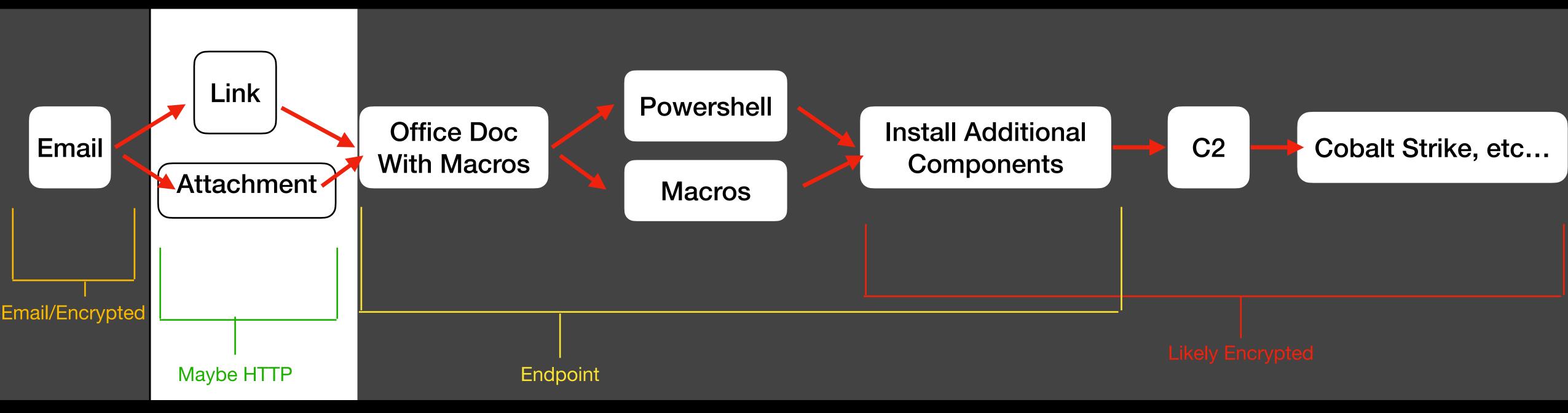
# he Viewer:

Notes for the Viewer: One more piece of context: Visibility is difficult because most traffic is SSL

## DEEPSEC

## VISISING VISISING SSL

## Emotet



Notes for the Viewer: With SSL, you are most likely to see only the



## With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)



## **IcedID Dropper -> Cobalt Strike**

27721	2022-08-10 04:17:47.753017	172.93.98.170	10.8.9.101	ТСР	58	80 → 58697 [SYN, ACK] Seq=0 Ack=1 Win=64240
27722	2022-08-10 04:17:47.753188	10.8.9.101	172.93.98.170	ТСР	54	58697 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=
27723	2022-08-10 04:17:47.753357	10.8.9.101	172.93.98.170	HTTP	132	GET /download/a2.dll HTTP/1.1
27724	2022 00 10 04.17.47 752424	172 02 09 170	10 0 0 101	TCD	E 4	00 . E0607 [ACK] Con-1 Ack-70 Win-64240 Lon

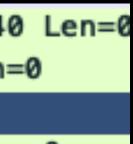
• • •	Wireshark · Follow HTTP Stream (tcp.strea
GET /download/a2.dl	L HTTP/1.1
Connection: Keep-Al	ive
Host: 172.93.98.170	
HTTP/1.1 200 OK	
Date: Wed, 10 Aug 20	
Server: Microsoft-I	IS/8.5
Content-Type: appli	cation/octet-stream
Cache-Control: max-a	age=1
Connections keep als	ive

Notes for the Viewer: With SSL, you are most likely to see only the



eam eq 1020) · 2022-08-09-IcedID-part-2-with-Cobalt-Strike.pcap

## With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)





## IcedID Dropper -> Cobalt Strike

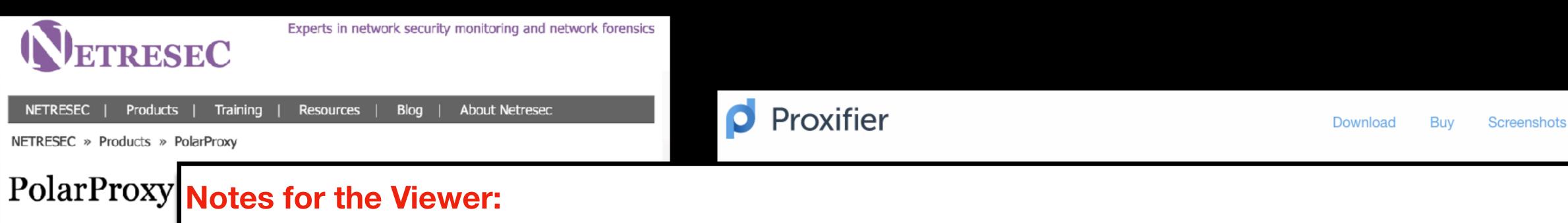
30047	2022-08-10 04:17:49.014657	172.93.98.170	10.8.9.101	HTTP	714 HTTP/1.1 200 OK
30048	2022-08-10 04:17:49.014680	10.8.9.101	172.93.98.170	TCP	54 58697 → 80 [ACK] Seq=79 Ack=2134239 Win=63580 Len=0
30049	2022-08-10 04:17:49.015324	10.8.9.101	172.93.98.170	TCP	54 58697 → 80 [FIN, ACK] Seq=79 Ack=2134239 Win=63580 Len=0
30050	2022-08-10 04:17:49.015349	172.93.98.170	10.8.9.101	ТСР	54 80 → 58697 [ACK] Seq=2134239 Ack=80 Win=64239 Len=0
30051	2022-08-10 04:17:49.151010	213.227.154.169	10.8.9.101	TLSv1	220 Change Cipher Spec, Application Data, Application Data
30052	2022-08-10 04:17:49.151105	10.8.9.101	213.227.154.169	TCP	54 58699 → 443 [ACK] Seq=365 Ack=300 Win=65535 Len=0
30053	2022-08-10 04:17:49.151485	10.8.9.101	213.227.154.169	TLSv1	134 Change Cipher Spec, Application Data
30054	2022-08-10 04:17:49.151553	213.227.154.169	10.8.9.101	ТСР	54 443 → 58699 [ACK] Seq=300 Ack=445 Win=64240 Len=0
30055	2022-08-10 04:17:49.151944	10.8.9.101	213.227.154.169	TLSv1	579 Application Data
30056	2022-08-10 04:17:49.151972	213.227.154.169	10.8.9.101	TCP	54 443 → 58699 [ACK] Seq=300 Ack=970 Win=64240 Len=0
30057	2022-08-10 04:17:49.172055	213.227.154.169	10.8.9.101	TLSv1	1376 Application Data, Application Data, Application Data, Application Data
30058	2022-08-10 04:17:49.172118	10.8.9.101	213.227.154.169	тср	54 58698 → 443 [ACK] Seq=970 Ack=1711 Win=65535 Len=0

Notes for the Viewer: With SSL, you are most likely to see only the



### With SSL, you are most likely to see only the initial second-stage GET request over HTTP (maybe)





responders and malware res malware. PolarProxy decrypt while also saving the decryp be loaded into Wireshark or (IDS).

Here is an example PCAP fil https://www.netresec.com

PolarProxy for Linux x64

PolarProxy for Linux ARM

PolarProxy for Linux AArch64/ARM64

PolarProxy for macOS x64 (Intel)

PolarProxy for macOS ARM64 (M1/M2)

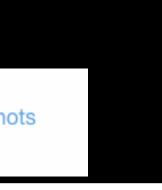
https://www.netresec.com/?page=PolarProxy



PolarProxy is a transparent a Many solutions exist for decrypting your networks SSL traffic for analysis. Most companies won't designed to intercept and de give you access to that data, just decrypting it for use against their security products. If you are doing this yourself though, there are several options. Here I talk about using PolarProxy to MITM your SSL, writing out clear text PCAPs. It forwards the traffic to the destination still encrypted. It's a free method to provide visibility into your network. Proxifier is a Windows proxy solution that will send all traffic through a proxy. There are options available for OSX and Linux as well.



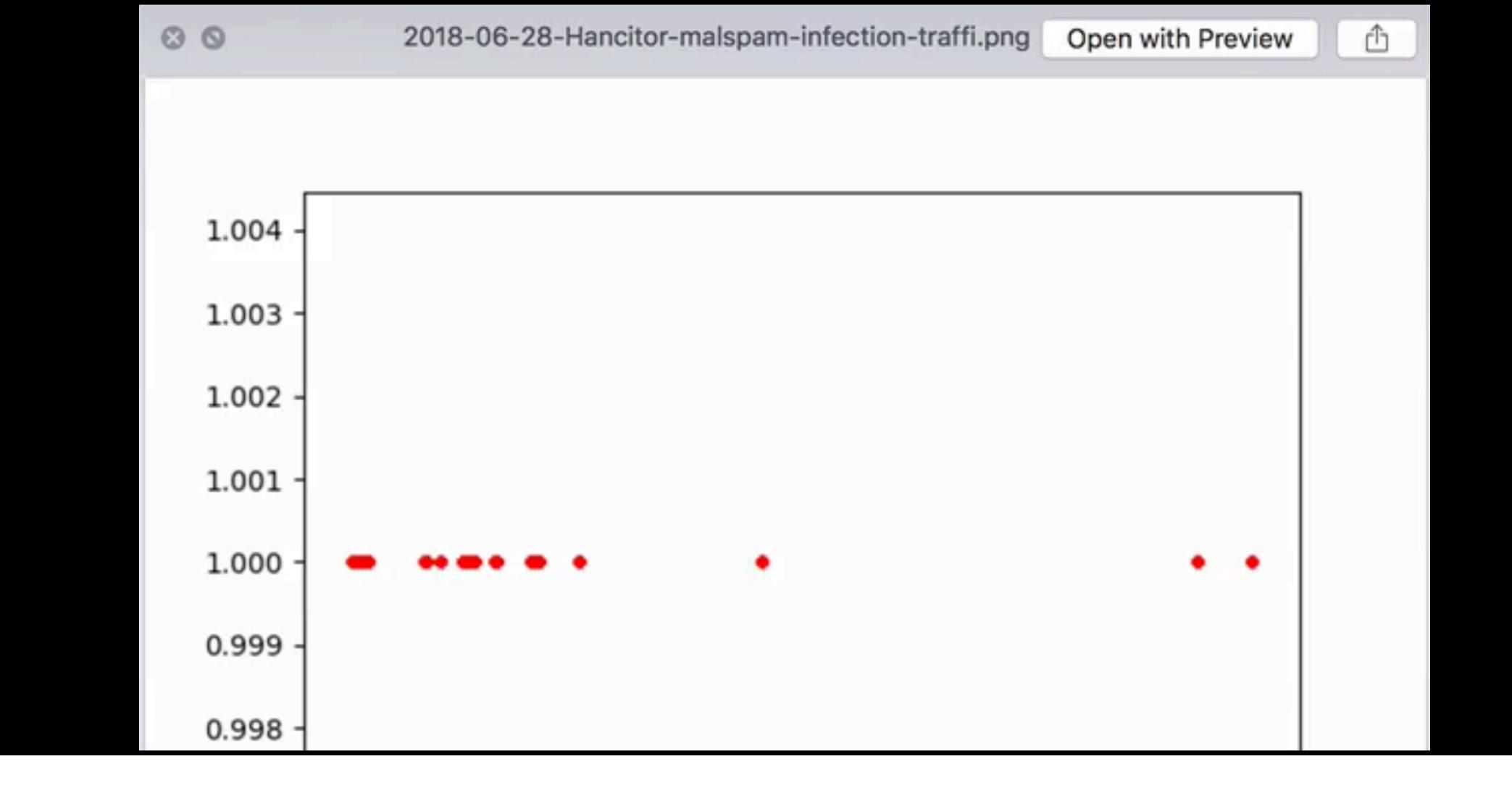
https://www.netresec.com/?page=PolarProxy





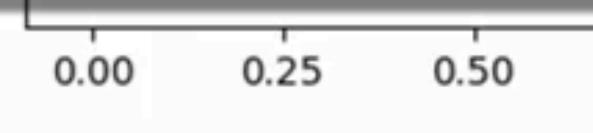


Can we build a signature Using network Timing?



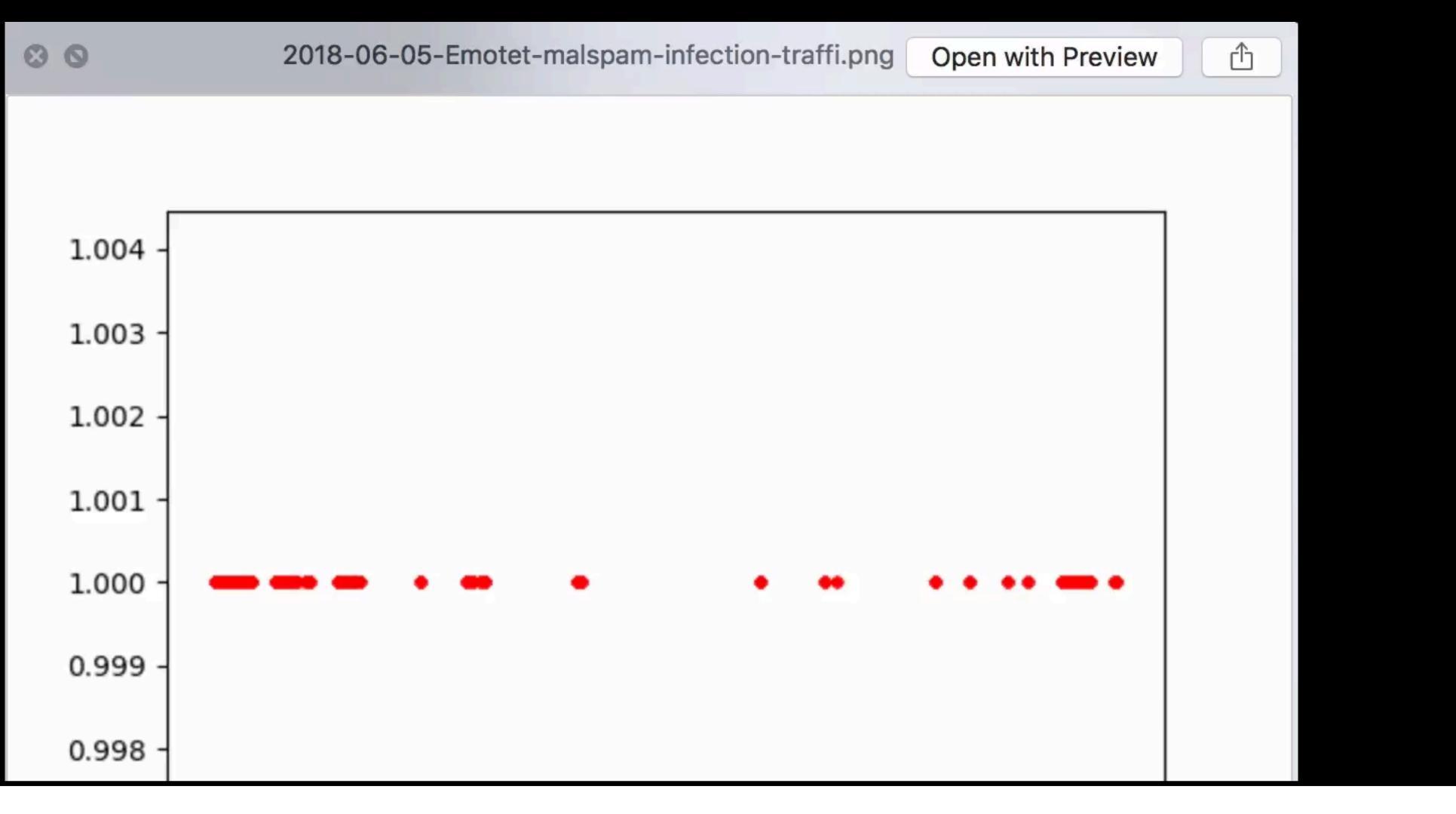
Hancitor malware and how the timing of network transactions is similar.





## Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for

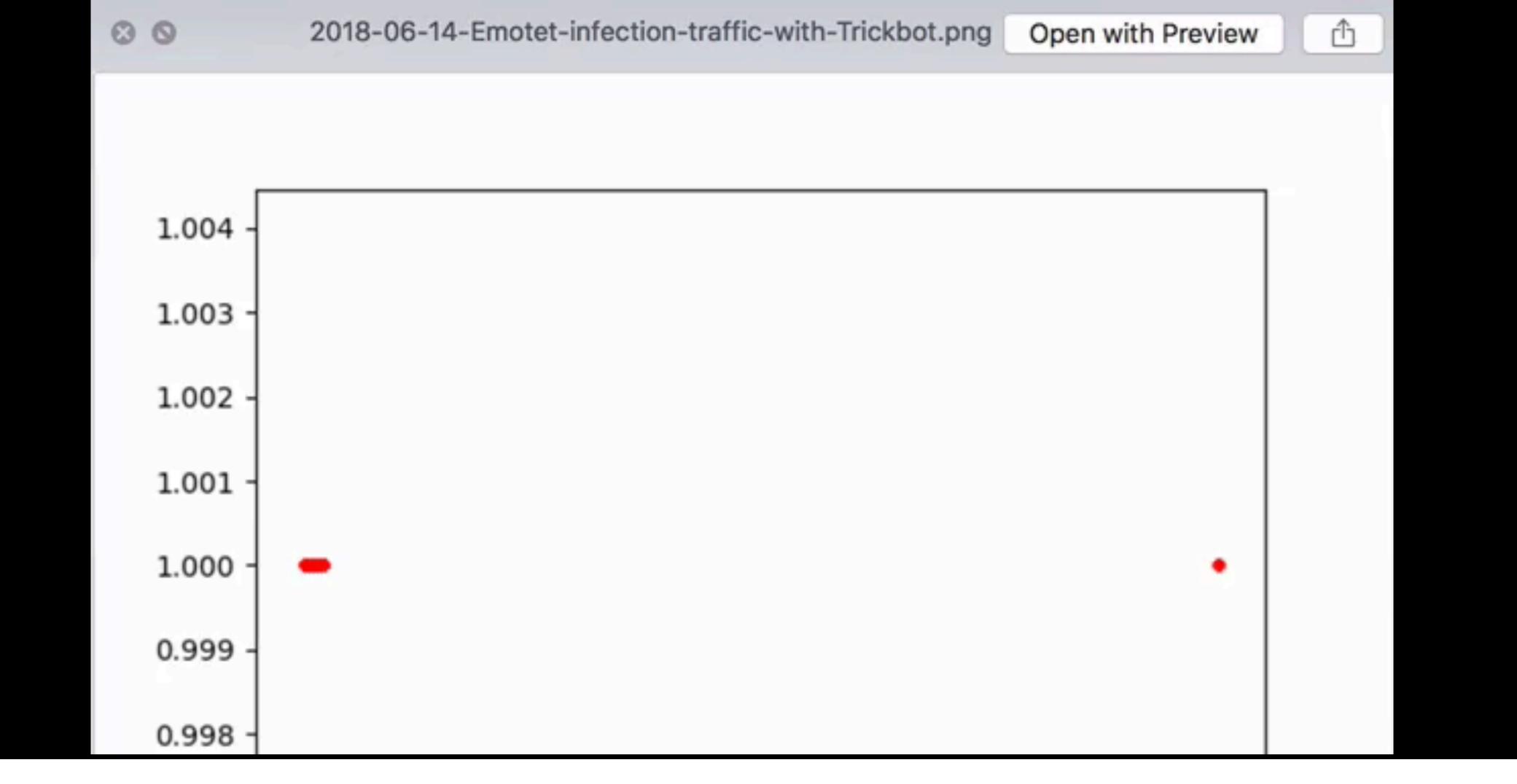
0 75	1 00	1 05	1 50	
0.75	1.00	1.25	1.50	
				1e9



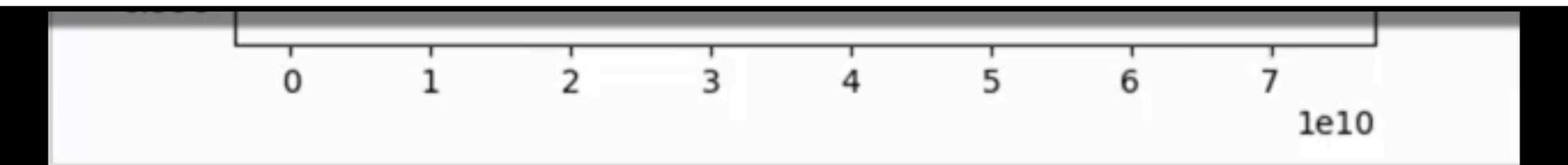
## Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for Emotet malware and how the timing of network transactions is similar.



0.0 0.2 0.4 0.6 0.8 1.0 1.2 1.4									
	0.0	0.2	0.4	0.6	0.8	1.0	1.2	1.4	
									1e9



## Video showing the initial thing that gave me this idea. Comparing multiple similar PCAPs for Trickbot malware and how the timing of network transactions is similar.





**Notes for the Viewer:** Beginning the process of trying to find patterns that can be used to create a signature.



# **Finding Patterns**

**Notes for the Viewer:** We'll start by looking at dropper downloads.



# Dropper Downloads

·//////	tranes	notione	
ZUUZ	llalisc	actions	

### Two Separate icedID Downloads

<b>0</b>				
() /	' trar	isac	TIO	ns
		1000		

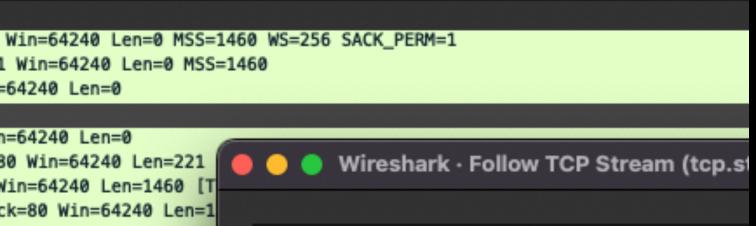
	Protoc	Leng	Info		
	тср	66	63087 → http(80)	[SYN,	ECN, CWR] Seq=0 W
'	тср	58	http(80) → 63087	[SYN,	ACK] Seq=0 Ack=1
1	тср	54	63087 → http(80)	[ACK]	Seq=1 Ack=1 Win=6
	НТТР	133	GET /download/ms	b.exe	HTTP/1.1
	тср	54	http(80) → 63087	[ACK]	Seq=1 Ack=80 Win=
1	тср	275	http(80) → 63087	[PSH,	ACK] Seq=1 Ack=80
	тср	1514	http(80) → 63087	[ACK]	Seq=222 Ack=80 Wi
	тср	1346	http(80) → 63087	[PSH,	ACK] Seq=1682 Ack
	тср	54	63087 → http(80)	[ACK]	Seq=80 Ack=2974 V
	тср	1514	http(80) → 63087	[ACK]	Seq=2974 Ack=80 V
	тср	1514	http(80) → 63087	[ACK]	Seq=4434 Ack=80 W
1	тср	1514	http(80) → 63087	[ACK]	Seq=5894 Ack=80 V
	тср	1178	http(80) → 63087	[PSH,	ACK] Seq=7354 Ack
,	тср	1514	http(80) → 63087	[ACK]	Seg=8478 Ack=80 V
,	тср	1514	http(80) → 63087	[ACK]	Seq=9938 Ack=80 V
	тср	1262	http(80) → 63087	[PSH,	ACK] Seg=11398 Ad
	тср	54	63087 → http(80)	[ACK]	Seg=80 Ack=12606
,	тср	1514	http(80) → 63087	[ACK]	Seg=12606 Ack=80
,	тср	1346	http(80) → 63087	[PSH,	ACK] Seg=14066 Ad
	TCP	54	63087 → http(80)		Seg=80 Ack=15358
	TCP	1514	http(80) → 63087		Seg=15358 Ack=80
	TCP	1346	http(80) → 63087		ACK] Seq=16818 A

Protoc	Leng	Info
TCP	66	50462 → http(80) [SYN] Seq=0 Win
TCP	58	<pre>http(80) → 50462 [SYN, ACK] Seq=</pre>
TCP	54	50462 → http(80) [ACK] Seq=1 Ack
HTTP	135	GET /download/sys.exe HTTP/1.1
TCP	54	http(80) → 50462 [ACK] Seq=1 Ack
TCP	274	<pre>http(80) → 50462 [PSH, ACK] Seq=</pre>
TCP	1442	<pre>http(80) → 50462 [PSH, ACK] Seq=</pre>
TCP	54	50462
TCP	1442	http( 🛑 😑 🔵 Wireshark · Fol
TCP	1442	http(
TCP	54	50462
TCP	1442	http: GET /download/sys.exe H
TCP	1442	http( Connection: Keep-Alive
TCP	54	50462 Host: 104.238.220.131
TCP	1442	http( HTTP/1.1 200 OK
TCP	1442	http( Date: Mon, 8 Aug 2022 2
TCP	1442	http( Server: Microsoft-IIS/8
TCP	54	50462 Content-Type: applicati

### **Notes for the Viewer: Two similar PCAPs**

TCP	1514	httpl	MZ
TCP	1370	http(	program cannot be run in
TCD	54	50462	

## DEEPSEC



Win=64240 Len=0 Win=64240 Len=1460 Win=64240 Len=1460 Win=64240 Len=1460 ck=80 Win=64240 Len=1 Win=64240 Len=1460 Win=64240 Len=1460 ck=80 Win=64240 Len= Win=64240 Len=0 Win=64240 Len=1460 ck=80 Win=64240 Len= Win=64240 Len=0 Win=64240 Len=1460 ck=80 Win=64240 Len=

GET /download/msb.exe HTTP/1.1 Connection: Keep-Alive Host: 209.222.98.13 HTTP/1.1 200 OK Date: Mon, 25 Jul 2022 19:56:38 GMT Server: Microsoft-IIS/8.5 Content-Type: application/octet-stream Cache-Control: max-age=1 Connection: keep-alive X-Powered-By: ASP.NET Content-Length: 2134016

MZ.....@.....@ program cannot be run in DOS mode.

n=64240 Len=0 MSS=1460 WS=256 SACK\_PER =0 Ack=1 Win=64240 Len=0 MSS=1460 k=1 Win=64240 Len=0

k=82 Win=64240 Len=0 =1 Ack=82 Win=64240 Len=220 [TCP segme =221 Ack=82 Win=64240 Len=1388 [TCP se

llow TCP Stream (tcp.stream eq 0) ·

### HTTP/1.1

21:27:00 GMT 8.5 ion/octet-stream

n DOS mode.

2052	trans	actions

Protoc	Leng	Info		
TCP	66	63087 → http(80)	[SYN,	ECN, CWR] Seq=0 Win=64240 Len=0 MSS=14
TCP	58	http(80) → 63087	[SYN,	ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
TCP	54	63087 → http(80)	[ACK]	Seq=1 Ack=1 Win=64240 Len=0
HTTP	133	GET /download/mst	o.exe	HTTP/1.1
TCP	54	http(80) → 63087	[ACK]	Seq=1 Ack=80 Win=64240 Len=0
TCP	275	http(80) → 63087	[PSH,	ACK] Seq=1 Ack=80 Win=64240 Len=221
TCP	1514	http(80) → 63087	[ACK]	Seq=222 Ack=80 Win=64240 Len=1460 [T
TCP	1346	http(80) → 63087	[PSH,	ACK] Seq=1682 Ack=80 Win=64240 Len=1
TCP	54	63087 → http(80)	[ACK]	Seq=80 Ack=2974 Win=64240 Len=0
TCP	1514	http(80) → 63087	[ACK]	Seq=2974 Ack=80 Win=64240 Len=1460 [
TCP	1514	http(80) → 63087	[ACK]	Seq=4434 Ack=80 Win=64240 Len=1460 [
TCP	1514	http(80) → 63087	[ACK]	Seq=5894 Ack=80 Win=64240 Len=1460 [
TCP	1178	http(80) → 63087	[PSH,	ACK] Seq=7354 Ack=80 Win=64240 Len=1
TCP	1514	http(80) → 63087	[ACK]	Seq=8478 Ack=80 Win=64240 Len=1460 [
TCP	1514	http(80) → 63087	[ACK]	Seq=9938 Ack=80 Win=64240 Len=1460 [
TCP	1262	http(80) → 63087	[PSH,	ACK] Seq=11398 Ack=80 Win=64240 Len=
TCP	54	63087 → http(80)	[ACK]	Seq=80 Ack=12606 Win=64240 Len=0
TCP	1514	http(80) → 63087	[ACK]	Seq=12606 Ack=80 Win=64240 Len=1460
TCP	1346	http(80) → 63087	[PSH,	ACK] Seq=14066 Ack=80 Win=64240 Len=
TCP	54	63087 → http(80)	[ACK]	Seq=80 Ack=15358 Win=64240 Len=0
TCP	1514	http(80) → 63087	[ACK]	Seq=15358 Ack=80 Win=64240 Len=1460
TCP	1346	http(80) → 63087	[PSH,	ACK] Seq=16818 Ack=80 Win=64240 Len=

### Similar byte lengths

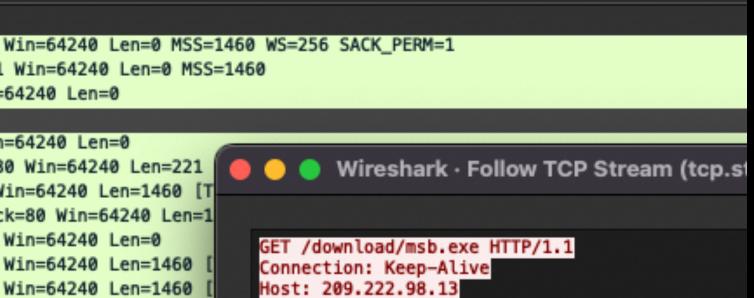
110

9010	Protoc   I	Leng	Info
	TCP	66	50462 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS
	TCP	58	<pre>http(80) → 50462 [SYN, ACK] Seq=0 Ack=1 Win=6424</pre>
	TCP	54	50462 → http(80) [ACK] Seq=1 Ack=1 Win=64240 Len
	HTTP	135	GET /download/sys.exe HTTP/1.1
07 transactions	TCP	54	<pre>http(80) → 50462 [ACK] Seq=1 Ack=82 Win=64240 Let</pre>
	TCP	274	http(80) → 50462 [PSH, ACK] Seq=1 Ack=82 Win=642
	TCP	1442	<pre>http(80) → 50462 [PSH, ACK] Seq=221 Ack=82 Win=6-</pre>
	TCP	54	50462
	TCP	1442	http( 🛑 😑 🔵 Wireshark · Follow TCP Stream
	TCP	1442	http(
	TCP	54	50462
	TCP	1442	http( GET /download/sys.exe HTTP/1.1
	TCP	1442	http( Connection: Keep-Alive
	TCP	54	50462 Host: 104.238.220.131
	TCP	1442	http( HTTP/1.1 200 OK
	TCP	1442	http: Date: Mon, 8 Aug 2022 21:27:00 GMT
	TCP	1442	http: Server: Microsoft-IIS/8.5
	TCP	54	50462 Content-Type: application/octet-stream

## **Notes for the Viewer: They have similar byte lengths**

TCP	1514	httpl	MZ
TCP	1370	http(	program cannot be run in
TCD	54	50467	

## DEEPSEC



HTTP/1.1 200 OK Date: Mon, 25 Jul 2022 19:56:38 GMT Server: Microsoft-IIS/8.5 Content-Type: application/octet-stream Cache-Control: max-age=1 Connection: keep-alive X-Powered-By: ASP.NET Content-Length: 2134016

MZ.....@.....@..... program cannot be run in DOS mode.

=64240 Len=0 MSS=1460 WS=256 SACK\_PER Ack=1 Win=64240 Len=0 MSS=1460 =1 Win=64240 Len=0

=82 Win=64240 Len=0 Ack=82 Win=64240 Len=220 [TCP segme 221 Ack=82 Win=64240 Len=1388 [TCP se

ow TCP Stream (tcp.stream eq 0) ·

### TTP/1.1

n DOS mode.

2052 transactions	Difference	in	microseconds:	9
			microseconds:	
	Difference	in	microseconds:	2

Similar timing, at least in the beginning (The GET request)	Difference	in	microseconds: microseconds: microseconds:	82
	Difference	in	microseconds:	50
	Difference	in	microseconds:	629
1107 transactions	Difference	in	microseconds:	318
	Difference	in	microseconds:	92

## Notes for the Viewer: Looking at the time in between transactions, there are some similarities



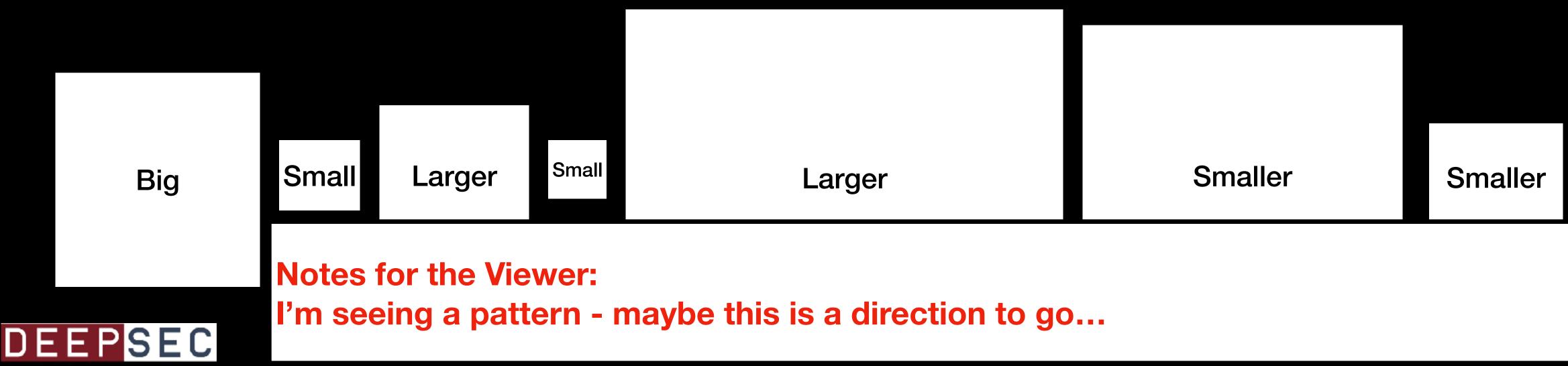
93622 (12:56:39.441422 - 12:56:39.535044) 98 (12:56:39.535044 - 12:56:39.535142) 159 (12:56:39.535142 - 12:56:39.535301) 56 (12:56:39.535301 - 12:56:39.535357) 92677 (12:56:39.535357 - 12:56:39.628034) 1444 (12:56:39.628034 - 12:56:39.629478) 21 (12:56:39.629478 - 12:56:39.629499)

3480 (14:27:00.681914 - 14:27:00.740394) 2 (14:27:00.740394 - 14:27:00.740476) 30 (14:27:00.740476 - 14:27:00.740656) 0 (14:27:00.740656 - 14:27:00.740706) 2994 (14:27:00.740706 - 14:27:00.803700) 189 14:27:00.803700 - 14:27:00.806889) 2 (14:27:00.806889 - 14:27:00.806981)

Insactions	Difference	in	microseconds:	9
	Difference	in	microseconds:	9
	Difference	in	microseconds:	1
	Difference	in	microseconds:	5
	Difference	in	microseconds:	9
	Difference	in	microseconds:	1
	Difference	in	microseconds:	2

Similar timing, at least in the beginning (The GET request)	Difference Difference	in in	microseconds: microseconds: microseconds:	82 180
			microseconds: microseconds:	
1107 transactions			microseconds: microseconds:	

2052 tra



93622 (12:56:39.441422 - 12:56:39.535044) (12:56:39.535044 - 12:56:39.535142) 98 (12:56:39.535142 - 12:56:39.535301) 159 (12:56:39.535301 - 12:56:39.535357) 56 (12:56:39.535357 - 12:56:39.628034) 92677 (12:56:39.628034 - 12:56:39.629478)1444 21 (12:56:39.629478 - 12:56:39.629499)

(14:27:00.681914 - 14:27:00.740394) 480 (14:27:00.740394 - 14:27:00.740476) (14:27:00.740476 - 14:27:00.740656)(14:27:00.740656 - 14:27:00.740706)994 (14:27:00.740706 - 14:27:00.803700) 14:27:00.803700 - 14:27:00.806889) .89 (14:27:00.806889 - 14:27:00.806981)

**Notes for the Viewer:** Let's look at C2 beaconing

## DEEPSEC

Beaconing

· · ·			
Time	Source	Destination	Protoc   Leng   Info
0.000000	10.7.25.2	21-193-93-172.reverse-dns	TCP 66 63089 → https(443) [SYN, ECN, CWR] Seq=0 Win=
0.437583	21-193-93-172.reverse-dns	10.7.25.2	TCP 58 https(443) → 63089 [SYN, ACK] Seq=0 Ack=1 Wir
0.437723	10.7.25.2	21-193-93-172.reverse-dns	TCP 54 63089 → https(443) [ACK] Seq=1 Ack=1 Win=6553
0.441232	10.7.25.2	21-193-93-172.reverse-dns	TLSv1 322 Client Hello
0.441367	21-193-93-172.reverse-dns	10.7.25.2	TCP 54 https(443) → 63089 [ACK] Seq=1 Ack=269 Win=64
0.598193	21-193-93-172.reverse-dns	10.7.25.2	TLSv1 1514 Server Hello, Change Cipher Spec, Application
0.598216	21-193-93-172.reverse-dns	10.7.25.2	
0.598331	10.7.25.2	21–193–93–172. re 🔴 💛 🕒 Wiresh	hark · Follow TCP Stream (tcp.stream eq 0) · 2022-07-25-IcedID-v
0.724488	21-193-93-172.reverse-dns	10.7.25.2	
0.724615	10.7.25.2	21–193–93–172. ге	
0.729226	10.7.25.2	21–193–93–172. re	.P!0&{.@YZ#;5U]G.WR.Z. <gg.cp*.hp(< td=""></gg.cp*.hp(<>
0.729502	21–193–93–172.reverse-dns	10.7.25.2 (.'.	
0.868485	21-193-93-172.reverse-dns		=.<.5./sezijiru.com+
0.868600	10.7.25.2	21 - 102 - 02 - 172 mm	.\$q/.`Z~
1.268318	10.7.25.2		zv8[j.ZQ.][*.ic.'."(
1.268487	21-193-93-172.reverse-dns	10.7.25.2G.WR.Z. <g< td=""><td>g.CP*.hp+3.\$pdl&gt;a&amp;&amp;B.0}</td></g<>	g.CP*.hp+3.\$pdl>a&&B.0}
1.397717	21–193–93–172.reverse–dns	10.7.25.2 .p.#\f.K	.(T.P.}.)*Fcb{mg7yu.Y.`]sl.:]syep P4
1.397851	10.7.25.2		i?D\$S.C+cfa'.No}.=OBl.f.U/*q.#.\Y.
1.398339	21–193–93–172.reverse–dns		[Ro
1.398353	21-193-93-172.reverse-dns	10.7.25.2 {plpk	.0(0g.a.@.?}`l2^]hkWJ.0Vix';N'.c%\
1.398364	21-193-93-172.reverse-dns		; S&q.07%vw}{.&n.#}X!.BM}d8I)0B.
1.398373	21-193-93-172.reverse-dns		MT.AD.5.t.E}.!.21FLt.(V].GM.D.1
1. 66 butos s	n viro (E20 bits) 66 butos cont		?AxM.W"M6zYxk,.W{yI
	on wire (528 bits), 66 bytes captu NovilettB 15:47:50 (00:08:02:15:47:		.cl)T.P>A.d
	<pre>iewlettP_1c:47:ae (00:08:02:1c:47: /emailer 4</pre>		
	/ersion 4, Src: 10.7.25.2 (10.7.25		YAT,od?j .X.w.KPWUC.M.4.\$.0:x.BG.P0
mission Contro	l Protocol, Src Port: 63089 (6308		c.:DBImoS. <qhc.c.].bt:( 8.tw.7.< td=""></qhc.c.].bt:( 8.tw.7.<>

l ime	Source	Destination	Protoc	-	•
0.00000	10.8.8.101	193.109.120.51	TCP	66	50063 → https(443) [SYN] Seq=0 Win=64240 Len
0.185307	193.109.120.51	10.8.8.101	ТСР	58	<pre>https(443) → 50063 [SYN, ACK] Seq=0 Ack=1 Win</pre>
0.185736	10.8.8.101	193.109.120.51	TCP	54	50063 → https(443) [ACK] Seq=1 Ack=1 Win=6424
0.186912	10.8.8.101	193.109.120.51	TLSv1	329	Client Hello
0.186956	193.109.120.51	10.8.8.101	TCP	54	https(443) → 50063 [ACK] Seq=1 Ack=276 Win=64
0.386316	193.109.120.51	10.8.8.101	TLSv1	1348	Server Hello, Certificate, Server Key Exchange
0.387282	10.8.8.101	193.10 <u>9.120.51</u>	TLSv1	147	Client Key Exchange, Change Cipher Spec, Enc.
0.387359	193.109.120.51	10.8. 👝 👝 Wireshark · Follow	N TCP S	tream	(tcp.stream eq 0) · 2022-08-08-IcedID-wit
0.570262	193.109.120.51	10.8.			
0.578222	10.8.8.101	193.1			
0.578279	10.8.8.101	193.1			
0.578309	193.109.120.51	10.8.	10	11. 1	t.bQ"hAO.`m.o.:(,.+.0./.\$.#
0.578338	193.109.120.51				ultomductingbig.pro++
1.791292	193.109.120.51	10.8.	#		
1.806082	10.8.8.101	193.1	.FiZ	.bMn.	LM.44/h.1
1.806213	193.109.120.51	10.8.: +fgJwh#C@C\0	0 0	k	01 0

## Notes for the Viewer: Two similar PCAPs with CobaltStrike beaconing

### Cobalt Strike Beaconing, Sample 1

Cobalt Strike Beaconing, Sample

## DEEPSEC



Cobalt Strike Beaconing, Sample 1 279 Packets Difference Difference Difference Difference Difference Difference Difference Difference Difference Difference	in n in n in n in n in n in n	
--	--	--

### Notes for the Viewer: Looking at the time in between transactions, there are some similarities

Cobalt Strike Beaconing, Sample 2

24 Packets Difference in microseconds: 185307 (13:15:56.474085 - 13:15:56.659392) Difference in microseconds: 429 (13:15:56.659392 - 13:15:56.659821) Difference in microseconds: 1176 (13:15:56.659821 – 13:15:56.660997) Difference in microseconds: 44 (13:15:56.660997 - 13:15:56.661041) Difference in microseconds: 199360 (13:15:56.661041 - 13:15:56.860401) Difference in microseconds: 966 (13:15:56.860401 - 13:15:56.861367) Difference in microseconds: 77 (13:15:56.861367 – 13:15:56.861444) Difference in microseconds: 182903 (13:15:56.861444 - 13:15:57.044347) Difference in microseconds: 7960 (13:15:57.044347 - 13:15:57.052307)



icroseconds: 437583 (12:56:54.546469 - 12:56:54.984052) icroseconds: 140 (12:56:54.984052 - 12:56:54.984192) icroseconds: 3509 (12:56:54.984192 - 12:56:54.987701) icroseconds: 135 (12:56:54.987701 - 12:56:54.987836) icroseconds: 156826 (12:56:54.987836 - 12:56:55.144662) icroseconds: 23 (12:56:55.144662 - 12:56:55.144685) icroseconds: 115 (12:56:55.144685 - 12:56:55.144800) icroseconds: 126157 (12:56:55.144800 - 12:56:55.270957) icroseconds: 127 (12:56:55.270957 - 12:56:55.271084)





### Emotet and Trickbot beacon 1:

		1		
ource	Destination	Protoc   Le		
0.87.201.221	DESKTOP-USER1PC.local			empowerid(7080) → 64263 [ACK] Seq=1073301 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local		514	empowerid(7080) → 64263 [ACK] Seq=1074761 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP 1	514	empowerid(7080) → 64263 [ACK] Seq=1076221 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP 1	514	empowerid(7080) → 64263 [ACK] Seq=1077681 Ack=32543 Win=64240 Len=1460 [TCP segment
ESKTOP-USER1PC.local	80.87.201.221	TCP	54	64263 → empowerid(7080) [ACK] Seq=32543 Ack=1068921 Win=65535 Len=0
0.87.201.221	DESKTOP-USER1PC.local	TCP 1	514	empowerid(7080) → 64263 [ACK] Seq=1079141 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP 1	514	empowerid(7080) → 64263 [ACK] Seq=1080601 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP 1	514	empowerid(7080) → 64263 [ACK] Seq=1082061 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP 15	514	empowerid(7080) → 64263 [ACK] Seq=1083521 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCP	114	empowerid(7080) → 64263 [PSH, ACK] Seq=1084981 Ack=32543 Win=64240 Len=60 [TCP segme
0.87.201.221	DESKTOP-USER1PC.local	TCP 1		empowerid(7080) → 64263 [ACK] Seq=1085041 Ack=32543 Win=64240 Len=1460 [TCP segment
0.87.201.221	DESKTOP-USER1PC.local	TCD 11	614	amoussid/7000) . 64762 [ACK] Cos-1006501 Ack-27542 Wis-64240 Lon-1460 [TCD cosmont
0.87.201.221	DESKTOP-USER1PC.local	😑 🔵 Wireshark 🛛	Follo	llow TCP Stream (tcp.stream eq 11) · 2020-09-30-Emotet-infection-with-Trickb
0.87.201.221	DESKTOP-USER1PC.local			
0.87.201.221	DESKTOP-USER1PC.local			
0.87.201.221	DESKTOP-USER1PC.local	POST /pIXPXFus4dL9VH	v/Ae4	e4Qu00cWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/ HTTP/1.1
0.87.201.221				(Windows NT 6.3; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
ESKTOP-USER1PC.local				<pre>cation/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8</pre>
0.87.201.221		Accept-Language: en-l		
0.87.201.221		Accept-Encoding: gzi; DNT: 1	ρ, αε	det late
0.87.201.221	DECKTOD ICEDIDC LOCAL	Connection: keep-aliv	ve	
ESKTOP-USER1PC.local				pIXPXFus4dL9VHy/Ae4Qu00cWgMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/
ESKTOP-USER1PC.local	80.87.201.221	Upgrade-Insecure-Requ	uests	ts: 1
ESKTOP-USER1PC.local				/form-data; boundary=UZ9rmC1SsoZVjPcS5Vu
ESKTOP-USER1PC.local		Host: 80.87.201.221:7		
ESKTOP-USER1PC.local	00.0/./01.//1	Content-Length: 4804 Cache-Control: no-cao		
ESKTOP-USER1PC.local	80.87.201.221		cne	
s on wire (4208 bits), 526 bytes	captured (4200 bitc)			
vlettP_1c:47:ae (00:08:02:1c:47:	- A Brits Hilton - AB A			9rmC1SsoZVjPcS5Vu
rsion 4, Src: DESKTOP-USER1PC.lo				<pre>rm-data; name="emdseqxxlbwpxzof"; filename="rhyjvabjbzq"</pre>
Protocol, Src Port: 64263 (6426		Content-Type: applica	ation	on/octet-stream
		?.VP.we.0.tn)		Active sectors and the sector sectors and the
egments (5499 bytes): #2352(647)	, #2353(1400), #2354(.			.V+&F.%{.3<*500x S,[]9&ia
rotocol				ya:k.i <n!vcebc.e{.8=*0< td=""></n!vcebc.e{.8=*0<>
Encapsulation, Type: multipart/				tiJE.v&5Ll.l+.#5B.m0JC9v.E.7v.[.\$'

### Encap

Source

bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
bd2212fc.virtua.com.br	10.12.29.101
10.12.29.101	bd2212fc.virtu
	10.12.29.101 10.12.29.101 10.12.29.101 10.12.29.101 10.12.29.101 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br bd2212fc.virtua.com.br bd2212fc.virtua.com.br bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br 10.12.29.101 bd2212fc.virtua.com.br

| Destination bd2212fc.virt

bytes on wire (10064 bits), 1258 bytes captured ( HewlettP\_1c:47:ae (00:08:02:1c:47:ae), Dst: Neto Version 4, Src: 10.12.29.101 (10.12.29.101), Dst rol Protocol, Src Port: 61117 (61117), Dst Port: P Segments (7466 bytes): #7436(422), #7437(1460),

### Emotet and Trickbot beacon 2:

## DEEPSEC

	Protoc	Leng	Info
tua.com.br	TCP	66	61117 → http-alt(8080) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	TCP	58	http-alt(8080) → 61117 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
tua.com.br	TCP	54	61117 → http-alt(8080) [ACK] Seq=1 Ack=1 Win=65535 Len=0
tua.com.br	TCP	476	61117 → http-alt(8080) [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=422 [TCP segment of a reassemb
tua.com.br	TCP	1514	61117 → http-alt(8080) [ACK] Seq=423 Ack=1 Win=65535 Len=1460 [TCP segment of a reassemble
tua.com.br	TCP	1514	61117 → http-alt(8080) [ACK] Seq=1883 Ack=1 Win=65535 Len=1460 [TCP segment of a reassemble
tua.com.br	TCP	1514	61117 → http-alt(8080) [ACK] Seq=3343 Ack=1 Win=65535 Len=1460 [TCP segment of a reassemble
tua.com.br	TCP	1514	61117 → http-alt(8080) [ACK] Seq=4803 Ack=1 Win=65535 Len=1460 [TCP segment of a reassemble
	TCP		http-alt(8080) → 61117 [ACK] Seq=1 Ack=423 Win=64240 Len=0
tua.com.br	нттр	1258	POST /tqg9o/ikxapt5fx226p47wwsd/3tfkg3j/07x0v0hpn2d919md3/ HTTP/1.1
	🛑 🔵 🔵 Wire	shark	· Follow TCP Stream (tcp.stream eq 61) · 2020-12-29-Emotet-infection-with-Trickbot-
	••••		
	POST /tqg9o/	ikxapt!	5fx226p47wwsd/3tfkg3j/07x0v0hpn2d919md3/ HTTP/1.1
	DNT: 0		
tua.com.br			.252/tqg9o/ikxapt5fx226p47wwsd/3tfkg3j/07x0v0hpn2d919md3/
	Content-Type	mult:	ipart/form-data; boundary=AdkZ4QlvQ a/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
tua.com.br	Host: 189.34		
	Content-Leng		
tua.com.br	Connection:		
	Cache-Contro	l: no-	cache
tua.com.br			
	-	dkZ401	
tua.com.br			n: form-data; name="SCnFw0CbRKEjlLBM"; filename="RG0GcCRtTswkNwGazc"
			ication/octet-stream
tua.com.br			
(10054 bits)			H.Xcn.X."w~`ph+y&C2
(10064 bits)			vH!. <r)mlews!u:0[~j.m7n#0:;n*. .B6.[.&amp;G.?2t0}[ks&lt;.</r)mlews!u:0[~j.m7n#0:;n*. 
tgear_b6:93:f1 (	{.F.0G1		Z2.j.8{.@tLkt.c^v.9Kfw.@<+D.\
st: bd2212fc.vir			3(.YB?.[i.b0Ga.LG.{.7.G.~"G':~Zo't}",u@~vp.>E+
: http-alt (8080			\$.MUhD <arfoe.< td=""></arfoe.<>
), #7438(1460),		11	Environ E a E a March a G & K L 7 Ch a ( unit el M a

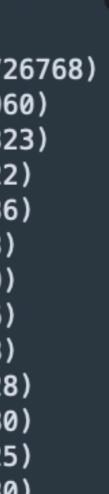
1527 Total	Pa	ckets														
Difference	in	microseconds:	28	5959	) (	09:	50:	:16.	520	476	- (	09:	50:	16.8	30643	3
Difference	in	microseconds:	52	2 (0	9:	50:	16.	. 806	6435	-	<b>09:</b> !	50:	16.	8069	957)	
Difference	in	microseconds:	91	(09	):5	<b>0:</b> 1	.6.8	3069	957	- 0	9:5	0:1	6.8	0704	48)	
Difference	in	microseconds:	13	7 (0	9:	50:	16.	. 807	7048	-	<b>09:</b> !	50:	16.	8071	185)	
Difference	in	microseconds:	10	(09	):5	<b>0:</b> 1	.6.8	3071	L85	- 0	9:5	0:1	6.8	0719	95)	
Difference	in	microseconds:	5	(09:	50	:16	. 80	0719	95 –	09	:50	:16	. 80	7200	<b>)</b> )	
Difference	in	microseconds:	4	(09:	50	:16	. 80	0720	00 -	09	:50	:16	. 80	7204	4)	
Difference	in	microseconds:	74	(09	):5	<b>0:</b> 1	.6.8	3072	204	- 0	9:5	0:1	6.8	0727	78)	
Difference	in	microseconds:	62	(09	):5	<b>0:</b> 1	.6.8	3072	278	- 0	9:5	0:1	6.8	0734	40)	
Difference	in	microseconds:	40	(09	):5	<b>0:</b> 1	.6.8	3073	340	- 0	9:5	0:1	6.8	0738	30)	
Difference	in	microseconds:	39	(09	):5	<b>0:</b> 1	.6.8	3073	80	- 0	9:5	0:1	6.8	0741	19)	
Difference	in	microseconds:	78	3370	) (	09:	50:	:16.	807	419	- (	09:	50:	17.5	59078	3
Difference	in	microseconds:	17	7 (0	9:	50:	17.	.590	789	_	09:	50:	17.	5909	966)	

### Notes for the Viewer: Looking at the time in between transactions, there are some similarities



Emotet and Trickbot beacon 2:

	5493 Total Packets	
35)	Difference in microseconds:	249919 (10:19:19.476849 - 10:19:19.72
	Difference in microseconds:	192 (10:19:19.726768 - 10:19:19.7269)
	Difference in microseconds:	363 (10:19:19.726960 - 10:19:19.7273
	Difference in microseconds:	99 (10:19:19.727323 - 10:19:19.72742
	Difference in microseconds:	14 (10:19:19.727422 - 10:19:19.72743)
	Difference in microseconds:	7 (10:19:19.727436 - 10:19:19.727443)
	Difference in microseconds:	6 (10:19:19.727443 - 10:19:19.727449)
	Difference in microseconds:	7 (10:19:19.727449 - 10:19:19.727456)
	Difference in microseconds:	2 (10:19:19.727456 - 10:19:19.727458)
	Difference in microseconds:	70 (10:19:19.727458 - 10:19:19.72752
	Difference in microseconds:	52 (10:19:19.727528 - 10:19:19.72758)
39)	Difference in microseconds:	45 (10:19:19.727580 - 10:19:19.72762
	Difference in microseconds:	55 (10:19:19.727625 - 10:19:19.72768)



# Benign vs Malicious

Notes for the Viewer: What if we add in some benign network traffic?



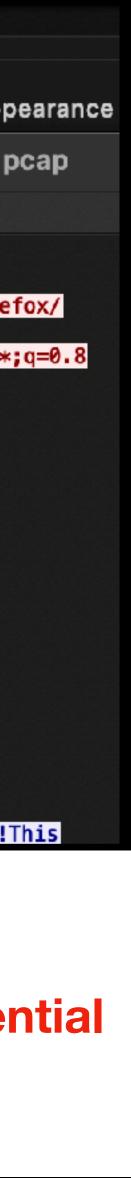
## Benign .exe Download

īme	Source	Destination
000000	evol.lan	li744-28.members.linode.com
.048434	li744-28.members.linode.com	evol.lan
.048696	evol.lan	li744-28.members.linode.com
.048807	evol.lan	li744-28.members.linode.com Appe
.054736	li744-28.members.linode.com	A Attendende Fallen TOD Omeren (ten studen an O) benime and demolated a
193391	li744-28.members.linode.com	🕽 😑 🌑 Wireshark · Follow TCP Stream (tcp.stream eq 0) · benign_exe_download.p
1.193707	evol.lan	
1.195468	li744-28.members.linode.com	
1.195616	evol.lan	GET /existential.exe HTTP/1.1
196584	li744-28.members.linode.com	Host: samplevault.net
196586	li744-28.members.linode.com	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:103.0) Gecko/20100101 Firef 103.0
196649	evol.lan	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
1.196763	evol.lan	Accept-Language: en-US,en;q=0.5
497034	li744-28.members.linode.com	Accept-Encoding: gzip, deflate
		DNT: 1
		Connection: keep-alive
		Upgrade-Insecure-Requests: 1 Sec-GPC: 1
		HTTP/1.1 200 OK
		Date: Wed, 24 Aug 2022 18:58:19 GMT
		Server: Apache/2.4.38 (Debian)
		Last-Modified: Wed, 24 Aug 2022 18:55:28 GMT
6: 1514 bytes	on wire (12112 bits), 1514 bytes captured (12112 bi	ETag: "1800-5e701397c408b" Accept-Ranges: bytes
	LTechno_18:d6:06 (94:83:c4:18:d6:06), Dst: Apple_09:	Content-Length: 6144
	ersion 4, Src: li744-28.members.linode.com (23.239.2)	Keep-Alive: timeout=5, max=100
	l Protocol, Src Port: http (80), Dst Port: 55278 (55)	Connection: Keep-Alive
Control Control		Content-Type: application/x-msdos-program
		MZ@@

**Notes for the Viewer:** dropper download.



### This is a download of a small .exe that is benign, but was created to be used in testing to look like a potential



## **Benign .exe Vs Malicious Dropper Download**

Benign:		
	Ron	ian
		IGII.

14 packets

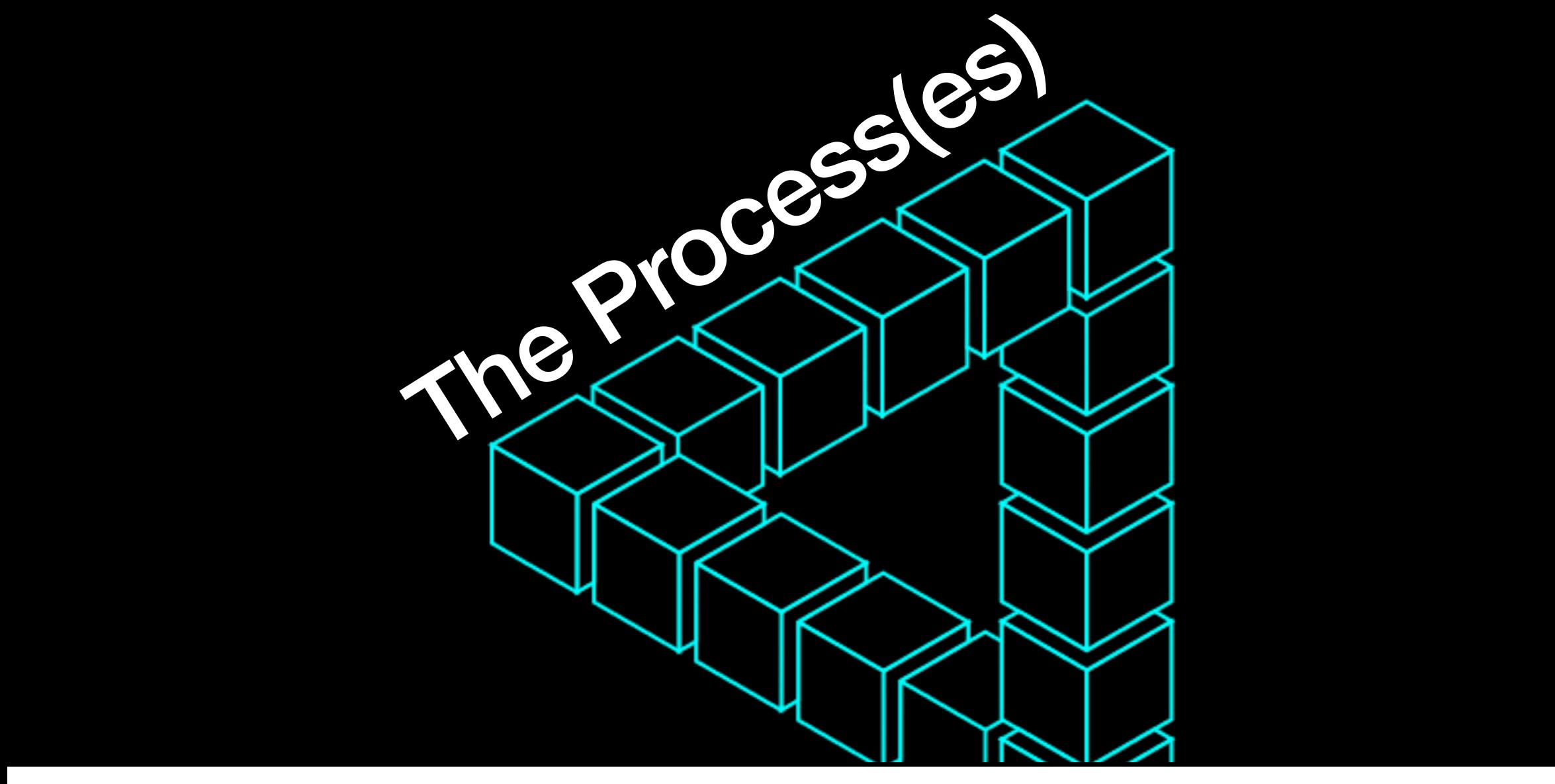
## Notes for the Viewer: The similarities break down earlier in the network traffic.

Difference in microseconds: 93622 (12:56:39.441422 - 12:56:39.535044) Difference in microseconds: 98 (12:56:39.535044 - 12:56:39.535142) Difference in microseconds: 159 (12:56:39.535142 - 12:56:39.535301) Malicious: Difference in microseconds: 56 (12:56:39.535301 - 12:56:39.535357) Difference in microseconds: 92677 (12:56:39.535357 - 12:56:39.628034) Difference in microseconds: 1444 (12:56:39.628034 - 12:56:39.629478) Difference in microseconds: 21 (12:56:39.629478 - 12:56:39.629499)



Difference in microseconds: 48434 (11:58:19.135349 - 11:58:19.183783) Difference in microseconds: 262 (11:58:19.183783 – 11:58:19.184045) Difference in microseconds: 111 (11:58:19.184045 - 11:58:19.184156) Difference in micro : 5929 (11:58:19.184156 - 11:58:19.190085) Difference in microseconds: 138655 (11:58:19.190085 – 11:58:19.328740) Difference in microseconds: 316 (11:58:19.328740 - 11:58:19.329056) Difference in micro 1761 (11:58:19.329056 - 11:58:19.330817) Difference in microsecods: 148 (11:58:19.330817 - 11:58:19.330965) Difference in microseconds: 968 (11:58:19.330965 – 11:58:19.331933) Difference in microseconds: 2 (11:58:19.331933 - 11:58:19.331935) Difference in microseconds: 63 (11:58:19.331935 – 11:58:19.331998) Difference in microseconds: 114 (11:58:19.331998 - 11:58:19.332112) Difference in microseconds: 300271 (11:58:19.332112 - 11:58:20.632383)

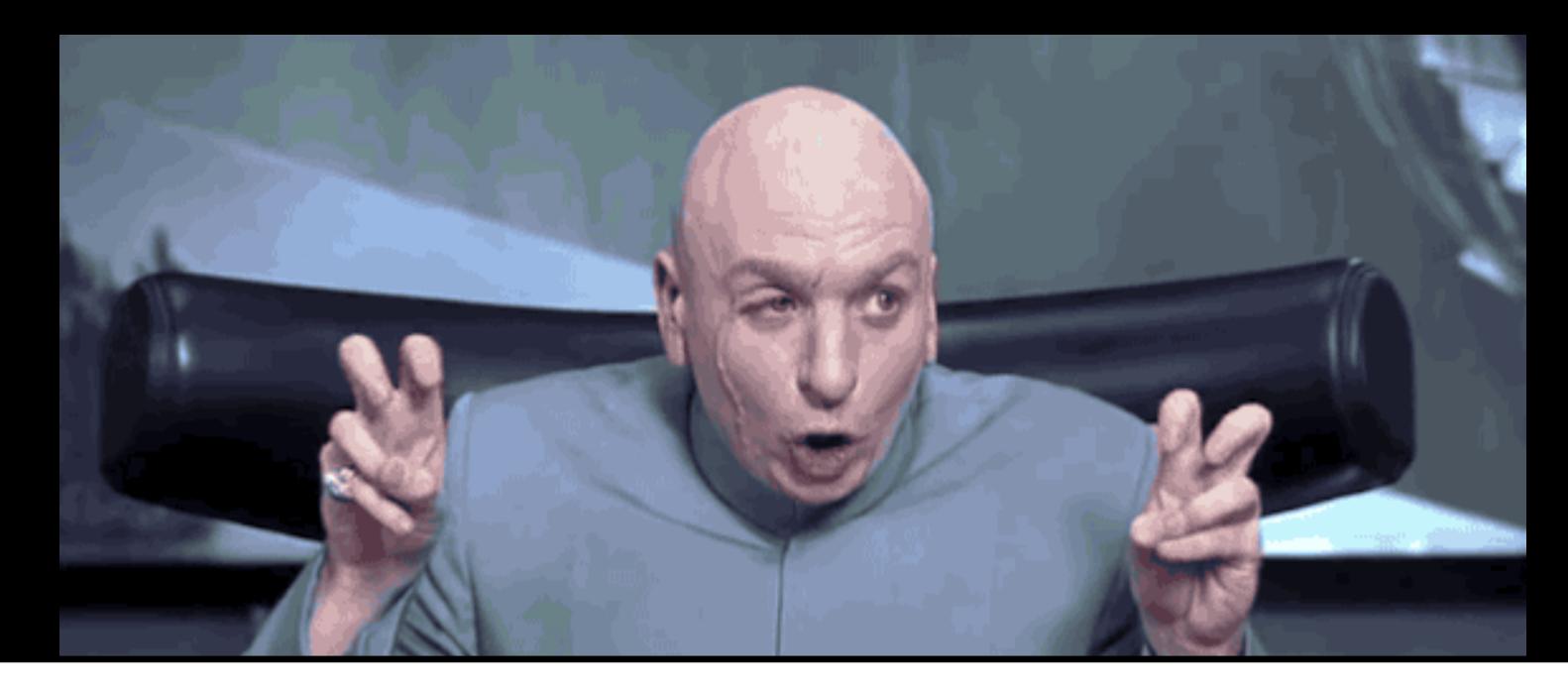




## Notes for the Viewer: Let's discuss the process that I'll use to figure out timing and build a signature.



# Challenges



## Notes for the Viewer: There are a few challenges in the process.





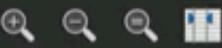
## Finding the Part I'm Interested in...

												202	2-04-	25-En	notet-ej	poch4-i	infect	tion-w	ith-spaml	ot-traffic.pcap	
		Ø	0			×	3	٩	<b>\$</b>	⇒	2	ি	垫			⊕ <b></b>	€,				
A A	oply a	display	filter	. <36/>																	• +
No.	T	ime			S	ource				D	stinati	on .			1	Protoc	Leng	Info			
	1 2	22-04-2	5 09:49:	:34.8899	066 0.	.0.0.0				25	5.255.2	55.255				DHCP	344	DHCP D	iscover -	ransaction ID 0x4f27af50	
	2 2	022-04-2	5 09:49:	:34.8953	69 10	0.4.25.1	11			10	.4.25.1	01				DHCP		DHCP 0		ransaction ID 0x4f27af50	
L	-	022-04-2									5.255.2					DHCP				ransaction ID 0x4f27af50	
		022-04-2									.4.25.1					DHCP		DHCP A		ransaction ID 0x4f27af50	
	-	022-04-2									4.0.0.2					IGMPv3				/ Join group 224.0.0.251 for any sources	
		22-04-2									4.0.0.2					IGMPv3				/ Join group 224.0.0.252 for any sources	
		22-04-2						e			oadcast					ARP				7 Tell 10.4.25.101	
		822-84-2									wlettP_		se			ARP				4:1f:72:c2:09:6a	
	_	22-04-2									.4.25.4					DNS				6eaa A wpad.formulaonefigurines.com	
	_	22-04-2									4.0.0.2					DNS IGMPv3				sponse 0x6eaa No such name A wpad.formulaonefigurines.com SOA formulafigs-dc.formulao / Leave group 224.0.0.252	
		22-04-2									4.0.0.2					IGMPV3				/ Join group 224.0.0.252 for any sources	
		22-04-2									.4.25.4					DNS				dfc9 A wpad.mshome.net	
		22-04-2									4.0.0.2					MDNS				8000 ANY DESKTOP-J95JQDS.local, "QM" question	
		22-84-2									4.0.0.2					LLMNR				26f0 ANY DESKTOP-J95JQDS	
		22-84-2									4.0.0.2					MDNS				sponse 0x0000 A 10.4.25.101	
	17 2	22-04-2	5 09:49:	34.9189	23 10	0.4.25.1	01				.4.25.4					DNS				bcel SRV _ldaptcp.Default-First-Site-Namesites.dcmsdcs.formulaonefigurines.com	
	18 2	22-04-2	5 09:49:	34.9193	68 10	0.4.25.4					.4.25.1					DNS				sponse @xbce1 SRV _ldaptcp.Default-First-Site-Namesites.dcmsdcs.formulaonefigur	in
	19 2	22-04-2	5 09:49:	34.9286	541 10	0.4.25.1	01			10	.4.25.4					DNS				bd16 A formulafigs-dc.formulaonefigurines.com	
	20 2	022-04-2	5 09:49:	34.9208	179 10	0.4.25.4	1			10	.4.25.1	01			1	DNS	114	Standa	rd query r	sponse 0xbd16 A formulafigs-dc.formulaonefigurines.com A 10.4.25.4	
	21 2	022-04-2	5 09:49:	34.9215	510 10	0.4.25.1	101			10	.4.25.4					ONS				4b25 SRV _ldaptcp.dcmsdcs.formulaonefigurines.com	
		822-84-2								10	.4.25.1	01			1	DNS				sponse 0x4b25 SRV _ldaptcp.dcmsdcs.formulaonefigurines.com SRV 0 100 389 formulaf	
		022-04-2									.4.25.4				1	DNS				f474 SRV _ldaptcp.e100423e-bd3f-477e-ae13-62deff7ad5f1.domainsmsdcs.formulaonefig	
		022-04-2									.4.25.1					DNS				sponse 0xf474 SRV _ldaptcp.e100423e-bd3f-477e-ae13-62deff7ad5f1.domainsmsdcs.form	ul
		022-04-2									.4.25.4					DNS				72eb SRV _ldaptcp.Default-First-Site-Namesites.formulaonefigurines.com	
_	26 2	022-04-2	5 09:49:	:34.9269	25 1	0.4.25.4		_	_	10	.4.25.1	01				DNS	199	Standa	rd query r	sponse 0x72eb SRV _ldaptcp.Default-First-Site-Namesites.formulaonefigurines.com S	RV

> Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)

## **Notes for the Viewer:** Challenge 1: Finding the bad thing I'm interested in and isolating it.







## **Acquiring Relevant Threat Traffic**

А https://www.malware-traffic-analysis.net/2022/index.html



## [2013]-[2014]-[2015]-[2016]-[2017]-[2018]-[2019]-[2020]-[2021]-[2022]

 2022-10-10 -- Qakbot (Qbot) infection with Cobalt Strike 2022-10-4

**Notes for the Viewer:** Challenge 2: Acquiring the relevant traffic, as in what's relevant to the risks in my network? What's current? Etc... this website, as well as others can be very useful in accomplishing this.

2022-09-

 $\bigcirc$ 

- 2022-09-
- 2022-092022-09-

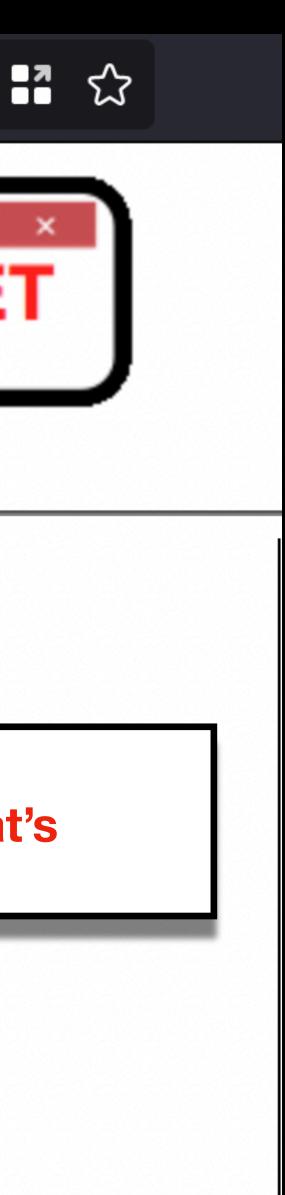
DEEPSEC<sup>08-</sup>

**Bookmark Link...** 

Save Link As...

Save Link to Pocket

Copy Link



# MALWARE-TRAFFIC-ANALX

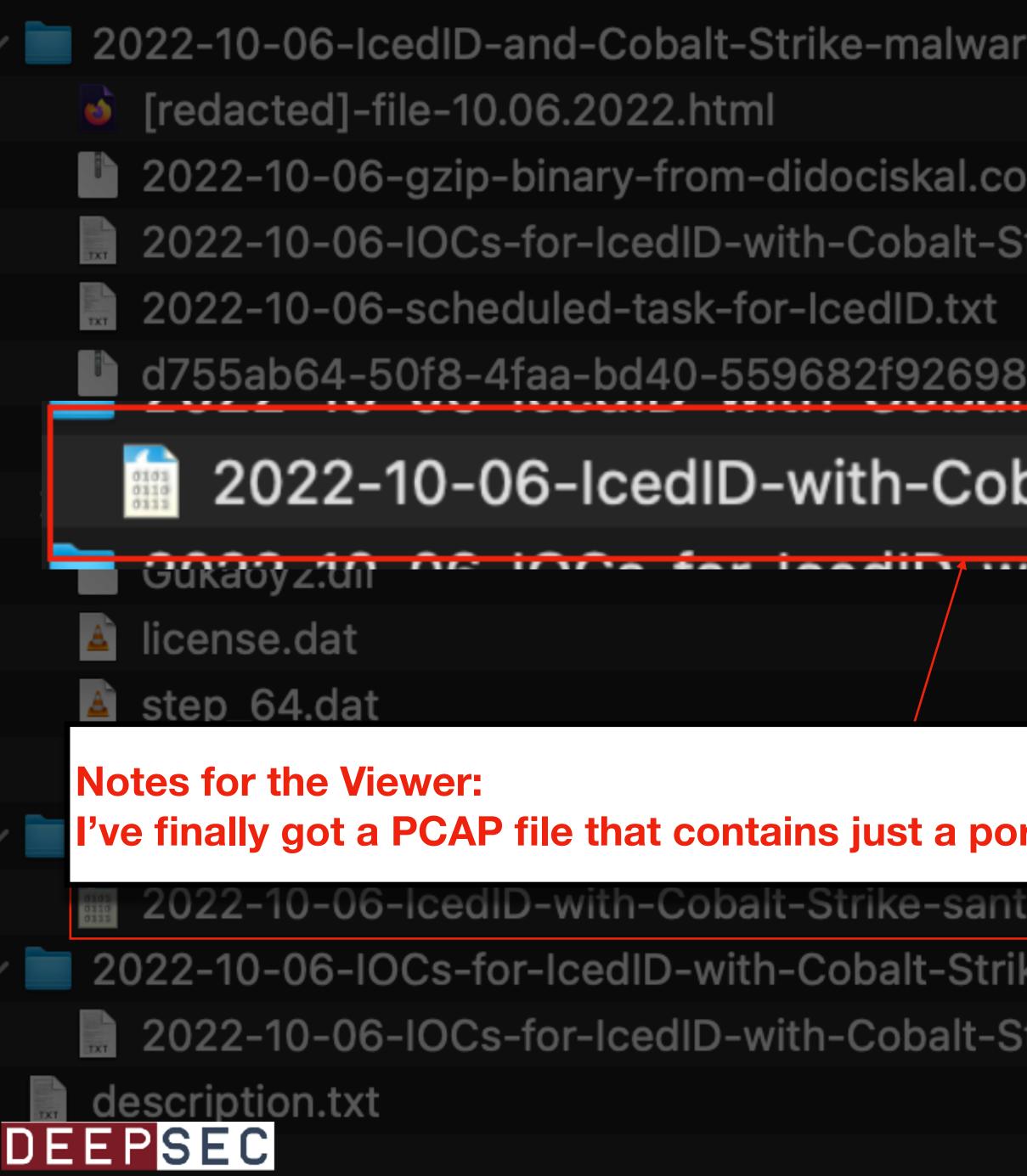
okbot) --> Cobalt Strike

obalt Strike Cobalt Strike rom Brazil malspam om scans/probes hitting a web server



# Once I have a Viable PCAP

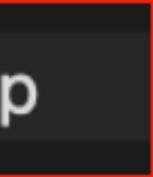




	ιοάαγ αι 25.01						
balt-Strike-santized-and-carved.pcap							
3.zip	Today at 23:01						
	Today at 23:01						
Strike.txt	Today at 23:01						
om.bin	Today at 23:01						
	Today at 23:01						
re-and-artifacts	Today at 23:01						

I've finally got a PCAP file that contains just a portion of the bad traffic I want to build a signature from.

tized-and-carved.pcap	Today at 23:01
ike	Today at 23:01
Strike.txt	Today at 23:01
	Today at 23:01





Today at 23:01

Todav at 23:01

## Isolated Trickbot POST from a larger PCAP

## TrickBot 1

						····· -
5	0.000247	10.9.30.101	80.87.201.221	HTTP	478	POST /
78	1.699744	80.87.201.221	10.9.30.101	HTTP	396	HTTP/1
83	1.706418	10.9.30.101	80.87.201.221	HTTP	478	POST /
321	4.434370	80.87.201.221	10.9.30.101	HTTP	311	HTTP/1
326	4.442984	10.9.30.101	80.87.201.221	HTTP	478	POST /
343	5.289803	80.87.201.221	10.9.30.101	HTTP	220	HTTP/1
348	5.299435	10.9.30.101	80.87.201.221	HTTP	478	POST /
459	10.289254	80.87.201.221	10.9.30.101	HTTP	1369	HTTP/1
464	10.295713	10.9.30.101	80.87.201.221	HTTP	494	POST /
577	12.092188	80.87.201.221	10.9.30.101	HTTP	663	HTTP/1
582	12.099466	10.9.30.101	80.87.201.221	HTTP	494	POST /
834	15.375483	80.87.201.221	10.9.30.101	HTTP	444	HTTP/1
839	15.388285	10.9.30.101	80.87.201.221	HTTP	526	POST /o

Notes for the Viewer: I've finally got a PCAP file that contains just a portion of the bad traffic I want to build a signature from. I'm not worried about having multiple POSTs. It doesn't have to be perfect. I just don't want 'clean' traffic in there.



/pIXPXFus4dL9VHy/Ae4Qu00cWqMiS6t/PR8Ag6INSGfX0v/P4eGV/jBuvXE/J7W3n4va8quznD/ HTTP/1.1 l.1 200 OK (text/html) /HZn5Um1RGxgZ4AC5/BW8yR5/RHTBz5XxAFoC/ivn0vfar/Xq6HEyvjsyv0U/ HTTP/1.1 l.1 200 OK (text/html) /CICnq0ruETzlLi/Bd5APHiVCt4zWEU/KDsFyce3t5NTCuNWc/ HTTP/1.1 l.1 200 OK (text/html) /hucUozNM1/kIARs4tFzz2LgSrAenQ/kqcmV0gVM6g/btrh6lz8jsM0F8/ HTTP/1.1 l.1 200 OK (text/html) /B1GC6eAbxy4DL71le/A5lrsR/ZTF0jhiNTGWIuSShlZR/lZJh2BIiq2hRZ5/lrq6gLJguipxQCN/P1yEI/ HTTP/1.1 l.1 200 OK (text/html) /vlddDI/QAmLy/zGRph9CuZ3/ HTTP/1.1 l.1 200 OK (text/html) /vlddDI/QAmLy/zGRph9CuZ3/ HTTP/1.1







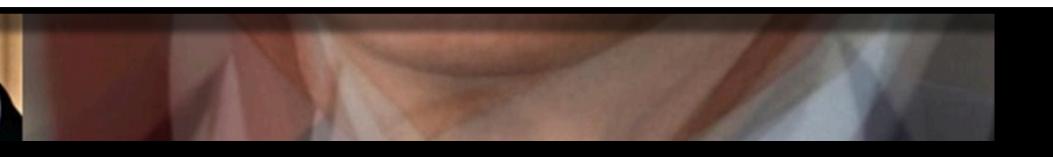
### **Notes for the Viewer:**

We've looked at the time in between network transactions - now let's try getting the average of all of those times. The idea is that some PCAP files will contain possibly thousands of transactions while others contain maybe only a few.





# Averages



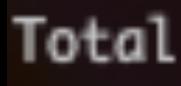


## **Calculate time in between transactions**

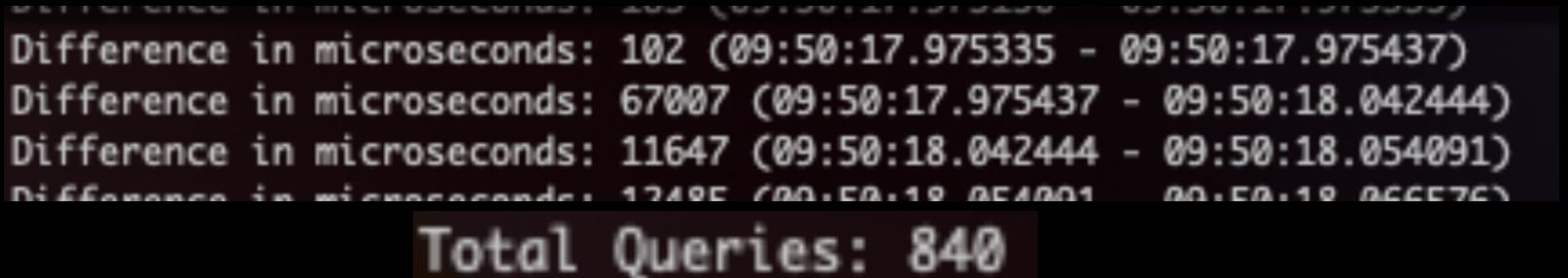
Time between queries: Difference in microseconds: 228 (09:50:16.806957 - 09:50:16.807185) Difference in microseconds: 10 (09:50:16.807185 - 09:50:16.807195) Difference in microseconds: 5 (09:50:16.807195 - 09:50:16.807200) Difference in microseconds: 4 (09:50:16.807200 - 09:50:16.807204) Difference in microseconds: 783585 (09:50:16.807204 - 09:50:17.590789) Difference in microseconds: 738 (09:50:17.590789 - 09:50:17.591527) Difference in microseconds: 145 (09:50:17.591527 - 09:50:17.591672) Difference in microseconds: 21950 (09:50:17.591672 - 09:50:17.613622) Difference in microseconds: 738 (09:50:17.613622 - 09:50:17.614360) Difference in microseconds: 209422 (09:50:17.614360 - 09:50:17.823782) Difference in microseconds: 129985 (09:50:17.823782 - 09:50:17.953767) Difference in microseconds: 841 (09:50:17.953767 - 09:50:17.954608) Difference in microseconds: 4351 (09:50:17.954608 - 09:50:17.958959)

#### **Notes for the Viewer:** 1: Get the microseconds between transactions.

Difference in microconde: 1249E (00.E0.19 0E4001



### DEEPSEC



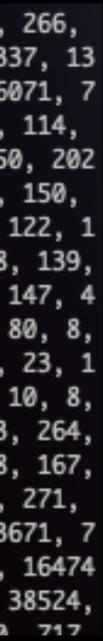
### Get all the Microseconds of those times

[228, 10, 5, 4, 783585, 738, 145, 21950, 738, 209422, 129985, 841, 4351, 851, 15150, 190, 185, 102, 67007, 11647, 12485, 146142, 123, 355, 175, 30, 237, 771, 62, 266, 745, 98, 142, 2384, 702, 135, 196, 44370, 629, 57793, 749, 11, 222, 130906, 942, 7216, 695, 301, 25, 811, 146, 7885, 898, 159, 87, 345, 18, 20649, 119, 271, 8, 337, 13 23, 824, 227, 14, 773, 6888, 718, 148, 239, 23, 251, 152, 167, 216, 7, 6583, 72, 9, 4, 6, 707215, 791, 102, 35053, 120, 153, 153, 121, 13125, 46462, 719, 133, 16071, 7 43, 100, 22161, 17049, 750, 3613, 810, 101, 13979, 16223, 90, 3719, 825, 176, 39487, 698, 168, 407973, 809, 102, 200, 89, 169, 191, 172, 160, 186, 152, 184, 155, 114, 159, 163, 174, 164, 214, 104, 222, 168, 114, 133, 279, 167, 94, 162, 209, 88, 165, 177, 207, 105, 2936, 134, 182, 100, 165, 153, 149, 194, 143, 169, 182, 151, 150, 202 , 149, 168, 174, 139, 464, 21, 354030, 9, 233, 206, 255, 16, 43, 278, 121, 137, 229, 78, 206, 184, 171, 151, 152, 76, 276, 184, 152, 146, 182, 98, 224, 135, 189, 150, 159, 156, 193, 145, 179, 1407, 157, 144, 170, 166, 160, 183, 126, 184, 187778, 704, 187, 9450, 722, 107, 219, 100, 171, 157, 161, 771, 173, 170, 1201, 154, 190, 122, 1 98, 1288, 169, 765, 162, 1975, 153, 176, 19183, 55, 287, 40, 220, 126, 107, 290, 177, 13, 269, 168, 170, 73113, 594, 194, 44, 183, 216, 105, 933, 107, 34837, 728, 139, 37418, 829, 154, 62151, 178, 67, 24524, 793, 114, 45977, 765, 1709, 22937, 697, 132, 39130, 767, 137, 27822, 723, 139, 51946, 95, 54, 8008, 838, 58, 6265, 771, 147, 4 6732, 1662, 167, 14968, 796, 157, 49576, 84, 170, 14163, 851, 13586, 7895, 9605, 841, 20327, 122, 138, 21636, 704, 75, 123528, 144, 102, 179, 292, 8, 1297, 194, 80, 8, 8492, 96, 15, 7, 4, 700859, 753, 101, 37864, 791, 115, 92451, 15, 118, 10629, 727, 58, 1838, 125, 197, 170, 8, 9506, 105, 9, 6, 6, 754535, 24, 17, 36, 405, 158, 23, 1 63, 8, 262, 306764, 60, 18, 517, 21, 142, 29, 24, 328, 7, 166, 244, 304642, 8, 21, 509, 22, 155, 7, 74, 203, 153, 144, 230, 194, 184, 155, 97, 184, 184, 314520, 10, 8, 338, 21, 183, 116, 118, 217, 172, 124, 178, 164, 279, 19, 187, 199, 49, 276, 152, 155, 170, 147, 72, 285, 153, 145, 165, 151, 171, 168, 150, 168, 292482, 38, 23, 264, 18, 200, 229, 21, 231, 227, 49, 229, 164, 139, 59, 235, 147, 159, 177, 162, 158, 155, 201, 170, 108, 232, 153, 140, 184, 149, 165, 189, 132, 1247, 157, 134, 178, 167, 6337, 77, 14, 16, 15, 954626, 91, 215, 19916, 646, 186, 45735, 259, 10200, 693, 972, 115, 19967, 816, 64, 355884, 2902, 85, 91, 298, 233, 10, 2887, 56, 257, 10, 271, 205, 11, 230, 221, 768, 158, 774, 170, 868, 61, 14336, 45, 143, 373, 12, 44, 246, 185, 168, 138, 13935, 47, 230, 213, 19, 230, 187, 192, 10, 382, 11, 163, 210, 3671, 7 26, 131, 31349, 823, 58, 30361, 91, 202, 3197, 814, 188, 26773, 605, 172, 99948, 12, 182, 106, 249, 70, 340, 23, 256, 8, 261, 159, 278, 34, 169, 16559, 730, 137, 16474 , 716, 191, 27928, 91, 174, 15332, 81, 246, 19381, 692, 203, 10125, 761, 9049, 4184, 125, 253, 19288, 29, 7078, 146, 33, 12, 9, 750988, 87, 178, 18970, 63, 213, 38524, 50 243 114 168 233 153 254 10

#### **Notes for the Viewer:** 2: and put them in a list

, 9, 10, 7, 66, 11, 26, 8, 7, 9, 10, 20, 10, 7, 12637, 128, 7, 27, 3, 985891]





### Get all the Microseconds of those times



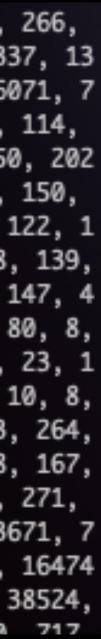
#### **Notes for the Viewer:** This list is the entire length of the PCAP.

, 9, 10, 7, 66, 11, 26, 8, 7, 9, 10, 20, 10, 7



6142, 123, 355, 175, 30, 237, 771, 62, 266, 59, 87, 345, 18, 20649, 119, 271, 8, 337, 13 , 153, 121, 13125, 46462, 719, 133, 16071, 7 69, 191, 172, 160, 186, 152, 184, 155, 114, 153, 149, 194, 143, 169, 182, 151, 150, 202 184, 152, 146, 182, 98, 224, 135, 189, 150, , 161, 771, 173, 170, 1201, 154, 190, 122, 1 4, 183, 216, 105, 933, 107, 34837, 728, 139, 46, 95, 54, 8008, 838, 58, 6265, 771, 147, 4 28, 144, 102, 179, 292, 8, 1297, 194, 80, 8, 9, 6, 6, 754535, 24, 17, 36, 405, 158, 23, 1 194, 184, 155, 97, 184, 184, 314520, 10, 8, 51, 171, 168, 150, 168, 292482, 38, 23, 264, 49, 165, 189, 132, 1247, 157, 134, 178, 167, , 91, 298, 233, 10, 2887, 56, 257, 10, 271, 30, 187, 192, 10, 382, 11, 163, 210, 3671, 7 1, 159, 278, 34, 169, 16559, 730, 137, 16474 , 9, 750988, 87, 178, 18970, 63, 213, 38524, 705 170 112 140 730 717





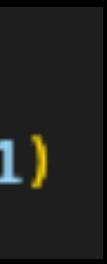
## Find the Average

## sum\_of\_trickbot1 = sum(trickbot1) average\_of\_microseconds\_trickbot1 = sum\_of\_trickbot1 / len(trickbot1)

# 14748.719904648391

**Notes for the Viewer: 3: Calculate the average of all of those microseconds.** 





Time between queries:

Difference in microseconds: 228 (09:50:16.806957 - 09:50:16.807185) Difference in microseconds: 10 (09:50:16.807185 - 09:50:16.807195) Difference in microseconds: 5 (09:50:16.807195 - 09:50:16.807200) Difference in microseconds: 4 (09:50:16.807200 - 09:50:16.807204) Difference in microseconds: 783585 (09:50:16.807204 - 09:50:17.590789) Difference in microseconds: 738 (09:50:17.590789 - 09:50:17.591527) Difference in microseconds: 145 (09:50:17.591527 - 09:50:17.591672) Difference in microseconds: 21950 (09:50:17.591672 - 09:50:17.613622) Difference in microseconds: 738 (09:50:17.613622 - 09:50:17.614360) Difference in microseconds: 209422 (09:50:17.614360 - 09:50:17.823782) Difference in microseconds: 129985 (09:50:17.823782 - 09:50:17.953767) Difference in microseconds: 841 (09:50:17.953767 - 09:50:17.954608) Difference in microseconds: 4351 (09:50:17.954608 - 09:50:17.958959) Difference in microseconds: 851 (09:50:17.958959 - 09:50:17.959810) Difference in microseconds: 15150 (09:50:17.959810 - 09:50:17.974960) Difference in microseconds: 190 (09:50:17.974960 - 09:50:17.975150) Difference in microseconds: 185 (09:50:17.975150 - 09:50:17.975335) Difference in microseconds: 102 (09:50:17.975335 - 09:50:17.975437) Difference in microseconds: 67007 (09:50:17.975437 - 09:50:18.042444) Difference in microseconds: 11647 (09:50:18.042444 - 09:50:18.054091) 00.E0.10 066E76) Difference in micrococonde: 1249E (00.E0.10 0E4001

### DEEPSEC

### Again with Another PCAP

## Isolated Trickbot POST

No.		Time	Source	Destination	Protocol	Length	Info
┢	6	0.000135	10.12.29.101	189.34.18.252	HTTP	1258	POST
•	1101	16.946285	189.34.18.252	10.12.29.101	HTTP	1015	HTTP
•	1106	16.959638	10.12.29.101	189.34.18.252	НТТР	1486	POST
	2224	33.285627	189.34.18.252	10.12.29.101	НТТР	609	HTTP
	2230	33.302493	10.12.29.101	189.34.18.252	HTTP	1018	P0ST
	2415	38.493605	189.34.18.252	10.12.29.101	HTTP	157	HTTP
	2421	38.502688	10.12.29.101	189.34.18.252	HTTP	74	P0ST
	2665	42.838930	189.34.18.252	10.12.29.101	HTTP	563	HTTP
	2671	42.852352	10.12.29.101	189.34.18.252	HTTP	1370	P0ST
	2897	48.905648	189.34.18.252	10.12.29.101	HTTP	288	HTTP
	2903	48.917313	10.12.29.101	189.34.18.252	HTTP	1290	P0ST
L	2905	49.827338	189.34.18.252	10.12.29.101	HTTP	1042	HTTP





F /tqg9o/ikxapt5fx226p47wwsd/3tfkg3j/07x0v0hpn2d919md3/ HTTP/1.1

P/1.1 200 OK (text/html)

T /xomdq50t/se7srsiitec3m/f54e1juni4kuk7fjb/t99r946mvo/4okinw5f6ydnhll/ HTTP/1.1

P/1.1 200 OK (text/html)

T /bkynd5lifqfsi52b/uv7prprsl/3sppbt6b5vy7kmzb3/v5djoxr/4ffc8gdir/ HTTP/1.1

P/1.1 200 OK (text/html)

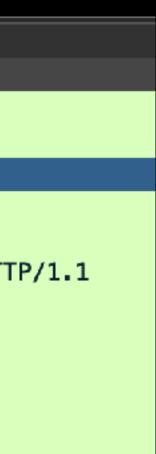
T /wjg8qaqd7v5a1963ris/3une6mc1wpq/p701bp/2rue8040hzdt4/f8jppv/o1yjc7bglajqueh4/ HTTP/1.1 P/1.1 200 OK (text/html)

T /n74ib0xs4u/gwu50m6qpx2j2emq/hq2xxkl10fvht/ HTTP/1.1

P/1.1 200 OK (text/html)

T /jpksx0k4h/x6w356jvwlgq7x/fjgjxvec/df1fu0by8pfkm/rifmu7/msrdq8wu/ HTTP/1.1

P/1.1 200 OK (text/html)



# **PCAP 1:**

TrickBot 1 (20200930\_trickbotpost.pcap)



### **PCAP 2:** TrickBot 2 (20201229\_trickbotpost.pcap)



#### **Notes for the Viewer:** Compare two similar PCAPs, both with a very different number of total transactions (I called them queries for some reason)



# Total Queries: 840



#### **PCAP 1:** TrickBot 1 (20200930\_trickbotpost.pcap)

# Total Queries: 840 Average: 14748.719984648391

**PCAP 2:** TrickBot 2 (20201229\_trickbotpost.pcap)

# Total Queries: 2905 Average: 16125.116391184572

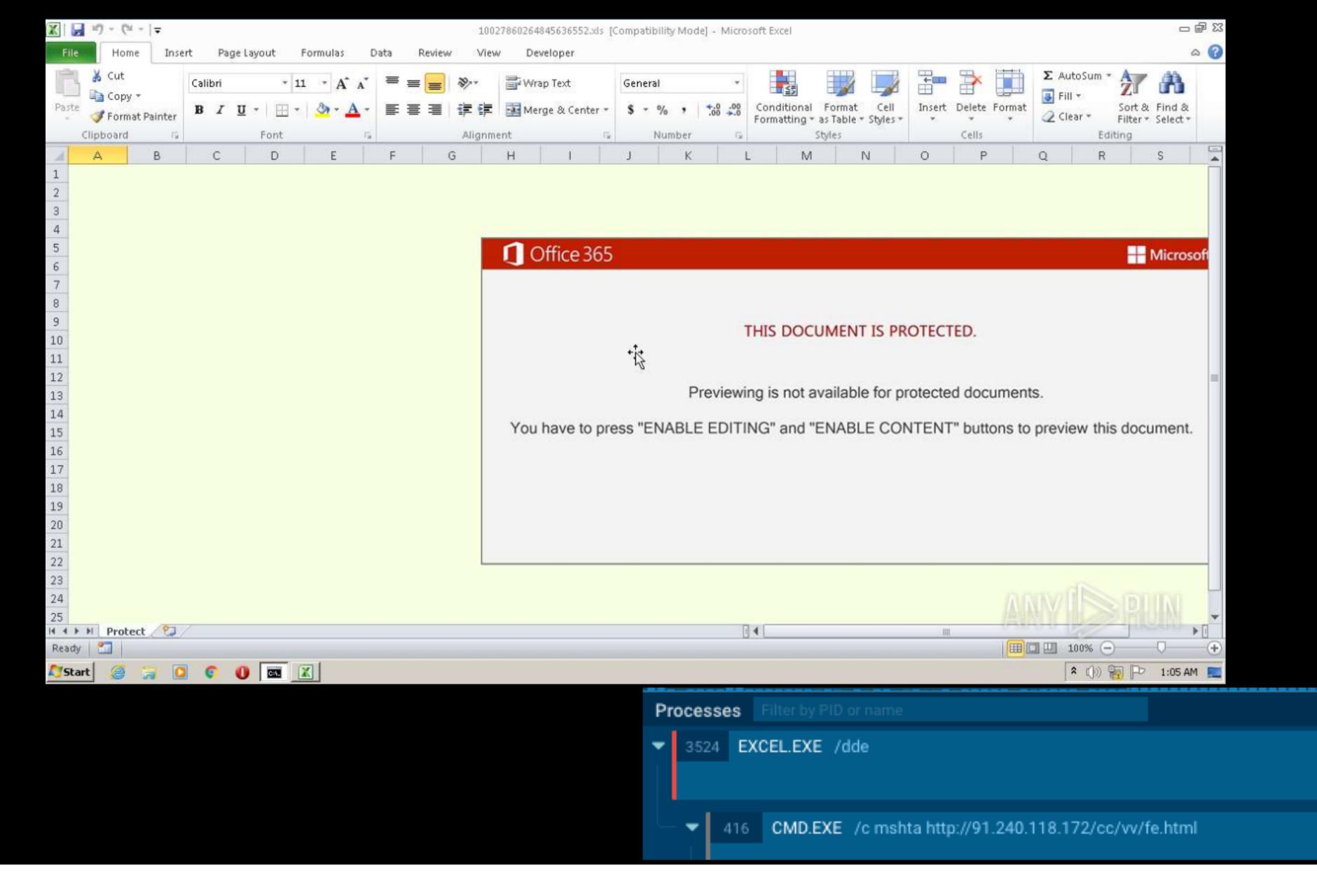
**Notes for the Viewer:** The average is not close out of context with other data that we'll see in a the next few slides, but for now **DEE** they're somewhat close...



**Notes for the Viewer: Trying with Emotet GET requests** 







#### Notes for the Viewer: I took a bunch of Emotet samples from the same campaign. DEE

8559dde7-764a-47ab-844e-9e1881a99e9a.pcap Average between queries: 144,443 Total Queries: 16

76efeed5-e608-49de-81f6-4f5356c4641a.pcap Average between queries: 9,747 Total Queries: 5450

ad85a-cebc-4425-b428-7a1707d8d80e.pcap Average between queries: 5,574 Total Queries: 5

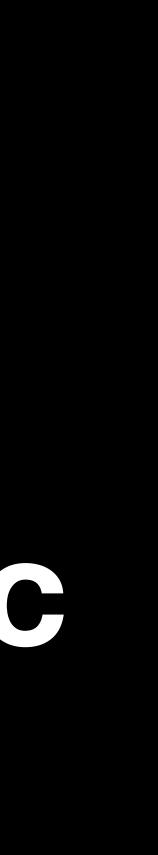
d74dfa64-f9bc-4696-b4f3-a66f329e0b27.pcap Average between queries: 3,804 Total Queries: 3425

Notes for the Viewer: I took a bunch of Emotet samples from the same campaign. Some are close, while the first isn't.

# **Compare Against Random Traffic**

Notes for the Viewer: Let's put some random traffic in the mix





### **Multiple Flows of Random Traffic**

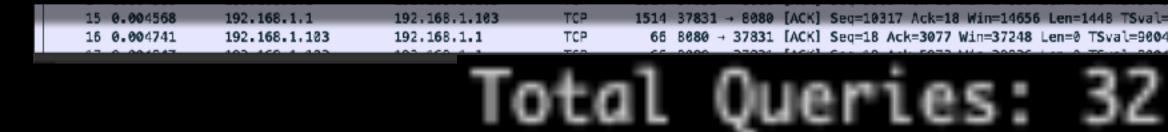
•••	•											
4	•	0		🔀 🏹	ৎ ৰ	🗢 🔿		<u></u>		9	୍	¢
Appl	y a displa;	y filter <	<b>∺/&gt;</b>									
No.	Time		Source		Dest	tination		Protocol	Length	Info		
Г	1 0.00	0000	192.168	.1.21	269	.180.174	.110	TCP	78	22000 →	1030	[\$
	2 0.00	0000	192.168	.1.21		.180.174		TCP		22000 -		
L	3 9.60			.174.110		.158.1.2		TCP	50	1030 → 2		
	4 0.00			.174.110		.168.1.2		TCP	68	22000 -		
	5 0.01	2993	192.168.	.1.21	269	.180.174	. 110	TCP	78	54 <b>96</b> 4 →		
	6 0.01		192.168.	.1.21		.180.174		TCP	78	54 <b>965</b> →		
	7 0.01			.174.110		.158.1.2		TCP	60	22000 -		
	8 0.01		209.180.	.174.110		.158.1.2		TCP	58	1030 - 3	54965	[F
	9 0.50			i_cd:d7:aa		P_Multic		LLDP		MA/b4:fl		
	10 0.63	0242		i_cd:d7:aa	i Spa	nning-tr	ee-(fo	or… STP	60	RST. Roo	pt = 3	27
	11 0.66		91.106.1			.168.1.2		TLSv1		Applicat		
	12 0.67		192.168.			105.174.		TCP		54606 →		
	13 0.67		192.168.			105.174.		TLSv1		Applicat		
	14 0.75		192.168.			.168.1.2		TCP	60	9300 → 5		
	15 0.75	9956	192.168.		192	.158.1.2		TCP	50	9300 - 5		
	16 0.83	8812	91.106.1	174.245		.168.1.2	-	TCP	66	22067 →		
	17 0 07	0000	102 100	4 24			-	700		54050	00 10	



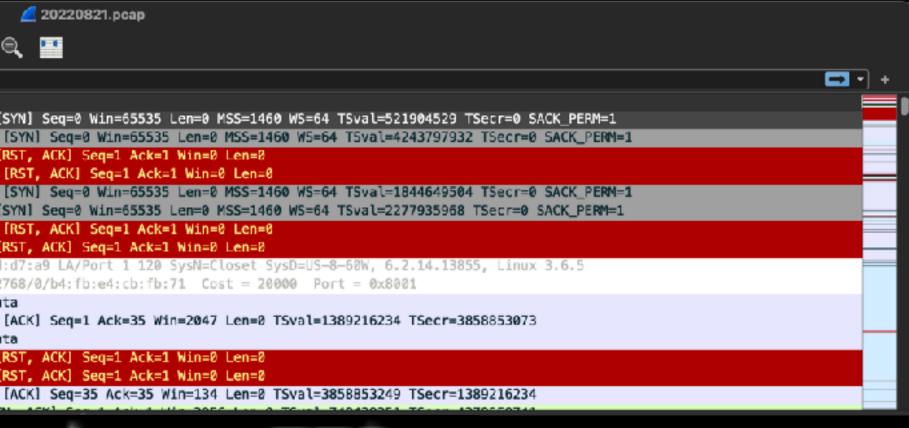
### **One Flow from this Traffic**

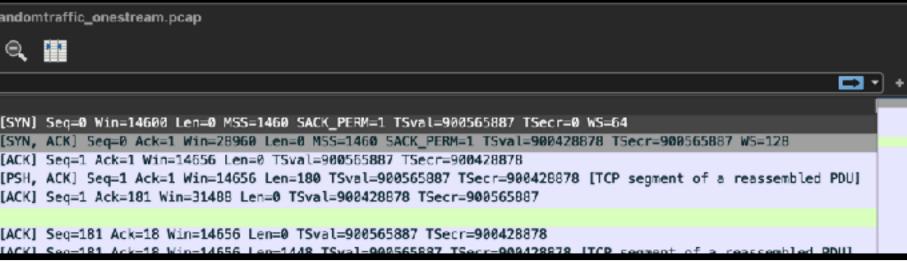
••	•						4	ran
	🔳 🙍 🎯	🚞 🖹 😫	् 🗢 🗢 🚰	중 🕹 🛽		•	Q,	¢
📕 Ar	pply a display filter	. <#/>						
No.	Time	Source	Destination	Protocol	Length	Info		
	1 0.000200	192.168.1.1	192.168.1.103	TCP	74	3 <b>78</b> 31 →	B <b>080</b>	[5
	2 0.000203	192.168.1.103	192.168.1.1	TCP	74	8080 - 3	7831	[5
	3 0.000448	192.168.1.1	192.168.1.103	TCP	66	37831 →	8 <b>080</b>	[A
	4 0.001146	192.168.1.1	192.168.1.103	TCP	246	37831 -	8080	[F
	5 0.001287	192.168.1.103	192.168.1.1	TCP	66	8080 - 3	7831	[A
	6 0.003409	192.168.1.103	192.168.1.1	HTTP	83	HTTP/1.1	100	
	7 0.003633	192.168.1.1	192.168.1.103	TCP	66	37831 →	8080	V
	8 0 00/502	102 168 1 1	102 168 1 183	TCP	1514	37831 -	8080	1/

#### Notes for the Viewer: Use a full PCAP with many network flows, and also take one flow from that PCAP to use.









l514 37831 → 8080 [ACK] Seq=10317 Ack=18 Win=14656 Len=1448 TSval=900565887 TSecr= 66 8080 → 37831 [ACK] Seg=18 Ack=3077 Win=37248 Len=0 TSval=900428878 TSecr=90056588









# 14748 719904648391: 16125 116391184572: 8356.612903225807: 72144.2343387471:

**Notes for the Viewer:** The two Trickbot averages of times in between look a lot closer now to each other than they do with the random traffic. Maybe this is a good direction to go?



# Trickbot POST 1 Trickbot POST 2 Random Traffic, one stream Random Traffic, full stream



### Find a sample of something I know is bad:

https://www.malware-traffic-analysis.net/2022/04/25/index.html В

#### 2022-04-25 (MONDAY) - EMOTET EPOCH 4 ACTIVITY (LNK FILES)

REFERENCE:

ASSOCIATED FILES:

 2022-04-25-IOCs-for-Emotet-epoch4.txt.zip 2.3 kB (2,302 bytes) 2022-04-25-Emotet-epoch4-malspam-10-examples.zip 46.0 kB (45,961 bytes) 2022-04-25-Emotet-enoch4-attachments zin 37.0 kB (37.037 bytes) 2022-04-25-Emotet-epoch4-infection-with-spambot-traffic.pcap.zip 8.5 MB (8,495,143 bytes) ZUZZ-04-Z5-EMOTET-EDOC04-Maiware-and-artitacts.zid Z99 KB (Z98.940 ovies)

#### **Notes for the Viewer:** Trying again with another sample to see I get similar results. This time a GET request for Emotet.

### DEEPSEC

https://www.malware-traffic-analysis.net/2022/04/25/index.html



https://twitter.com/Cryptolaemus1/status/1517634855940632576



Time		Dst	port	Host
2022-04-25	16:50:14	77.105.36.156	80	filn
2022-04-25	16:51:07	138.197.147.101	443	
2022-04-25	16:51:09	138.197.147.101	443	
2022-04-25	16:51:34	49.231.16.102	8080	
2022-04-25	16:51:36	138.197.147.101	443	
2022-04-25	16:51:58	138.197.147.101	443	
2022-04-25	16:52:00	138.197.147.101	443	
2022-04-25	16:52:01	93.104.209.56	8080	
2022-04-25	16:52:23	138.197.147.101	443	
2022-04-25	16:52:46	138.197.147.101	443	
2022-04-25	16:52:49	138.197.147.101	443	
2022-04-25	16:52:49	131.100.24.199	7080	
2022-04-25	16:53:15	138.197.147.101	443	
2022-04-25	16:53:40	138.197.147.101	443	
2022-04-25	16:53:43	138.197.147.101	443	
2022-04-25	16:53:43	51.210.176.76	443	
2022-04-25	16:54:08	138.197.147.101	443	
2022-04-25	16:54:36	138.197.147.101	443	
2022-04-25	16:54:37	138.197.147.101	443	
2022-04-25	16:54:39	49.231.16.102	8080	
2022-04-25	16:55:04	138.197.147.101	443	
2022-04-25	16:55:31	138.197.147.101	443	
2022-04-25	16:55:33	138.197.147.101	443	
2022-04-25	16:56:02	138.197.147.101	443	
2022-04-25	16:56:05	138.197.147.101	443	

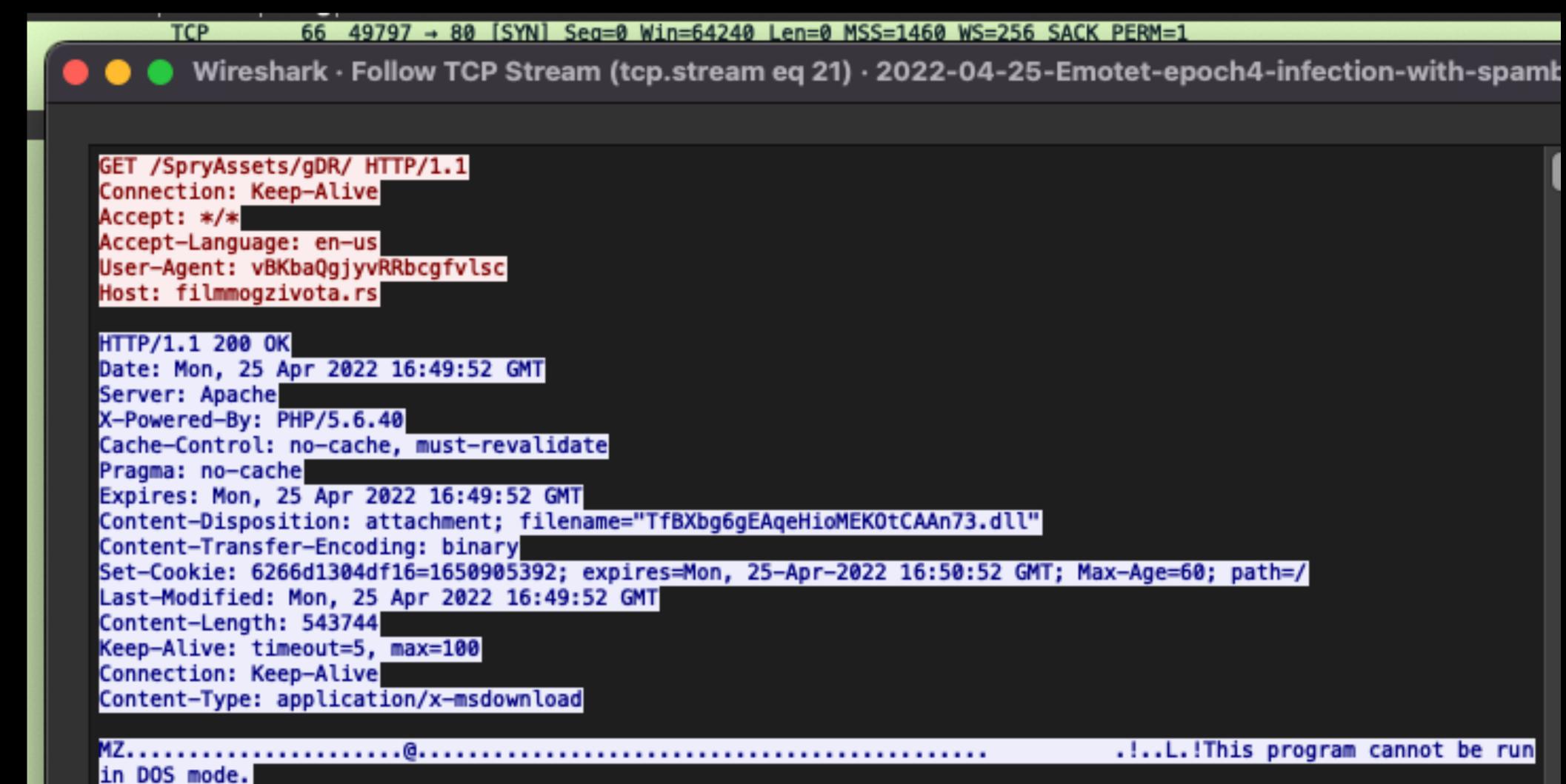
**Notes for the Viewer:** Trying again with another sample to see I get similar results. This time a GET request for Emotet.



t	Info				
.mmogzivota.rs	GET /SI	orvAsset	s/gDR/	HTTP/1.1	
	Client	Hello			
<b>4</b>	Client	Hello			
	Client	Hello			
	Client	Hello		EMO	l
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Hit	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			
	Client	Hello			

https://www.malware-traffic-analysis.net/2022/04/25/index.html

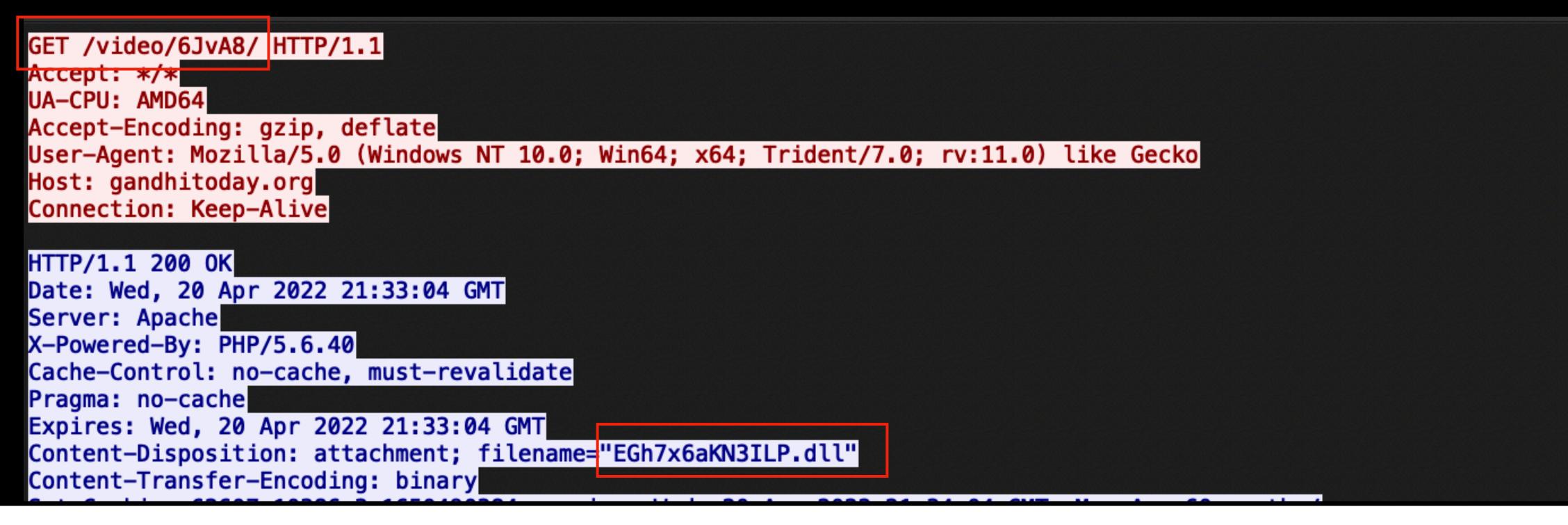




**Notes for the Viewer:** Take the whole PCAP, and just grab the part I want (the flow containing the GET request)

DEEPSEC2022-04-25-Emotet-epoch4-infection-with-spambot-traffic.pcap

# **Another PCAP with similar activity**



**Notes for the Viewer:** 

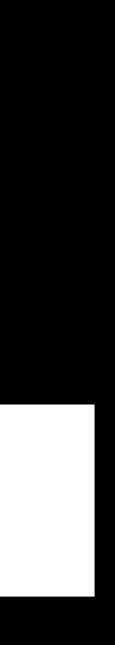
Grab the part I want (the flow containing the GET request) from a similar, but different PCAP



2022-04-20-Emotet-epoch4-infection-with-spambot-traffic.pcap



.!..L.!This program cannot be run



## The GET request: Not Really Matching

2022-04-20-Emotet-epoch4-dll\_download\_0.cap Average beteen queries: 8598.687198067633 Total Queries: 829

#############

1 Flows in 2022-04-20-Emotet-epoch4-dll\_download.pcap

#############

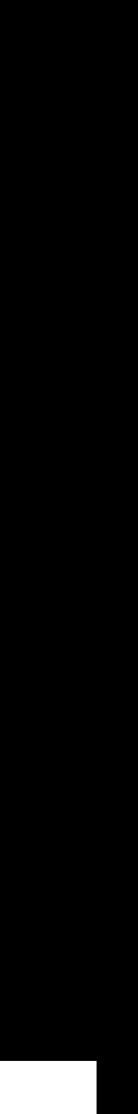
2022-04-25-Emotet-epoch4-dll\_download\_0.cap Average beteen queries: 3529.211367673179 Total Queries: 564

#############

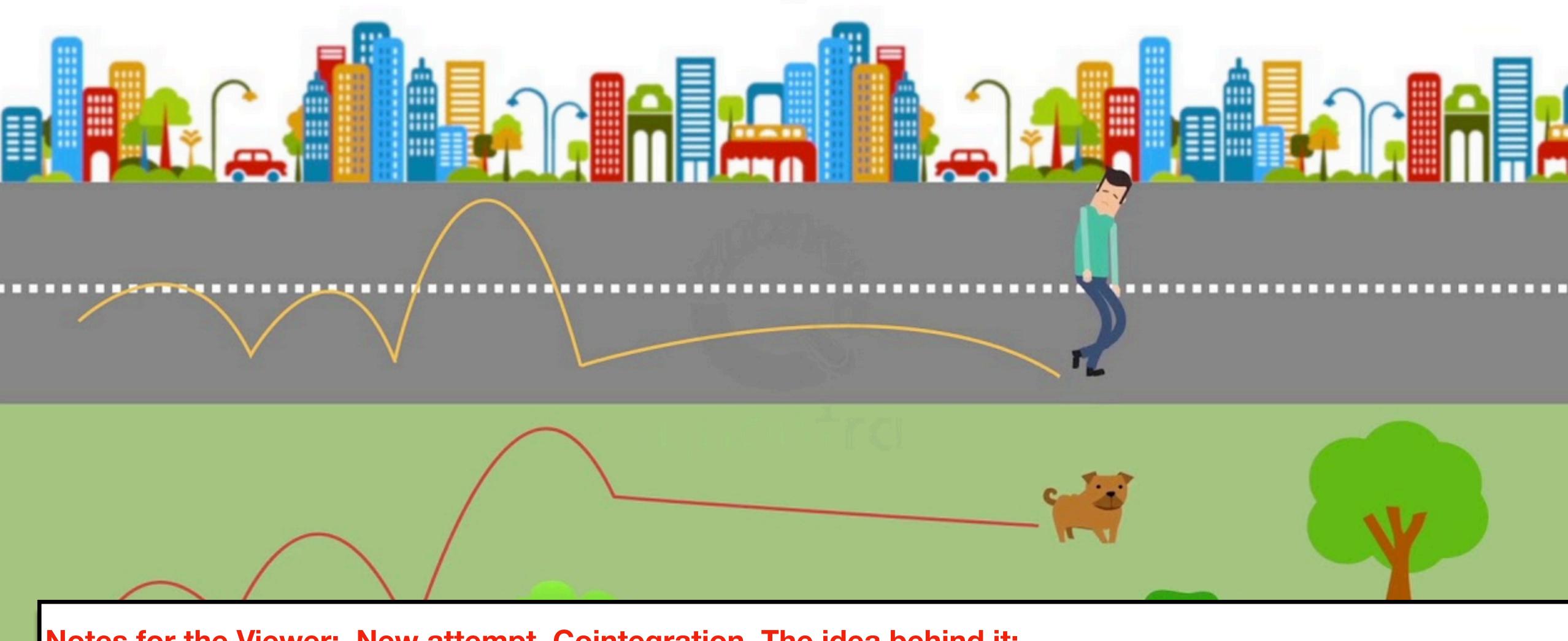
1 Flows in 2022-04-25-Emotet-epoch4-dll\_download.pcap

#############

Notes for the Viewer: They aren't matching very well this time. Maybe this isn't the best direction



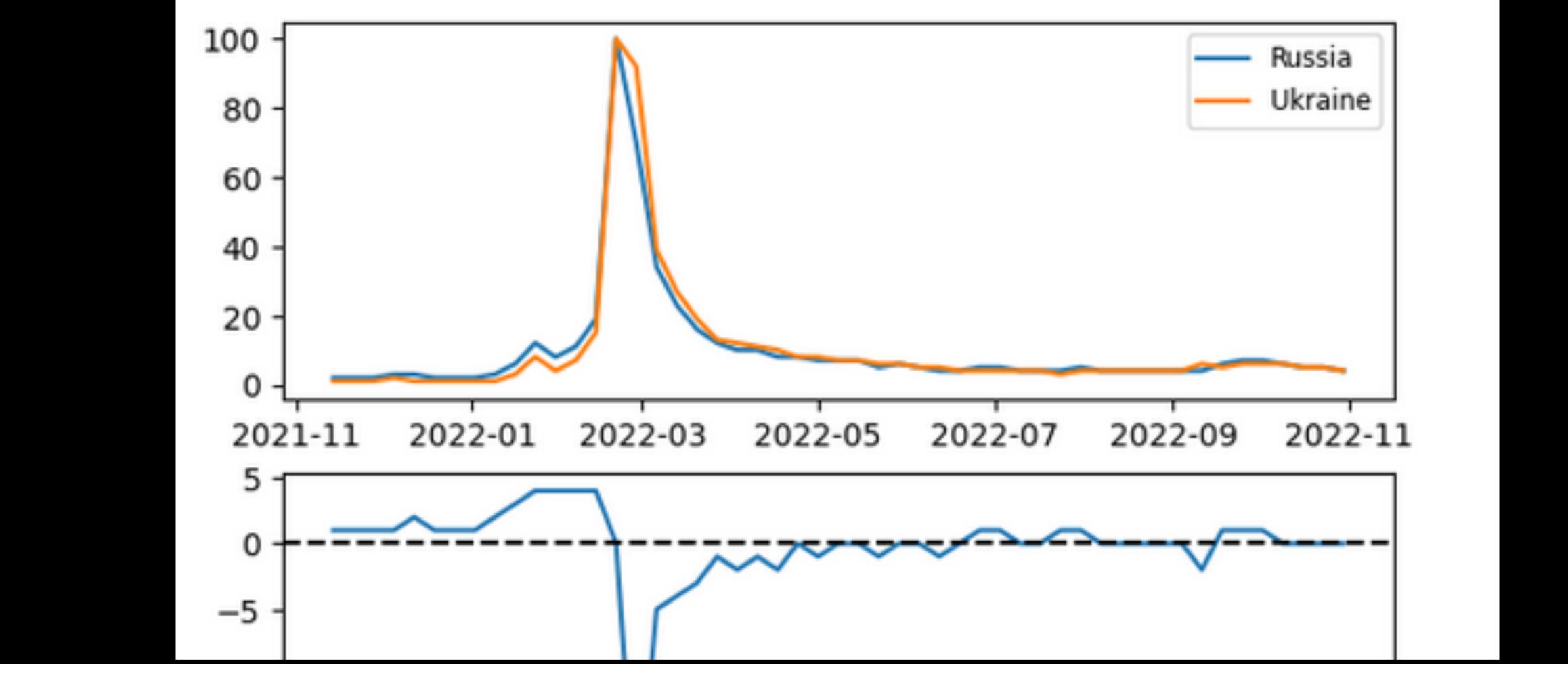
# Cointegration



Notes for the Viewer: New attempt, Cointegration. The idea behind it: Drunk guy and a dog are walking the same direction. They look like they might be together. That's correlation, but then if they start to drift apart, maybe they aren't together. So their timeline looks to be the same, but if they aren't going the same direction, they aren't cointegrated. If they do continue walking together, eventually it can be assumed that they are together, aka cointegrated.

D



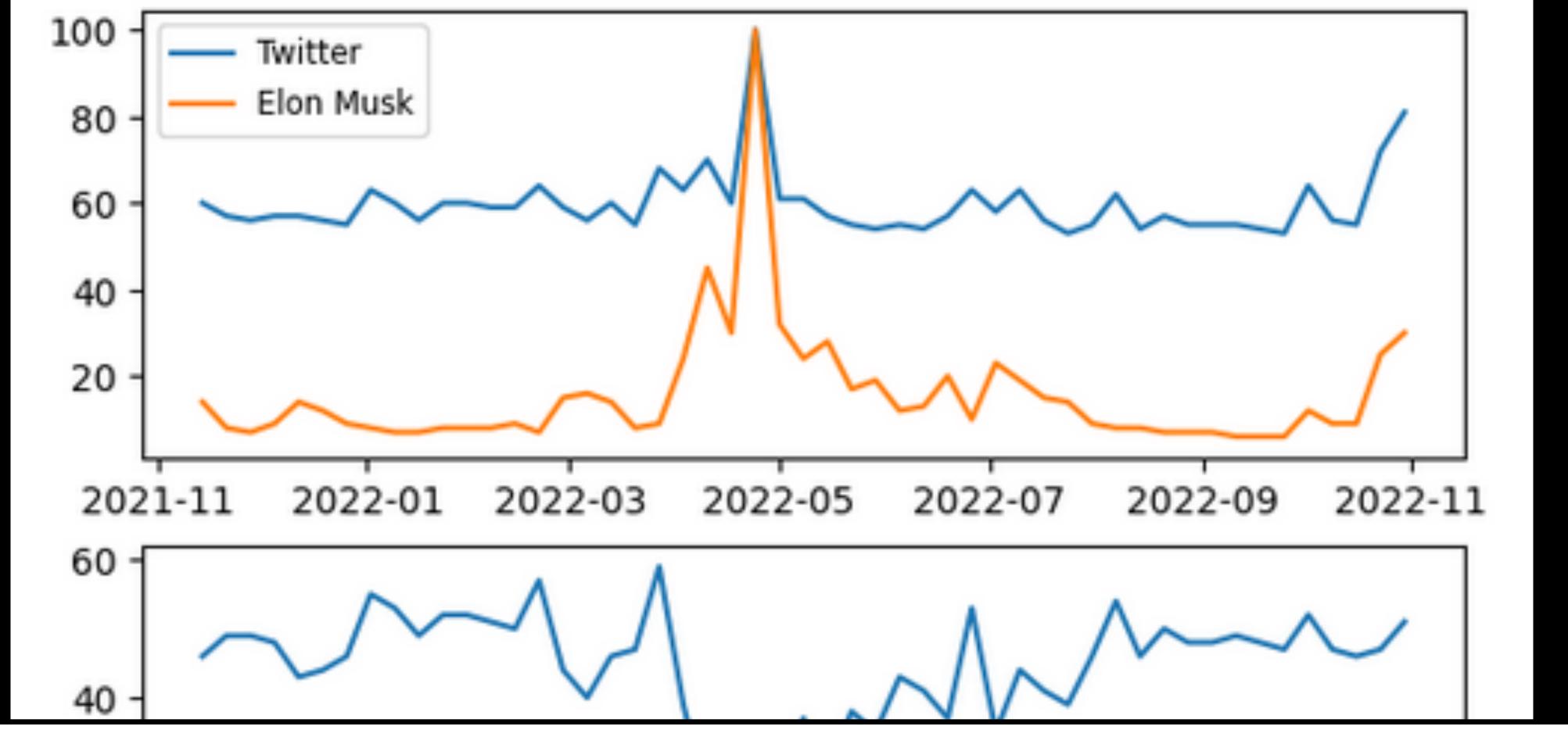


Notes for the Viewer: Conintegration example #1, just to understand. Google searches over one year for 'Russia' and 'Ukraine'. They look like they're together. The bottom graph (called 'the spread') primarily stays on 0, showing they are also cointegrating. So the searches correlate **AND** cointegrate



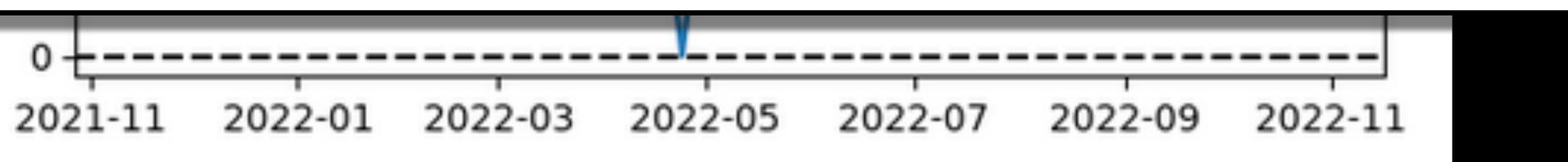
2021-11 2022-05 2022-09 2022-01 2022-03 2022-07 2022-11





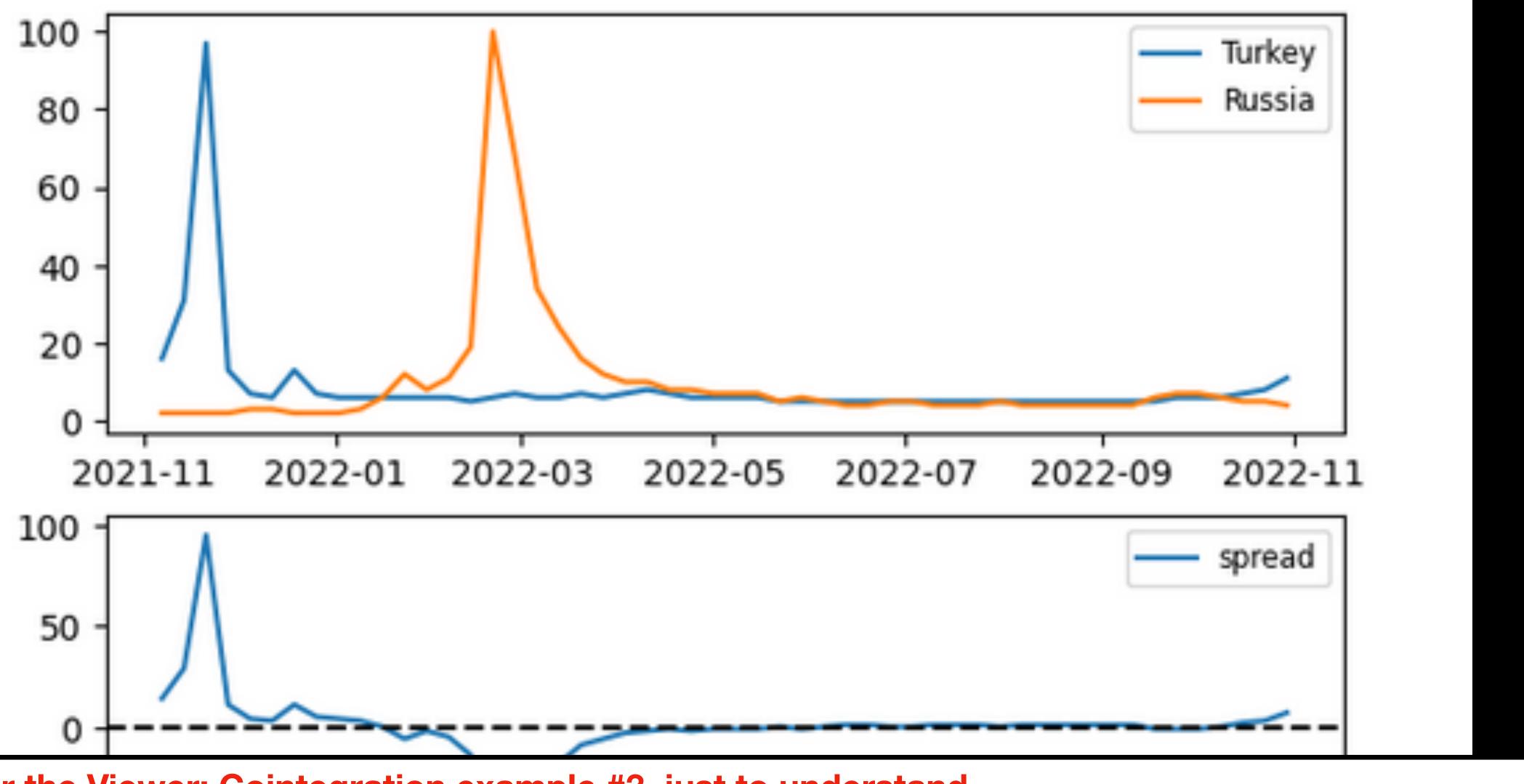
Notes for the Viewer: Conintegration example #2, just to understand. Google searches over one year for 'Twitter' and 'Elon Musk'. They look like they correlate, but the spread doesn't quite show a relationship since it's not primarily staying on 0. So the searches correlate but do not cointegrate

DEEPSEC







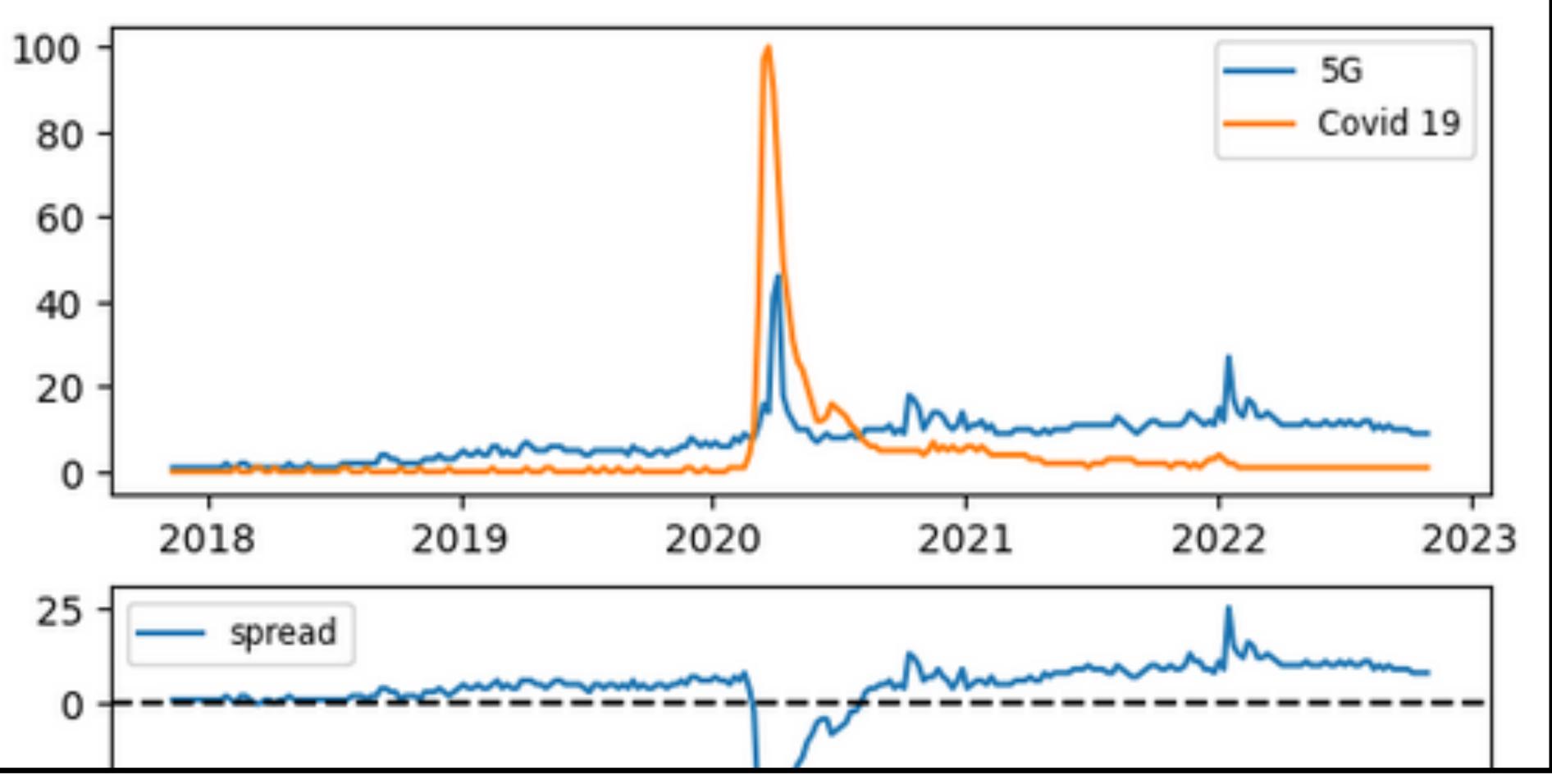


Notes for the Viewer: Cointegration example #3, just to understand. spread however primarily stays on 0, showing they are cointegrating. So the timelines are similar/matching.

-1002021-11 2022-01 2022-03 2022-05 2022-07 2022-09 2022-11 DEEPSEC

Google searches over one year for 'Turkey' and 'Russia'. They don't look like they're lining up, suggesting no correlation. The

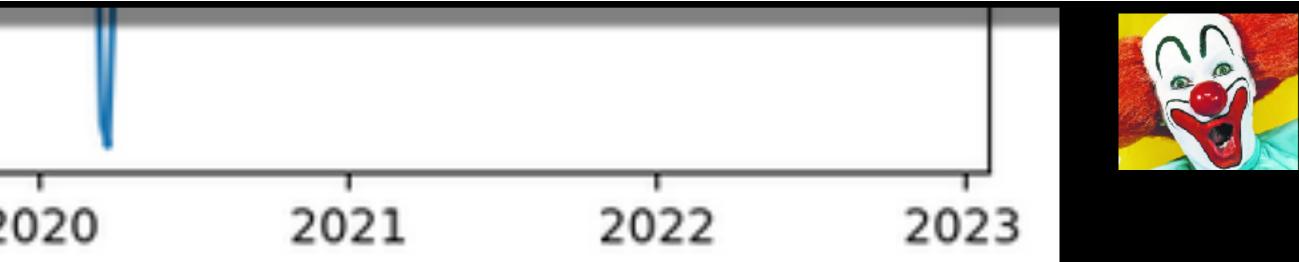






DEEPSEC

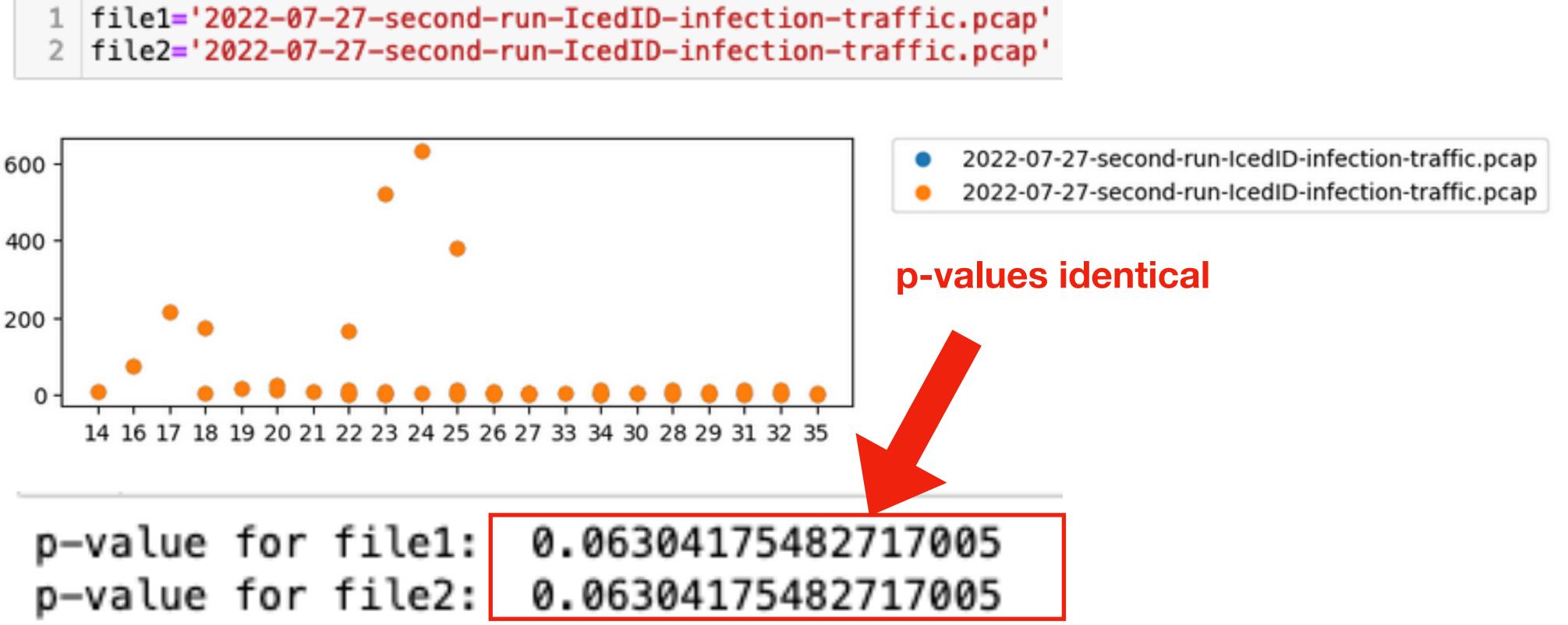
Notes for the Viewer: Conintegration example #4, just to understand. Google searches over one year for '5G' and 'Covid 19'. Timelines line up and the spread stays on 0. Unfortunately, google searches for 5G and Covid 19 cointegrate and correlate.

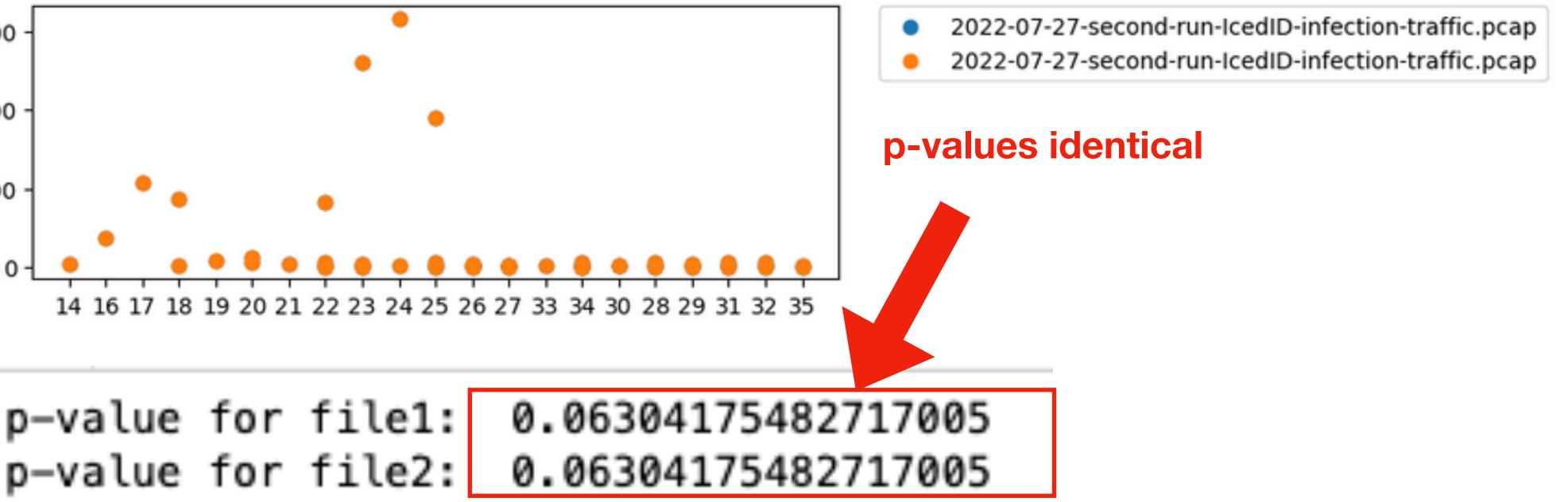


# Two identical PCAP files They should cointegrate



# Identical PCAP files: 100% Cointegration





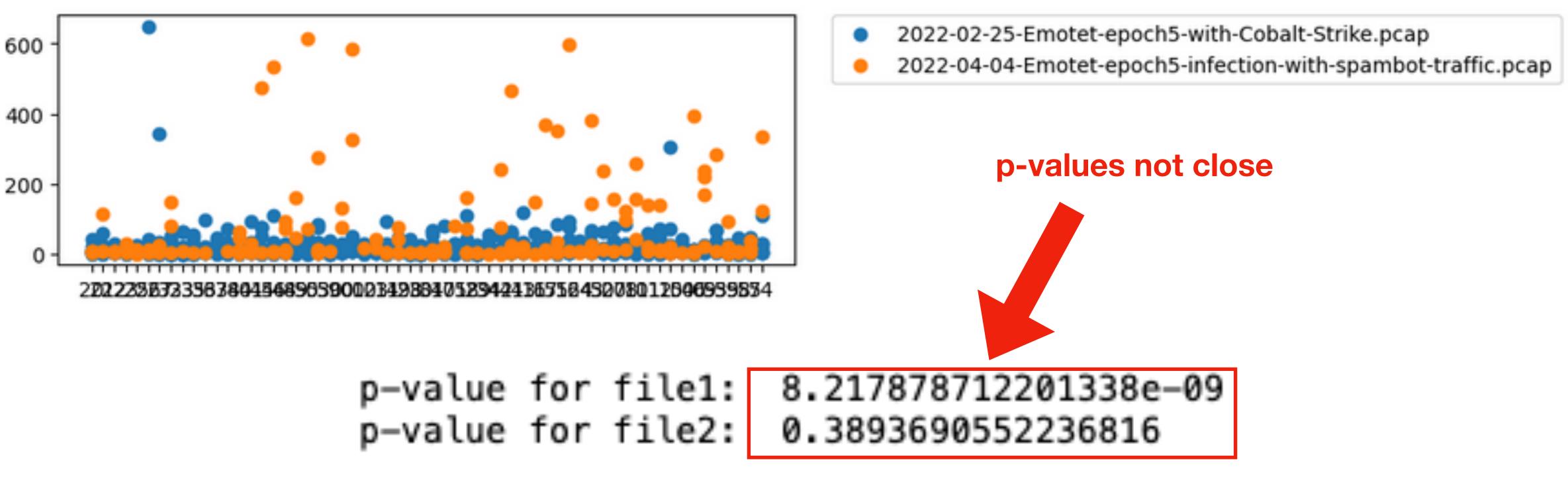




# Two different PCAP files They should not cointegrate



# Two different PCAP files: No Cointegration



**Notes for the Viewer:** 

### DEEPSEC

#### Two pcaps that seem similar, but are actually following different timelines. They likely won't cointegrate. There is likely too much going on in these since they are full packet captures with all the flows.



# But now there's a method to start finding similarities



# Two different PCAP files With similar traffic



# **Two PCAP files: Similar Traffic**











192.168.100.205







.stre	am eq 2				GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2 Connection: Keep-Alive Accept: */*
22 23 24 25	Time 0.350055 0.362456 0.362496 0.362522 0.407985 0.439880	Source 192.168.100.102 93.184.220.29 93.184.220.29 93.184.220.29 192.168.100.102 93.184.220.29	Destination 93.184.220.29 192.168.100.102 192.168.100.102 192.168.100.102 93.184.220.29 192.168.100.102	ProtocLeHTTP2TCP12TCP2OCSP3HTTP2OCSP5	User-Agent: Microsoft-CryptoAPI/6.1 Host: ocsp.digicert.com HTTP/1.1 200 OK Accept-Ranges: bytes Age: 4679 Cache-Control: 'max-age=158059' Content-Type: application/ocsp-response Date: Mon, 19 Sep 2022 03:49:48 GMT Last-Modified: Mon, 19 Sep 2022 02:31:49 GMT
	am or 0				Server: ECS (amb/6B86) X-Cache: HIT Content-Length: 1507

#### tcp.stream eq 0 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5858daff14fe131d HTTP/1.1 Connection: Keep-Alive Destination Protoc | Ler Time Source Accept: \*/\* 1 0.000000 192.168.100.205 93.184.221.240 HTTP 34 If-Modified-Since: Tue, 15 Sep 2020 17:59:10 GMT 126 If-None-Match: "06b9ae9898bd61:0" 3 0.060479 93.184.221.240 192.168.100.205 TCP User-Agent: Microsoft-CryptoAPI/6.1 4 0.060520 192.168.100.205 TCP 126 93.184.221.240 Host: ctldl.windowsupdate.com 126 0.060537 192.168.100.205 TCP 93.184.221.240 5 126 0.061314 93.184.221.240 192.168.100.205 TCP 6 HTTP/1.1 200 OK 39 0.062094 93.184.221.240 HTTP 192.168.100.205 7 Accept-Ranges: bytes 24 24 9.347911 192.168.100.205 HTTP 93.184.221.240 Age: 803 25 9.390606 93.184.221.240 192.168.100.205 Cache-Control: public,max-age=900 TCP 126 26 9 27 g **9. Notes for the Viewer:** 28 29 30 two separate PCAPs that are doing similar activity. It's benign - just GET requests to Microsoft domains 31 32 9.39243 192.100.100.20. TCP 126 DEEPSEC:184.221.240 192.168.100.205 TCP

126

тср

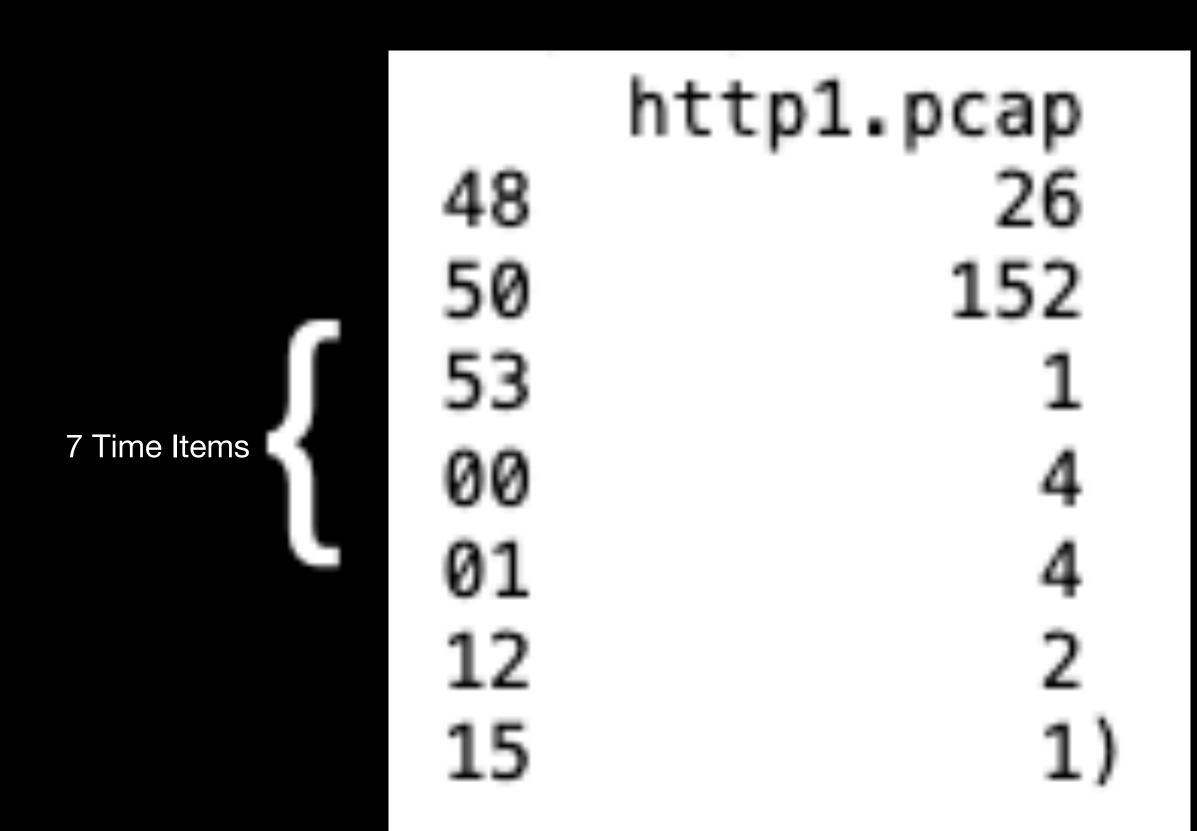
X-Powered-By: ASP.NET Content-Length: 4817



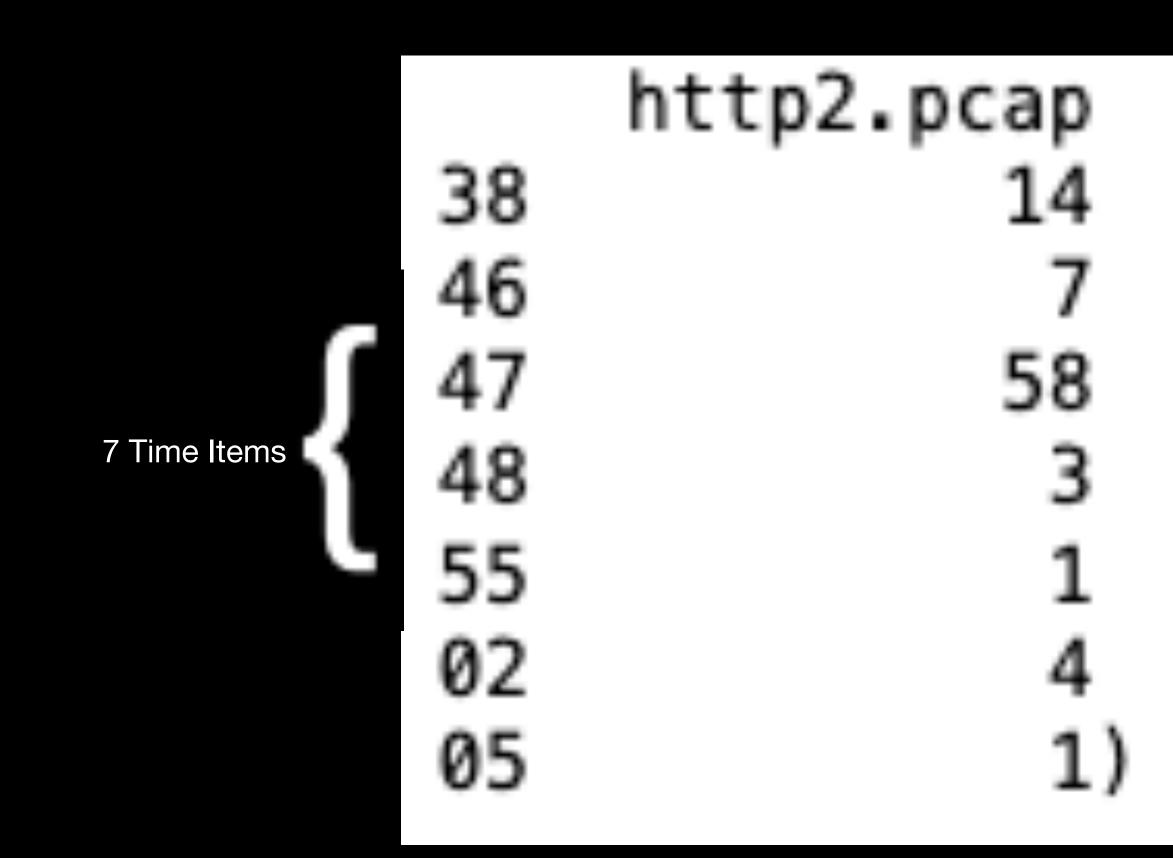


# **Two PCAP files: Similar Traffic**

**Transactions per Second** 

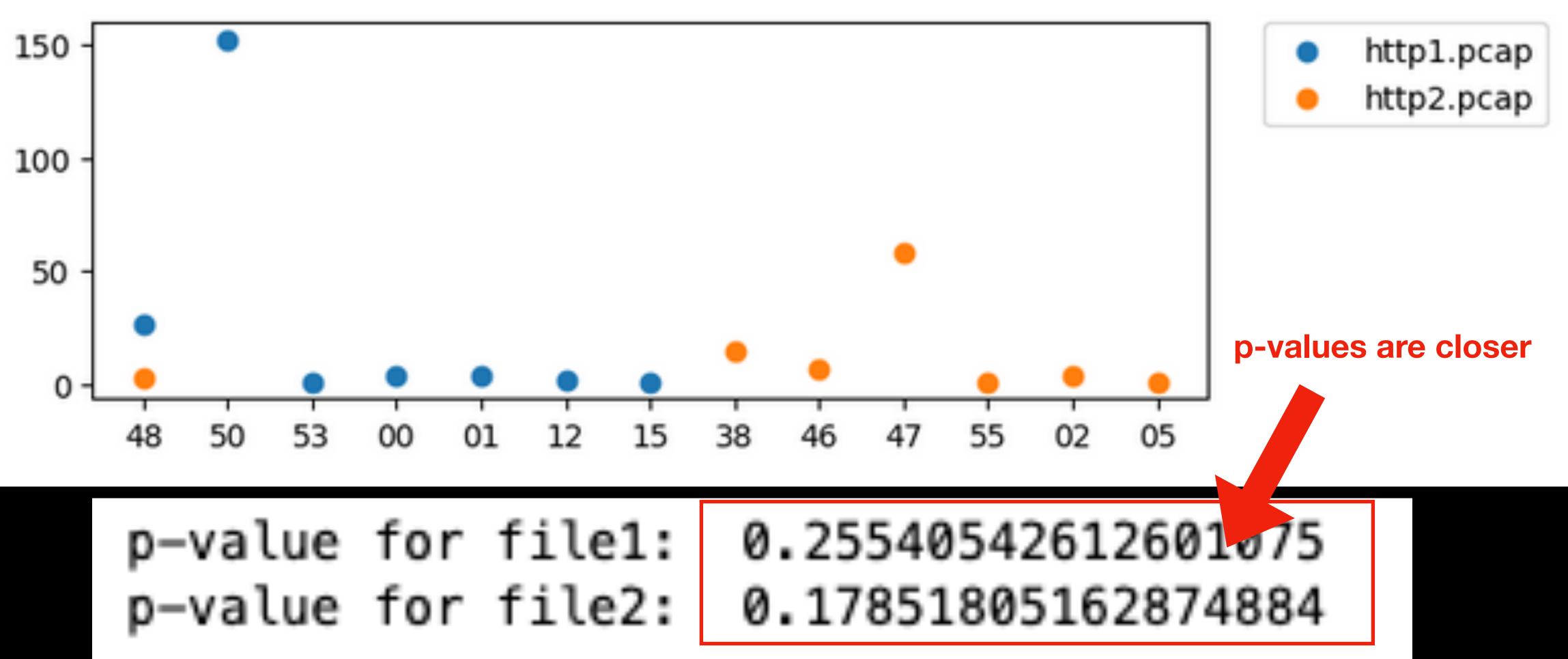








# **Two PCAP files: Similar Traffic**



### DEEPSEC

# **Problems with Cointegration**



# **Problems with Cointegration: The Time Value**

ht	tp1.pcap	2022-07-27-secon 14	d-run-IcedID-infection-traffic.pcap 7
48	26	16 17 18 18	76 213 174
50	152	19 20 21	16 27 7
53	1	22 23 24 25	164 519 632 378
00	4	26 27 33 34	5 2 6 2
01	4	26 27 30	2 6 6 6
12	2	34 27 20 22	4 3 13 2
15	1)	22 22 23 23	4 13 2

**Notes for the Viewer:** Two time-series of different lengths - I can't use them. I tried normalizing by calculating percentages, but that didn't quite work because then it's not enough data points to do the cointegration tests.

DEEPSEC

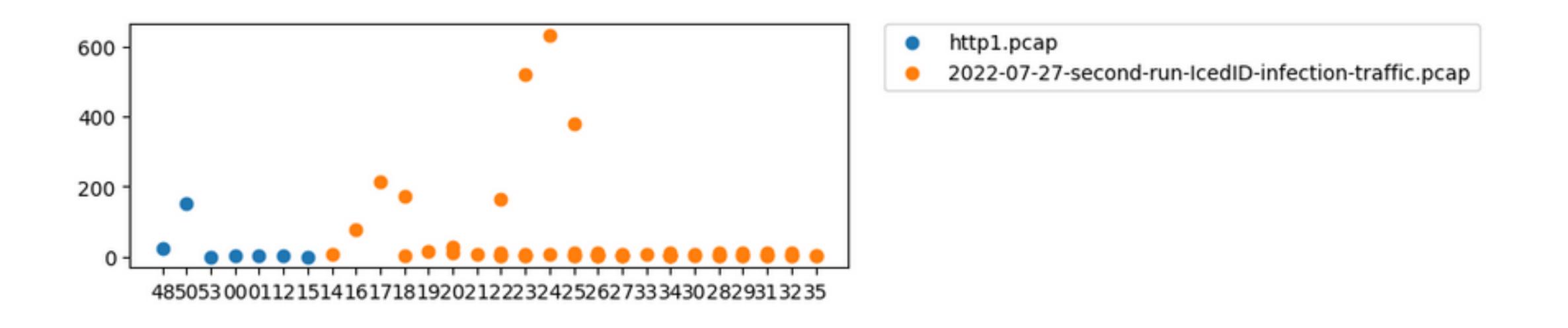
30 31





# **Problems with Cointegration: The Time Value**





# p-value for file2:

#### **Notes for the Viewer:**

D

We can run the cointegration test on the timelines, but it's a bit messed up using seconds for the time. And having drastically different timeline lengths can cause some confusion. Here though, you can see that the p-value's don't match, so at least we have that.

file2='2022-07-27-second-run-IcedID-infection-traffic.pcap'

### p-value for file1: 0.25540542612601075 0.06304175482717005



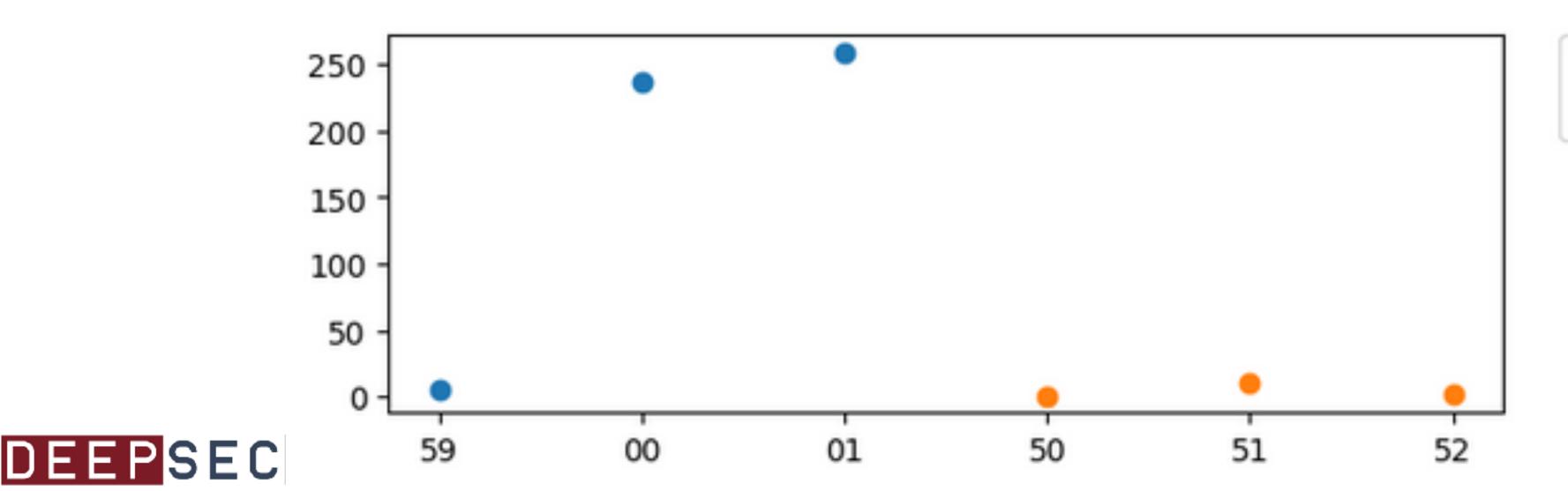
### Short Sample Size



### **Problems with Cointegration: Short Sample Size**

2

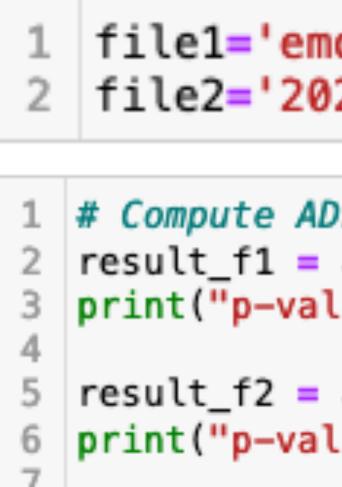
<pre>emotet_get.pcap</pre>
5
237
259



- file1='emotet\_get.pcap' file2='2021-01-04\_sig.cap'
  - 2021-01-04\_sig.cap 50 51 10 52 2)

emotet\_get.pcap 2021-01-04\_sig.cap

### **Problems with Cointegration: Short Sample Size**

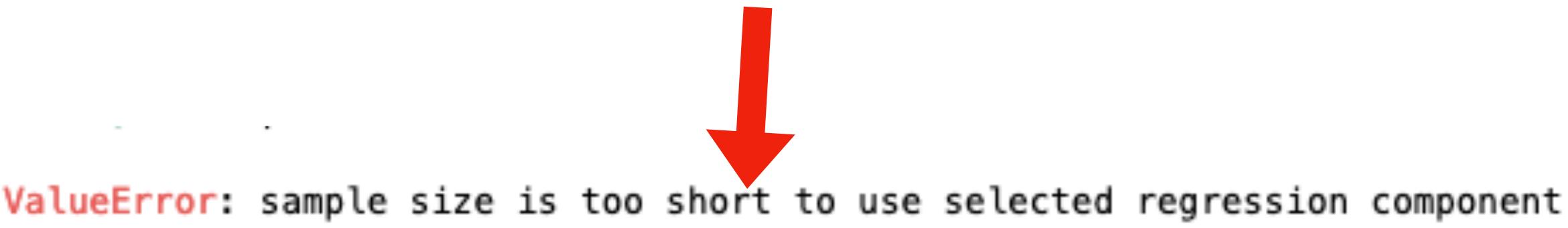




```
file1='emotet_get.pcap'
file2='2021-01-04_sig.cap'
```

```
# Compute ADF for the two PCAPs:
2 result_f1 = adfuller(df_f1[file1])
  print("p-value for file1: ",result_f1[1])
```

```
result_f2 = adfuller(df_f2[file2])
 print("p-value for file2: ",result_f2[1])
```

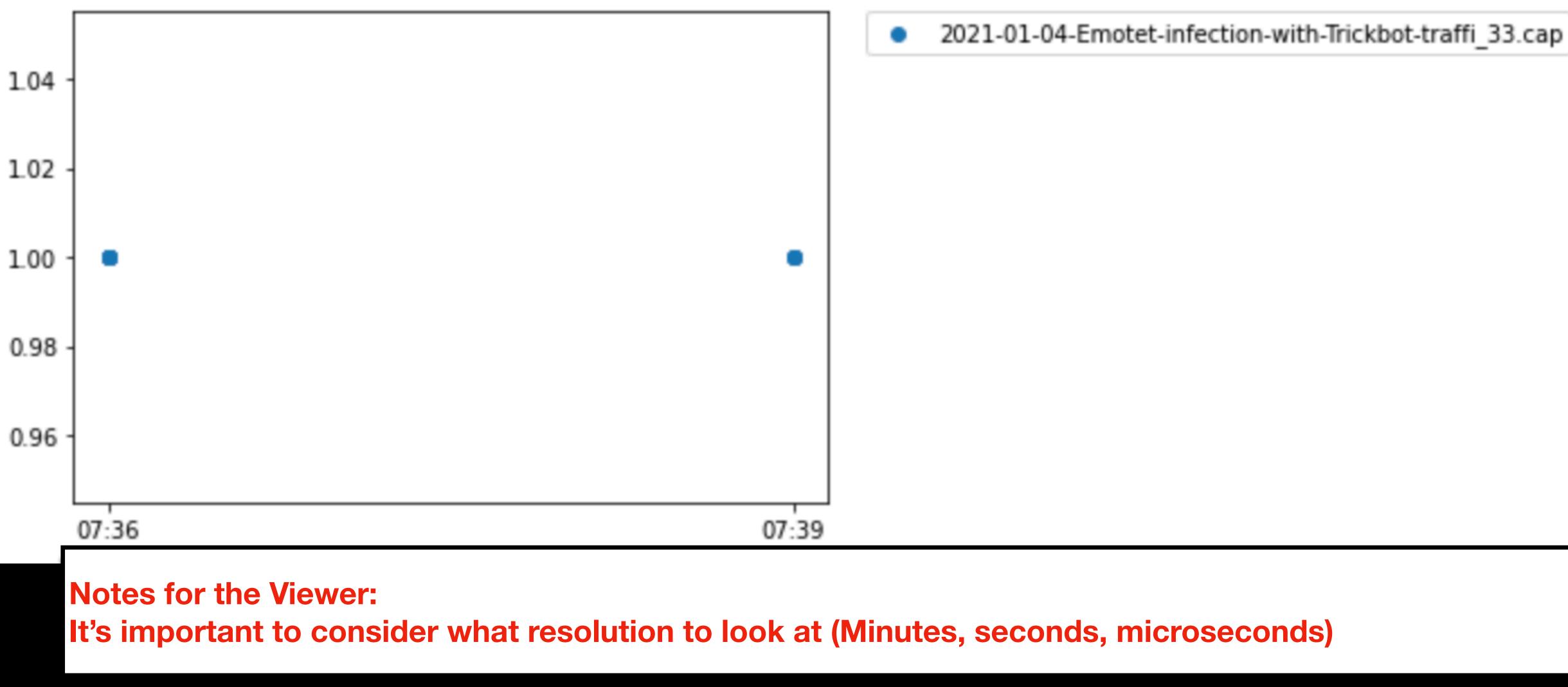




## Time Resolution

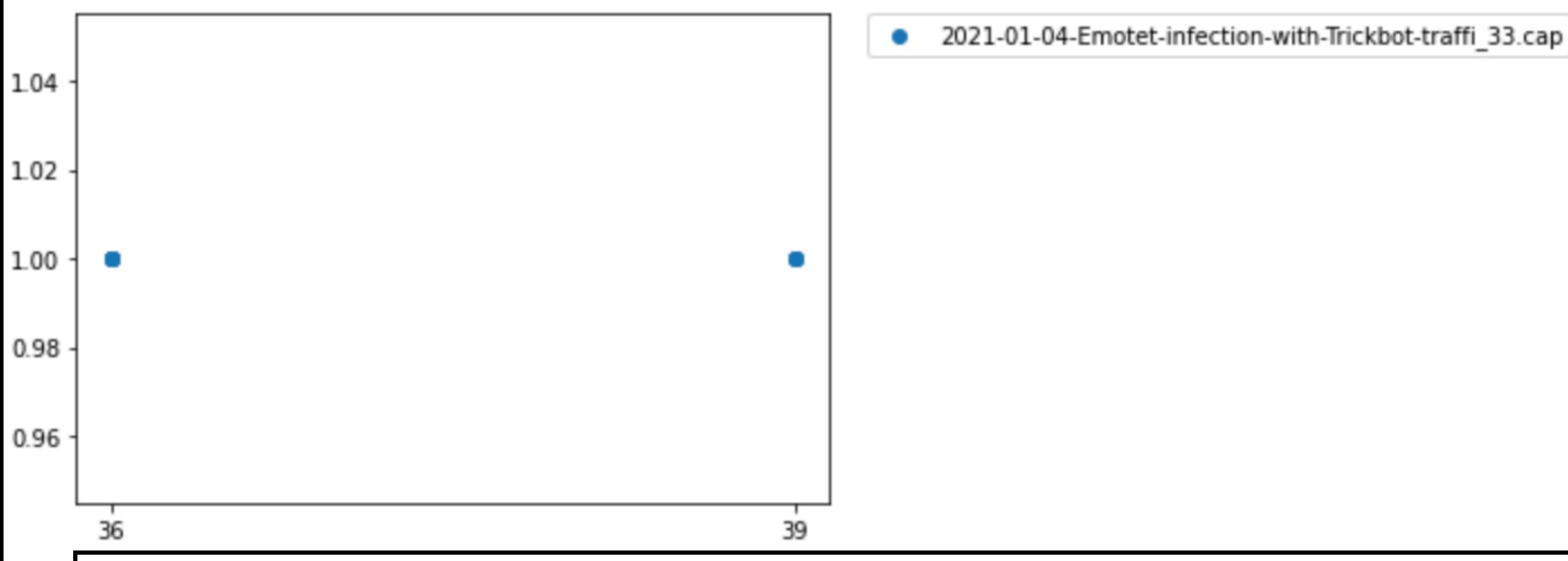
Notes for the Viewer: It's important to consider what resolution to look at (Minutes, seconds, microseconds)

## At the 'Minutes' Resolution





## At the 'seconds' Resolution

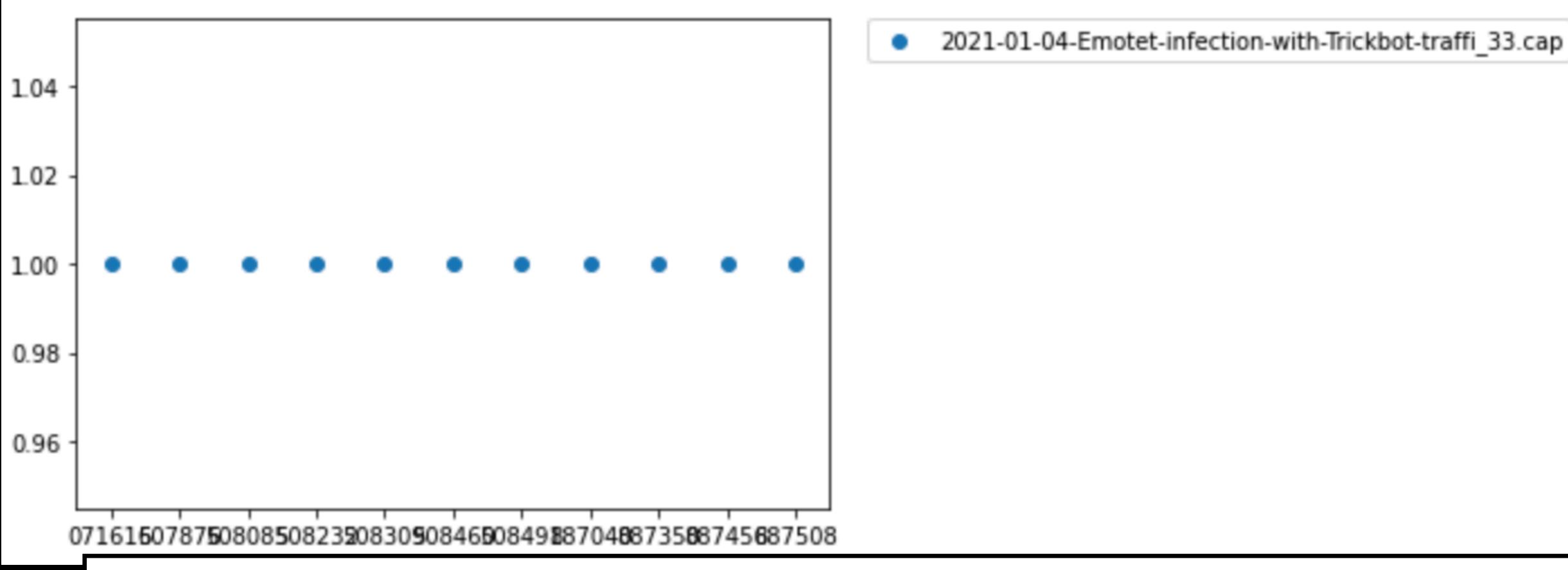


#### **Notes for the Viewer:** It's important to consider what resolution to look at (Minutes, seconds, microseconds)





## At the 'microseconds' Resolution



**Notes for the Viewer:** It's important to consider what resolution to look at (Minutes, seconds, microseconds)



**Notes for the Viewer:** It helps to normalize the times

### DEEPSEC

Normalize

### Normalized: Time a Transaction Occurred

for i in when\_transactions\_happened: print(i['date'],i['count'])

<u>2021–01–04–Em</u>otet–infection–with–Trickbot–traffi\_33.cap 2000-01-01T00:00:00.071616+00:00 1 2000-01-01T00:00:00.507876+00:00 1 2000-01-01T00:00:00.508085+00:00 1 2000-01-01T00:00:00.508232+00:00 1 2000-01-01T00:00:00.508309+00:00 1 2000-01-01T00:00:00.508460+00:00 1 2000-01-01T00:00:00.508491+00:00 1 

**Notes for the Viewer:** I rewrote the time to 2000-01-01, 00:00 to normalize

DEEPSEC-01-01T00:00.887508+00:00

### Normalized: Time Between Transactions

### for i in full\_timeline\_from\_zero: print(i)

2000 - 01 - 01T00:00:00+00:002000-01-01T00:00:00.436260+00:00 2000-01-01T00:00:00.436469+00:00 2000 - 01 - 01T00:00:00.436616 + 00:002000-01-01T00:00:00.436693+00:00 2000-01-01T00:00:00.436844+00:00 2000-01-01T00:00:00.436875+00:00 2000-01-01T00:00:00.815424+00:00 2000-01-01T00:00:00.815734+00:00 2000 - 01 - 01T00:00.815840 + 00:00

**Notes for the Viewer:** And then calculated the times in between starting from that normalized start time.

#### DEEPSEC

### 2021-01-04-Emotet-infection-with-Trickbot-traffi\_33.cap

### Combo of the two

start at zero	2000-01-01T00:00:00+00:00
	2000-01-01T00:00:00
436,260 ms between	2000-01-01T00:00:00.436260+
	2000-01-01T00:00:00
436469 ms between	2000-01-01T00:00:00.436469+
	2000-01-01T00:00:00
436616 ms between	2000-01-01T00:00:00.436616+
	2000-01-01T00:00:00
436693 ms between	2000-01-01T00:00:00.436693+
	2000-01-01T00:00:00
436844 ms between	2000-01-01T00:00:00.436844+
	2000-01-01T00:00:00
436875 ms between	2000-01-01T00:00:00.436875+
	2000-01-01T00:00:00
815424 ms between	2000-01-01T00:00:00.815424+
017704 mere le etu $x = e$	2000-01-01T00:00:00
815/34 ms between	2000-01-01T00:00:00.815734+
	2000-01-01T00:00:00
815840 ms between	2000-01-01T00:00:00.815840+
	2000-01-01T00:00:00
815892 ms between	2000-01-01T00:00:00.815892+
	2000-01-01T00:00:00

- 0.071616+00:00 1
- +00:00
- 0.507876+00:00 1 +00:00
- 0.508085+00:00 1 +00:00
- 0.508232+00:00 1 +00:00
- 0.508309+00:00 1
- +00:00
- 0.508460+00:00 1 +00:00
- 0.508491+00:00 1
- +00:00
- 0.887040+00:00 1
- +00:00
- 0.887350+00:00 1
- +00:00
- 0.887456+00:00 1
- +00:00
- 0.887508+00:00 1
- Transaction 1 Transaction 2 Transaction 3 Transaction 4 Transaction 5 Transaction 6 Transaction 7 Transaction 8 Transaction 9 Transaction 10 Transaction 11



## Signature Creation

**Notes for the Viewer:** Now we'll take various parts of what's already been shown to start developing a signature that can be applied to find specific network traffic



### 1: Separate all the flows

			(U		4.120 18.00	ICF - 303 UDF	. 230		
Address A ^	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
0.0.0	255.255.255.255	2	684 bytes	2	684 bytes	0	0 bytes	0.000000	0.0009
<b>192.168.1.1</b>	192.168.1.221	437	45.674 KiB	219	28.996 KiB	218	1 <b>6.6</b> 78 KiB	0.000699	318.9567
192.168.1.1	255 <b>.25</b> 5.255 <b>.25</b> 5	1	322 bytes	1	322 bytes	0	0 bytes	3.539167	0.0000
192.168.1.221	13.33.61.67	51	15 <b>.9</b> 88 KiB	24	3.360 KiB	27	1 <b>2.6</b> 28 KiB	149.666647	131.3836
192.168.1.221	13.77.161.179	6	354 bytes	4	228 bytes	2	126 bytes	51.449515	0.2600
192.168.1.221	34.240.211.33	33	4.615 KiB	16	3.353 KiB	17	1.263 KiB	179.483259	6.8793
192.168.1.221	37.1.217.172	23	2.514 KiB	12	1. <b>16</b> 4 KiB	11	1.350 KiB	138.918247	55.9 <b>94</b> 8
192.168.1.221	40.129.73.242	209	26.277 KiB	101	17.888 KiB	108	8.390 KiB	285.111452	37.1815
192.168.1.221	43.231.4.7	11	1.065 KiB	5	407 bytes	6	684 bytes	<b>57.00</b> 5241	2.0630
192.168.1.221	46.4.52.109	310	192.089 KiB	184	177.391 KiB	126	14.698 KiB	122 <b>.45104</b> 0	207.7845
192.168.1.221	46.28.66.2	143	32.562 KiB	65	21.941 KiB	78	1 <b>0.6</b> 20 KiB	122.212165	208.9215
192.168.1.221	46.137.75.217	33	4.514 KiB	16	3.251 KiB	17	1.263 KiB	266.025045	4.6886
192.168.1.221	46.226.52.104	33	4.553 KiB	16	3.290 KiB	17	1.263 KiB	196.090463	4.8636
192.168.1.221	47.43.18.9	1,021	150.433 KiB	495	110.665 KiB	526	39.768 KiB	124.075039	198.1918
192.168.1.221	52.41.212.0	97	35.338 KiB	45	8.518 KiB	52	26.820 KiB	266.660879	30.5 <b>6</b> 86
192.168.1.221	52.88.19.91	25	8.874 KiB	12	2.169 KiB	13	6.705 KiB	303.694859	16.1514
192.168.1.221	52. <b>16</b> 6.201.127	37	4.795 KiB	18	3.411 KiB	19	1.384 KiB	260.521988	10.4123
192.168.1.221	54.86.81.5	68	9.460 KiB	33	6.771 KiB	35	2.689 KiB	231.930751	35.3727
192.168.1.221	54.192.39.68	18	6.889 KiB	8	863 bytes	10	6.046 KiB	312.234250	10.2297
192.168.1.221	62.8.140.122	33	4.539 KiB	16	3.276 KiB	17	1.263 KiB	263.193602	8.5101
192.168.1.221	62.24.139.42	35	4.843 KiB	17	3.416 KiB	18	1.427 KiB	136.258808	7.1211
192.168.1.221	62.149.178.10	33	4.577 KiB	16	3.314 KiB	17	1.263 KiB	258.802042	3.7648
192.168.1.221	62.159.91.51	33	4.541 KiB	16	3.278 KiB	17	1.263 KiB	200.543042	10.9354
192.168.1.221	62.159.95.227	33	4.565 KiB	16	3.303 KiB	17	1.263 KiB	189.483022	8.7831
192.168.1.221	62.159.186.4	35	4.759 KiB	17	3.332 KiB	18	1.427 KiB	156.463835	13.3246
192.168.1.221	62.181.145.234	33	4.589 KiB	16	3.326 KiB	17	1.263 KiB	248.451866	10.6580
192.168.1.221	67.195.204.72	1,582	208.074 KiB	767	145.880 KiB	815	62.194 KiB	105.789059	198.3949
192.168.1.221	67.195.204.75	444	58.940 KiB	216	40.893 KiB	228	18.048 KiB	191.941130	79.4995
SEC 1.221	67.195.204.79	254	31.027 KiB	120	20.489 KiB	134	10.538 KiB	290.918861	39.8501
	67105 229 111	10	1 /70 ViD	6	125 butos	12	1 055 Kip	040 064547	10 0 4 9 6



### 2: Operate against each flow individually

	TXT	20	22-0	)2-25	5-En	notet	t-ep	och5	i-sp	a
	0101 0110 0111	20	22-0	)2-25	5-En	notet	t-ep	och5	i-sp	a
~		flo	wout	puts						
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	۰s
			2022	2-02-	-25-	Emo	tet-e	ерос	:h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	·s
			2022	2-02-	-25-	Emo	tet-e	epoc	:h5-	∙s∣
			2022	2-02-	-25-	Emo	tet-e	epoc	h5-	·s

DEEPSEC

mbot-traffic-snippet\_20221017-143616.txt mbot-traffic-snippet.pcap

pambot-traffic-snippet\_0.cap spambot-traffic-snippet\_1.cap pambot-traffic-snippet\_2.cap pambot-traffic-snippet\_3.cap pambot-traffic-snippet\_4.cap pambot-traffic-snippet\_5.cap pambot-traffic-snippet\_6.cap pambot-traffic-snippet\_7.cap pambot-traffic-snippet\_8.cap pambot-traffic-snippet\_9.cap pambot-traffic-snippet\_10.cap pambot-traffic-snippet\_11.cap pambot-traffic-snippet\_12.cap pambot-traffic-snippet\_13.cap pambot-traffic-snippet\_14.cap pambot-traffic-snippet\_15.cap pambot-traffic-snippet\_16.cap pambot-traffic-snippet\_17.cap

#### 2: Operate against each flow individually 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_20221017-143616.txt 2022-02-25-Emotet-epoch5-spambot-traffic-snippet.pcap Average beteen queries: 14135.07467057101 Total Queries: 1367 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_15.cap Average beteen queries: 8049.0 Total Queries: 3 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_14.cap Average beteen queries: 73373.6 Total Queries: 11 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_16.cap Average beteen queries: 133663.0588235294 Total Queries: 18 6 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_17.cap Total Queries: 25 2022-02-25-Emotet-epoch5-spambot-traffic-snippet\_13.cap Average beteen queries: 59165.142857142855 Total Queries: 36 DEEPSEC



## Calculate Percentages

	Time		Source	Destination	Protocol	Length   Info					
1	2022-03-29	07:17:49.109583	10.3.29.101	104.161.127.22	HTTP	500 GET	/wp-con	tent/Elw3k	PvOsZxM5/	HTTP/1.1	1
2	2022-03-29	07:17:49.313841	104.161.127.22	10.3.29.101	ТСР	1415 80 -	→ 563 <b>09</b>	[PSH, ACK]	Seq=1 Acl	k=447 Wir	n=6
3	2022-03-29	07:17:49.313918	104.161.127.22	10.3.29.101	TCP	1415 80 -	→ 563 <b>09</b>	[PSH, ACK]	Seq=1362	Ack=447	Wi
4	2022-03-29	07:17:49.314270	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ <b>56309</b>	[PSH, ACK]	Seq=2723	Ack=447	Wi
5	2022-03-29	07:17:49.314494	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ <b>56309</b>	[PSH, ACK]	Seq=4084	Ack=447	Wi
6	2022-03-29	07:17:49.314711	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=5445	Ack=447	Wi
7	2022-03-29	07:17:49.314939	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=6806	Ack=447	Wi
8	2022-03-29	07:17:49.315151	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=8167	Ack=447	Wi
9	2022-03-29	07:17:49.315647	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=9528	Ack=447	Wi
10	2022-03-29	07:17:49.315893	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=10889	9 Ack=447	7 W
11	2022-03-29	07:17:49.316113	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=12250	0 Ack=447	7 W
12	2022-03-29	07:17:49.431163	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=13613	L Ack=447	7 W
13	2022-03-29	07:17:49.431384	104.161.127.22	10.3.29.101	ТСР	1415 80 ·	→ 56309	[PSH, ACK]	Seq=14972	2 Ack=447	7 W
14	2022-03-29	07:17:49.431724	104.161.127.22	10.3.29.101	TCP	1415 80	→ 56309	[PSH, ACK]	Seq=16333	3 Ack=447	7 W
15	2022-03-29	07:17:49.431975	104.161.127.22	10.3.29.101	TCP	1415 80	→ 56309	[PSH, ACK]	Seq=17694	4 Ack=447	7 W
16	2022_03_20	07.17.10 111210	104 161 127 22	10 2 20 101	TCP	1/115 80	56300	IDSH ACKI	Sen-1005	Ack-447	7 h

501			10101201101	101	1110 0			Hent	ocq ooroo	Hen LLI	111 01210	2011 1001	
568	2022-03-29 07:18:34.204988	74.124.193.14	10.3.29.101	ТСР	1415 8	30 → 56321	[PSH,	ACK]	Seq=583870	Ack=214	Win=64240	Len=1361	[TCF
569	2022-03-29 07:18:34.206474	74.124.193.14	10.3.29.101	ТСР	1415 8	30 → 56321	[PSH,	ACK]	Seq=585231	Ack=214	Win=64240	Len=1361	[TCF
570	2022-03-29 07:18:34.206708	74.124.193.14	10.3.29.101	ТСР	1415 8	30 → 56321	[PSH,	ACK]	Seq=586592	Ack=214	Win=64240	Len=1361	[TCF
571	2022-03-29 07:18:34.206929	74.124.193.14	10.3.29.101	ТСР	1415 8	30 → 56321	[PSH,	ACK]	Seq=587953	Ack=214	Win=64240	Len=1361	[TCF
572	2022-03-29 07:18:34.207125	74.124.193.14	10.3.29.101	HTTP	1117 F	HTTP/1.1 2	:00 OK	(app	lication/x-r	nsdownloa	ad)		

**Notes for the Viewer:** lot of 0 time in between traffic. Not super useful. One PCAP has 572 packets

#### **DEEPSEC**

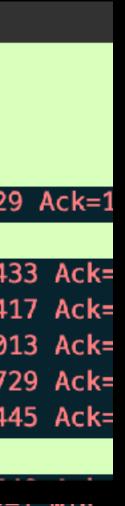
### network traffic is not all the same. Here, I'm looking at two PCAPs. A lot more transactions in one. Also a

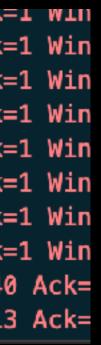




1	2022-04-20	14:33:18.628513	10.4.20.102	107.161.178.210	HTTP	279 GET /video/6JvA8/ HTTP/1.1
2	2022-04-20	14:33:59.595290	10.4.20.102	49.231.16.102	ТСР	1434 54331 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=1380
3	2022-04-20	14:33:59.595358	10.4.20.102	49.231.16.102	ТСР	1434 54331 → 8080 [ACK] Seq=1381 Ack=1 Win=1024 Len=1380
4	2022-04-20	14:33:59.595430	10.4.20.102	49.231.16.102	ТСР	926 54331 → 8080 [PSH, ACK] Seq=2761 Ack=1 Win=1024 Len=872
5	2022-04-20	14:37:57.405290	10.4.20.102	176.31.163.17	ТСР	1442 54360 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=1388
6	2022-04-20	14:37:57.552709	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=8329
7	2022-04-20	14:37:57.552873	10.4.20.102	176.31.163.17	ТСР	1442 54360 → 8080 [PSH, ACK] Seq=9717 Ack=1 Win=1024 Len=1388
8	2022-04-20	14:37:57.559324	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=1943
9	2022-04-20	14:37:57.701945	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=4441
10	2022-04-20	14:37:57.708372	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=6801
11	2022-04-20	14:37:57.713906	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=7772
12	2022-04-20	14:37:57.714774	10.4.20.102	176.31.163.17	ТСР	1442 [TCP Previous segment not captured] 54360 → 8080 [ACK] Seq=8744
13	2022-04-20	14:37:57.714847	10.4.20.102	176.31.163.17	ТСР	1442 54360 → 8080 [ACK] Seq=88833 Ack=1 Win=1024 Len=1388
43	2022-04-20	13:13:30.193343	42.22.02.200	.0.4.20.102		1442 [ICF Frevious segment not captured] 0000 → 04000 [ACK] Seq=244000 ACK=
		15:13:38.200169		0.4.20.102		1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=257300 Ack=
45	2022-04-20	15:13:38.269912	45.55.63.166 1	0.4.20.102		1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=265385 Ack=
46	2022-04-20	15:13:38.302228	45.55.63.166 1	0.4.20.102		1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=273713 Ack=
47	2022-04-20	15:13:38.366600	45.55.63.166 1	0.4.20.102		1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=279022 Ack=3
48	2022-04-20	15:13:38.367030	45.55.63.166 1	.0.4.20.102	тср :	1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=284574 Ack=
49	2022-04-20	15:13:38.436687	45.55.63.166 1	0.4.20.102	тср :	1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=298211 Ack=
50	2022-04-20	15:13:38.450193	45.55.63.166 1	0.4.20.102	тср 🛛	1442 [TCP Previous segment not captured] 8080 → 54383 [ACK] Seq=303763 Ack=3
51	2022-04-20	15:13:38.524592	45.55.63.166 1	.0.4.20.102	тср :	1199 [TCP Previous segment not captured] 8080 → 54383 [PSH, ACK] Seq=324340
52	2022-04-20	15:13:38.552988	45.55.63.166 1	0.4.20.102	ТСР	1137 [TCP Previous segment not captured] 8080 → 54383 [PSH, ACK] Seq=333813

Notes for the Viewer: The other PCAP has 52 packets





#### 992316552291476588

pyorre@scavpn-056 extractflows % python3 signature\_generation.py epoch4/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_http.pcap 0, 0,

Notes for the Viewer:

Here, I'm looking at two PCAPs. A lot more transactions in one. Also a lot of 0 time in between traffic. Not super useful.

	-	-	1	
0,	Ø,	Ø,	0,	0,
0,	Ø,	0,	0,	0,
0,	0,	0,	0,	0,
0,	0,	0,	0,	0,
Ø,	0,	Ø,	0,	0,
Ø,	0,	Ø,	Ø,	Ø,
Ø,	0,	Ø,	0e,×	Ø,
ø,	ø,	ø,	0,	ø,
0,	Ø,	ø,	Ø,	0,
0,	0,	Ø,	0,	0,
0,	0,	Ø,	0,	0,
Ø,	0,	Ø,	Ø,	0,
Ø,	Ø,	Ø,	Ø,	Ø,
Ø,	0,	Ø,	Ø,	0,
Ø,	1,	Ø,	2022	0,
0,	Ø,	Ø,	0,	0,
0,	Ø,	0,	0,	0,
0,	0,	0,	0,	0,
ø,	0,	ø,	0,	ø,
ø,	ø,	ø,	ø,	ø,
ø,	Ø,	ø,	ø,	0,
ø,	Ø,	Ø,	ø,	ø,
ø,	ø,	ø,	ø,	0,
0,	ø,	ø,	0,	0,
0,	0,		0,	
ø,	0,	ø,	ø,	ø,
ø,	0,			
ø,	0,			
ø,	ø,	ø,	Ø,	



#### 992316552291476588

pyorre@scavpn-056 extractflows % python3 signature\_generation.py epoch4/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_http.pcap 0, 0,

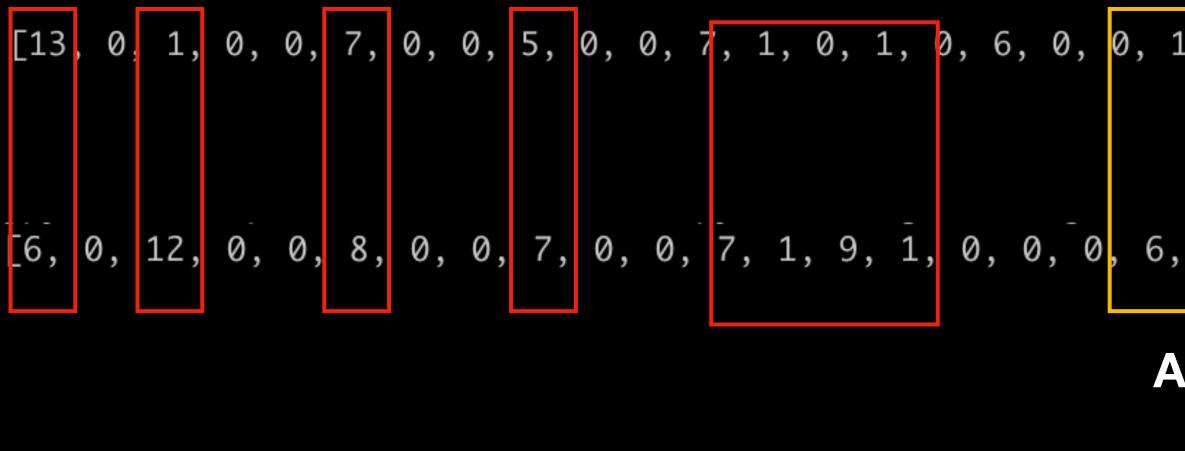
Notes for the Viewer:

Here, I'm looking at two PCAPs. A lot more transactions in one. Also a lot of 0 time in between traffic. Not super useful.

	-	-	1	
0,	Ø,	Ø,	0,	0,
0,	Ø,	0,	0,	0,
0,	0,	0,	0,	0,
0,	0,	0,	0,	0,
Ø,	0,	Ø,	0,	0,
Ø,	0,	Ø,	Ø,	Ø,
Ø,	0,	Ø,	0e,×	Ø,
ø,	ø,	ø,	0,	ø,
0,	Ø,	ø,	Ø,	0,
0,	0,	Ø,	0,	0,
0,	0,	Ø,	0,	0,
Ø,	0,	Ø,	Ø,	0,
Ø,	Ø,	Ø,	Ø,	Ø,
Ø,	0,	Ø,	Ø,	0,
Ø,	1,	Ø,	2022	0,
0,	Ø,	Ø,	0,	0,
0,	Ø,	0,	0,	0,
0,	0,	0,	0,	0,
ø,	0,	ø,	0,	ø,
ø,	ø,	ø,	ø,	ø,
ø,	Ø,	ø,	ø,	0,
ø,	Ø,	Ø,	ø,	ø,
ø,	ø,	ø,	ø,	0,
0,	ø,	ø,	0,	0,
0,	0,		0,	
ø,	0,	ø,	ø,	ø,
ø,	0,			
ø,	0,			
ø,	ø,	ø,	Ø,	



#### Similar traffic Times

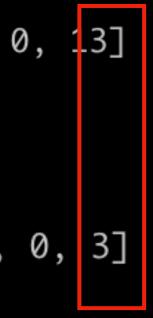


#### **Notes for the Viewer:**

One interesting thing in these percentages of the time in between packets as they relate to the total time of the whole flow is that they are fairly similar, despite being different. Maybe it's because this is SSL and it's just following the pattern of SSL traffic, which might be similar no matter what kind of flow it's on.

#### DEEPSEC

#### Similar traffic Times





## Acc a Itte chaos

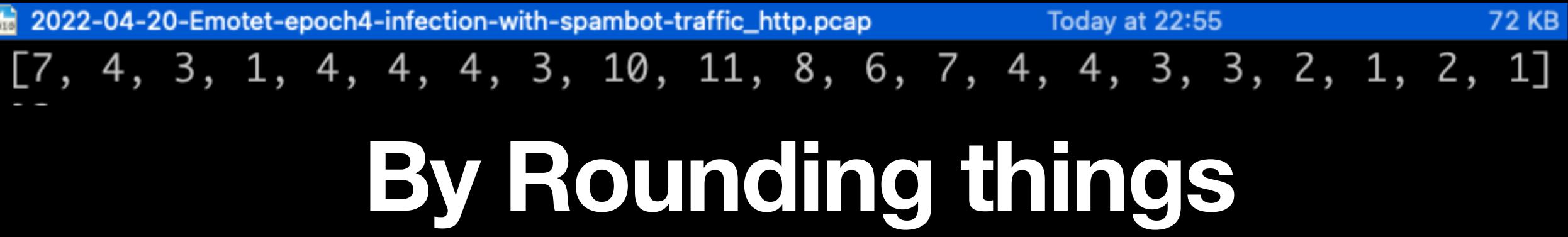
2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_http.pcap

[16, 14, 2, 2, 2, 2, 8, 5, 2, 10,

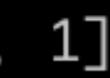
2022-04-20-Emotet-epoch4-infection-with-spambot-traffic\_http.pcap

**Notes for the Viewer:** I want to work with integers, not floats because I want the comparison to be a little 'looser' - so I'm converting to ints and rounding them.

р		Today at 22:53									
5,	5,	9,	1,	1,	2,	3,	3,	1,	1,	1,	1,







### 2022-07-07-Emotet-infection-with-Cobalt-Strike:

emotet20220707/1\_emotet\_get/1\_emotet\_get.pca Percent of each time in between toward the

emotet20220707/2\_emotet\_c2/2\_emotet\_c2.pcap
Percent of each time in between toward the

emotet20220707/3\_cobaltstriketraffic/3
Percent of each time in between toward

Notes for the Viewer: They are sometimes just below or above 100, but that's because I round them.

ap: total:	[2,	46,	2, 3	1,	12,	з,	4,	1,	13,	з,	5,	2]
p: total:	[2,	16,	1,	6,	2,	1,	1,	1,	2,	1,	з,	38]
/3_coba rd the									19	, 1	9,	2]

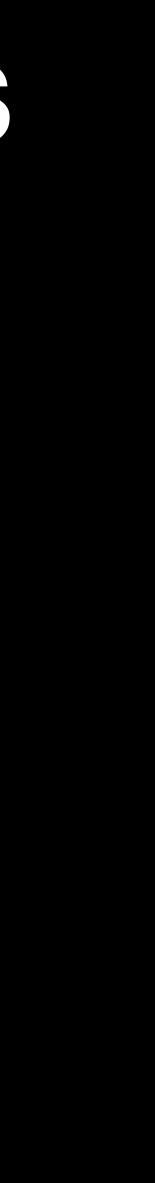


## Now we can find exact matches



## **DEEPSEC** Which isn't really Useful



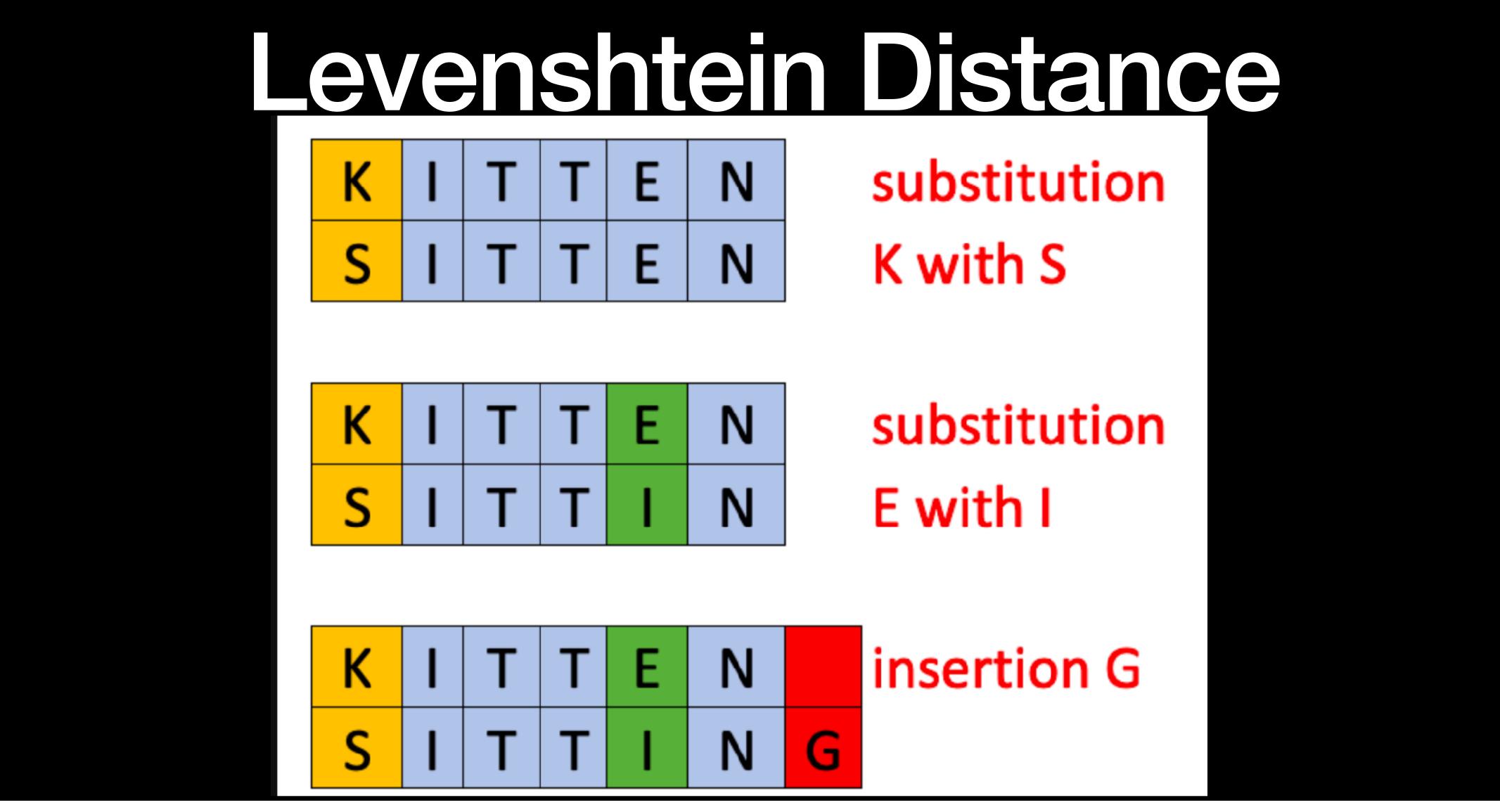


## Percentages and Distance

## Levenshtein Distance

**Notes for the Viewer:** I need my search to be even more 'loose'/less precise. So now I'm exploring Levenshtein Distance. This is typically used for word searches.



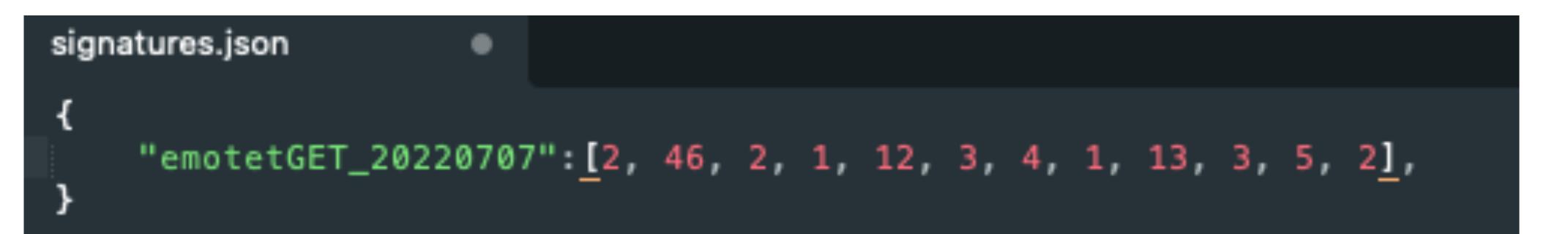


**Notes for the Viewer:** Levenshtein Distance is typically used for word searches - how many changes between two words shows how close they are.



### GET REQUESTS

emotet20220707/1\_emotet\_get/1\_emotet\_get.pcap:



**Notes for the Viewer:** a text file to be read by the test\_signature script

#### DEEPSEC

### Percent of each time in between toward the total: [2, 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]

#### Before applying Levenshtein Distance, let's make a static signature. Start by putting the percentages into



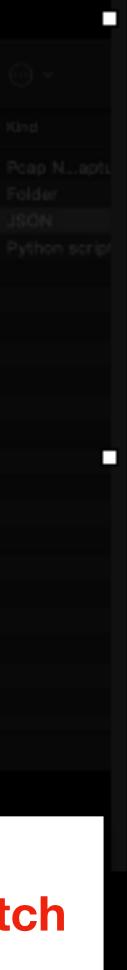
### Check Signature Against the PCAP it was created from

jpyorre@Joshs-MacBook-Pro test\_signatures % python3 test\_signature.py 1\_emotet\_ge t.pcap [{'filename': 'flowoutputs/1\_emotet\_get\_0.cap', 'percent of times in between': [2 , 46, 2, 1, 12, 3, 4, 1, 13, 3, 5, 2]ratio: flowoutputs/1\_emotet\_get\_0.cap: emotetGET\_20220707, 100 partial\_ratio: flowoutputs/1\_emotet\_get\_0.cap: emotetGET\_20220707, 100 jpyorre@Joshs-MacBook-Pro test\_signatures %

**Notes for the Viewer:** of percentage signature to percentages in a PCAP.



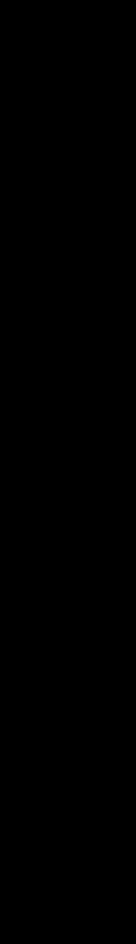
### Still from a video showing the process of detecting an exact match (no Levenshtein - just a perfect match



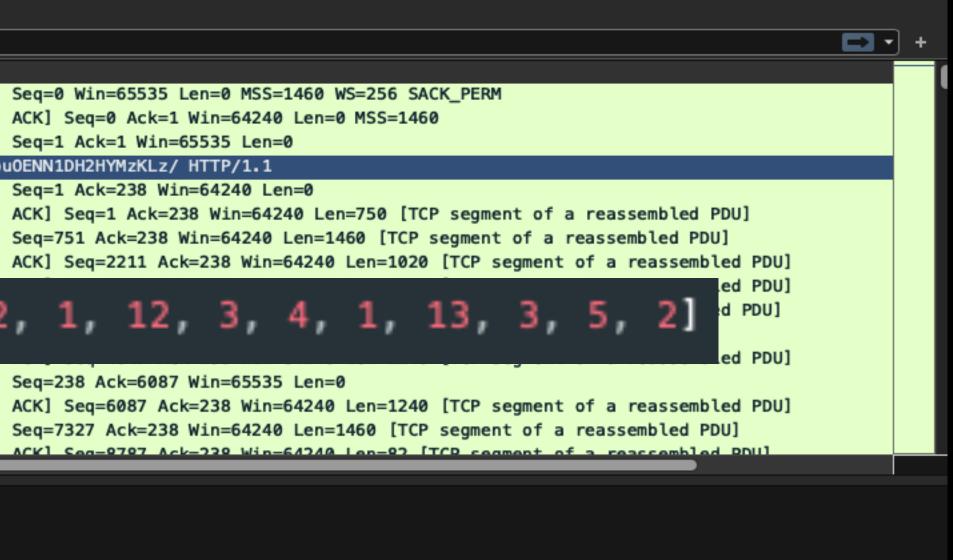
## What about a similar bad PCAP?

Notes for the Viewer: We need to try it on something that is not exactly the same.





						1_	_emotet_get.pc	ap						
<b>a</b> 🔳 🔊	( 🞯 📄 💼 🛿	2 👩 🔇	2 (= =)	🖮 🗛 🧶 📃	Ð.	ର୍ବ୍								
	ay filter <೫/>												+	
lo.	Time		Source	Destination	Pro	tocol  Lengt	r∣Info							
-	1 2022-07-07 11:18			193.53.245	.52 TC	P 66	6 57305 → 80			535 Len=0 MSS=1460 WS	_			
	2 2022-07-07 11:18							-		ck=1 Win=64240 Len=0	MSS=1460			
	3 2022-07-07 11:18 4 2022-07-07 11:18			193.53.245 193.53.245						Win=65535 Len=0 KLz/ HTTP/1.1				
	5 2022-07-07 11:18									8 Win=64240 Len=0				
	6 2022-07-	<b>•</b>				P 804			-		=750 [TCP segment of a reassemb			
	7 2022-07- 8 2022-07-	ir Si	dna	ure P	CAP	P 1514					60 [TCP segment of a reassemble			
	9 2022-07-										Len=1020 [TCP segment of a reas	ed PDU1		
1	10 2022-07-07 11:19	9:00.454899	193.53 <sup>11</sup> em	otetGET	202207	07" · I	2 46	2	1 1	2 3 4	1, 13, 3, 5, 2	] d PDU]		
-			10171		202207	· · ·	.2, 40	, -,	-, -		-, -3, 3, 3, .			
	12 2022-07-07 11:19			102 52 245	F2 TC	D E4	67205 00	[ACK] Com	-220 Ack-4	6007 Win-65525 Lon-0		ed PDU]		
	13 2022-07-07 11:19 14 2022-07-07 11:19			193.53.245 10.7.7.101						6087 Win=65535 Len=0 7 Ack=238 Win=64240 L	Len=1240 [TCP segment of a reas	sembled PDUl		
	15 2022-07-07 11:19							-			460 [TCP segment of a reassembl			
	16 2022_07_07 11.10	0.00 155750	102 52 245 5	10 7 7 101	TC	D 126	5 00 . 57205		1 500-070	7 Ack-220 Win-61210 1	on-92 [TCP commont of a reason	mbled PDU1		
> Frame 4: 29	91 bytes on wire (2	328 bits 00	00 00 04 4d	11 a7 08 a0 a8 cd	58 ad 6c 08	00 45 00	···M····· · X·	1E.						
	I, Src: IntelCor_58	ad:6c ( 00	10 01 15 f2	e2 40 00 80 06 3f	2a 0a 07 07	65 c1 35		• · e · 5						
	rotocol Version 4,	S 10 00	20 f5 34 df	d9 00 50 b6 61 b7 31 00 00 47 45 54	33 bf 8b 8a 3 20 2f 73 79	32 50 18 73 74 65	4 Pa 3							
	on Control Protocol	, Sra Pr		51 00 00 47 45 54	20 21 73 73	574 65	1 32 1 /	-	08-08 exe	_download-IcedID-with-(	Cobalt-Strike.pcap			
> Hypertext 1	Transfer Protocol									—				
			🛛 🖉	🚞 🛍 🛍	् ५ 🗢 🏻	) 👱 🤇	) ⊻ 🔜			₹.				
		📕 Apply a	ı display filter <	¥(>										
		No.	Time		Source		Destination		Protocol	Length Info				
		Г		08-08 14:27:00.681			104.238.220		ТСР		N] Seq=0 Win=64240 Len=0 MSS=14	_		
				08-08 14:27:00.740 08-08 14:27:00.740			10.8.8.101		ТСР ТСР		N, ACK] Seq=0 Ack=1 Win=64240 L K] Seq=1 Ack=1 Win=64240 Len=0			
		- <b> </b> +		08-08 14:27:00.740			104.238.220		HTTP	135 GET /download/s	-			
				08-08 14:27:00.740			10.8.8.101		тср		K] Seq=1 Ack=82 Win=64240 Len=0	0		
				08-08 14:27:00.803			10.8.8.101		ТСР		H, ACK] Seq=1 Ack=82 Win=64240	_		
				08-08 14:27:00.806 08-08 14:27:00.806			10.8.8.101		ТСР ТСР		H, ACK] Seq=221 Ack=82 Win=6424 K] Seq=82 Ack=1609 Win=64240 Le		tofa	reassembled PDU]
				08-08 14:27:00.810			104.250.220	0.131	TCF	54 50402 - 00 [ACI		240 Len=1388 [TCP segme	nt of a	reassembled PDU]
				08-08 14:27:00.813				. <b>C</b>						
				08-08 14:27:00.813		1	Our	JU	1501	cious i	PCAP Ack=82 Win=642 5 Win=64240 Le	en=0		
				08-08 14:27:00.816 08-08 14:27:00.827		20.131	10.8.8.101		тср		ACK=82 W1N=644	240 Len=1388 [ICP segme	пт от а	a reassembled PDU]
				08-08 14:27:00.827			104.238.220		ТСР		H, ACK] Seq=5773 Ack=82 Win=642 K] Seq=82 Ack=7161 Win=64240 Le	_	int or a	reassembled PD0]
				08-08 14:27:00.827			10.8.8.101		ТСР		H, ACK] Seq=7161 Ack=82 Win=642		nt of a	reassembled PDU]
			16 2022-	<u>00_00 11.77.00 021</u>	602 104 220 2	20 121	10 0 0 101		TCP	1442 80 . 50462 [DS	H ACK1 Sec-9540 Ack-92 Win-641	240 Lon-1200 [TCP coame	nt of a	reascembled PDU1
		> Frame	4: 135 bvtes	on wire (1080 bit:	0000 <b>20 e5</b>	2a b6 93 1	f1 00 08 02	1c 47 ae	08 00 45 (	00 ·*····G···E	Ε.			
				HewlettP_1c:47:ae	0010 <b>00 79</b>	52 0a 40 0	00 80 06 50	96 0a 08 (	08 65 68 0	ee ∘yR∘@···P···eh				
				Version 4, Src: 10	0030 fa f0		50 c9 d2 cb 00 47 45 54							
				ol Protocol, Src Po	0040 6f 61	64 2f 73 7	79732e 65	78 65 20 4	48 54 54 !	50 oad/sys.exe HTT				
		/ hyper	text Transfer	Protocot			0a 43 6f 6e 70 2d 41 6c							
					0070 73 74	3a 20 31 3	30 34 2e 32			2e st: 104. 238.220				
					0080 31 33	31 0d 0a (	od va			131				
	PSEC													





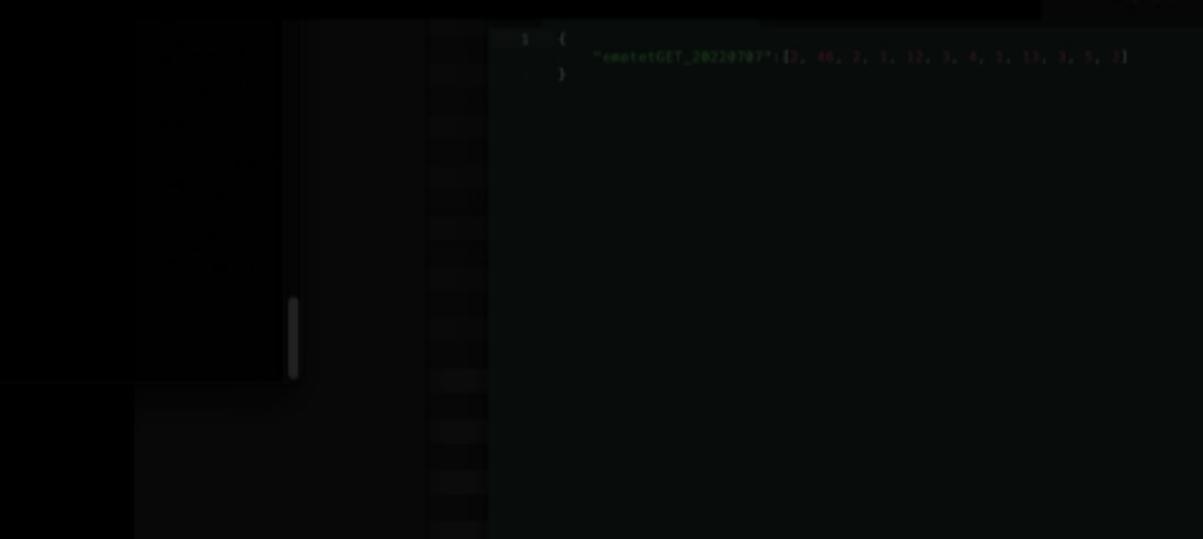


### **Check Signature Against similar bad PCAP**

{'filename': 'flowoutputs/2022-08-08\_exe\_download-IcedID-with-Cobalt-Strike\_0.cap', 'percent of times in betw n': [3, 4, 1, 2, 1, 2, 2, 1, 1, 1, 1, 8, 1, 1, 1, 2, 1, 1, 2, 2, 1, 8, 3, 3, 3, 1, 1, 1, 1, 4, 1]}] atio: flowoutputs/2022-08-08\_exe\_download-IcedID-with-Cobalt-Strike\_0.cap: emotetGET\_20220707, 47 artial\_ratio: flowoutputs/2022-08-08\_exe\_download-IcedID-with-Cobalt-Strike\_0.cap: emotetGET\_20220707, 7 4 pyorre@Joshs-MacBook-Pro test\_signatures %

**Notes for the Viewer:** Still from a video of signature and using Levenshtein Distance to compare two similar PCAPs. The percentages are different, but we have a partial ratio that is somewhat close, suggesting a relationship.





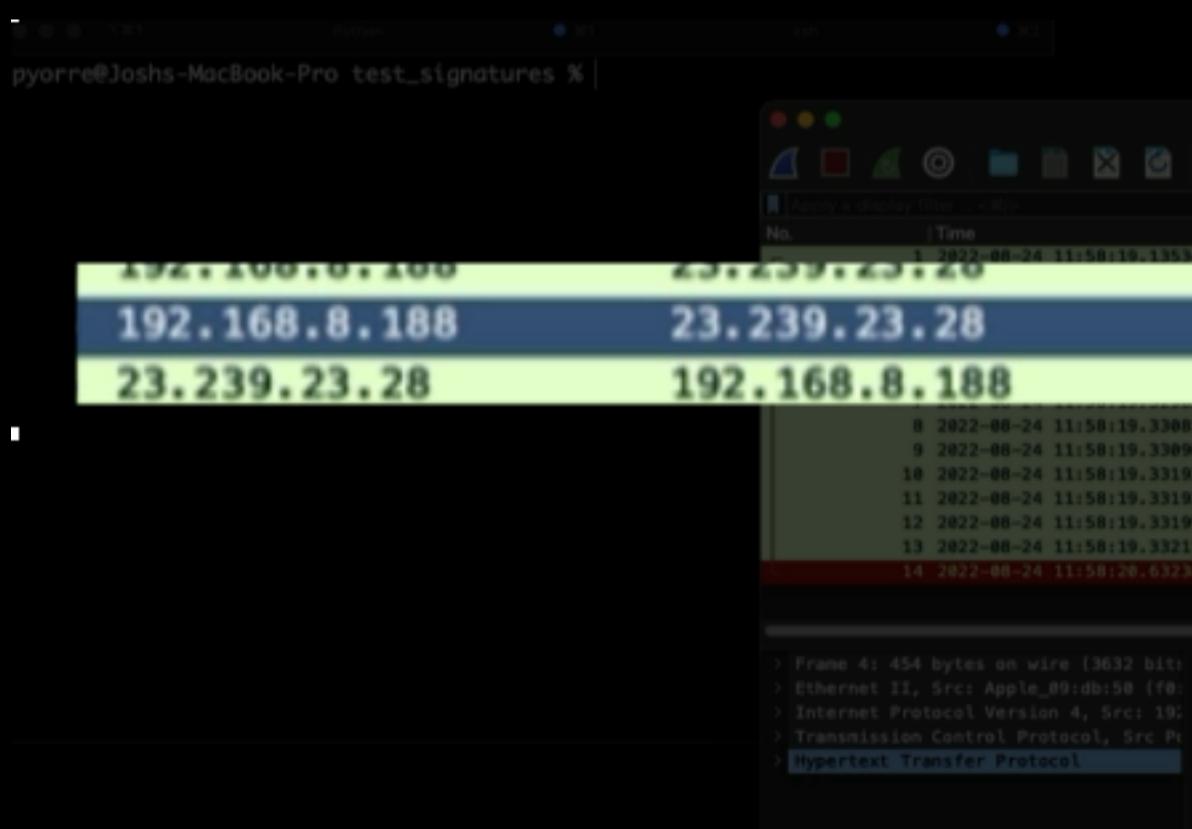




# What about a similar benign PCAP?



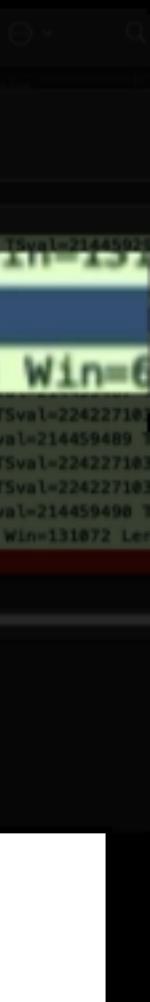
### Check Signature Against similar benign PCAP



#### Notes for the Viewer: Using a benign .exe download that is designed to look like a malware dropper



_							
TCP	0 23.23	99, 22	270	- 00	INCK!	26d-y	ACK-1 W
нттр	4	54 GE	Τ/	existe	ntial	.exe H	TTP/1.1
TCP		54 80	) -  5	55278	[ACK]	Seq=1	Ack=389
817       23.239.23.28         965       192.168.8.18         933       23.239.23.28         935       23.239.23.28         935       102.168.8.18         112       192.168.8.18         383       23.239.23.28	8 23.23 192.10 192.10 8 23.23 8 23.23	68.8.188 9.23.28 68.8.188 68.8.188 9.23.28 9.23.28 9.23.28	TCP TCP TCP TCP TCP TCP	1514 80 → 1 66 55278 1514 80 → 1 1514 80 → 1 66 55278 66 [TCP 1	→ 88 [ACK] Se → 88 [ACK] Se 55278 [ACK] Se 55278 [ACK] Se → 88 [ACK] Se vindow Update]	eq=1449 Ack=389 eq=389 Ack=2897 eq=2897 Ack=389 eq=4345 Ack=389 eq=389 Ack=5793	Win=64896 Len=1448 TS Win=129680 Len=0 TSva Win=64896 Len=1448 TS Win=64896 Len=1448 TS Win=128128 Len=0 TSva X] Seq=389 Ack=5793 W
	18 d6 06 f0 24 00 40 00 40 06 ee 00 50 33 e8 01 00 00 01 03 45 54 20 2f 65 65 78 65 20 40 73 74 3a 20 73 6e 65 74 0d 04 20 4d 6f 7a 65						

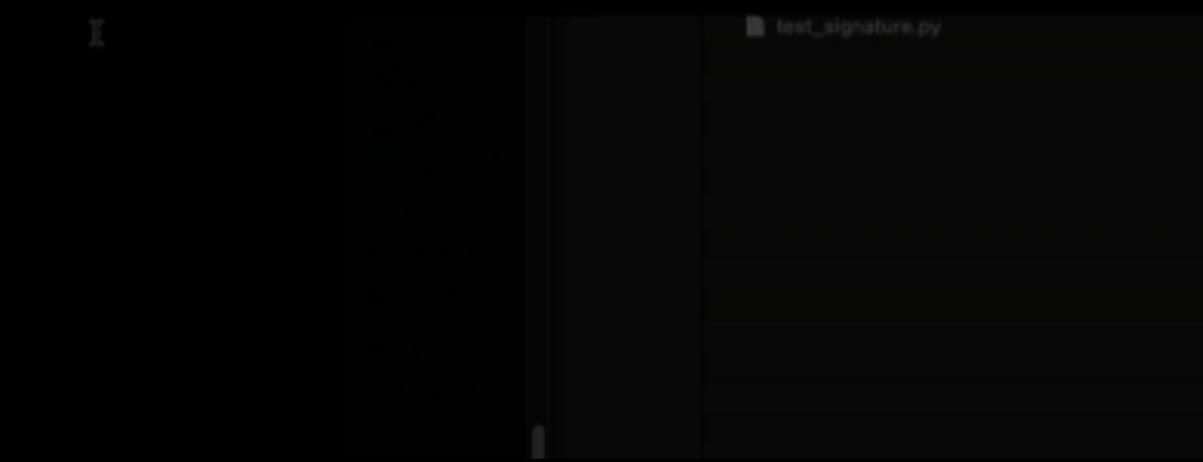


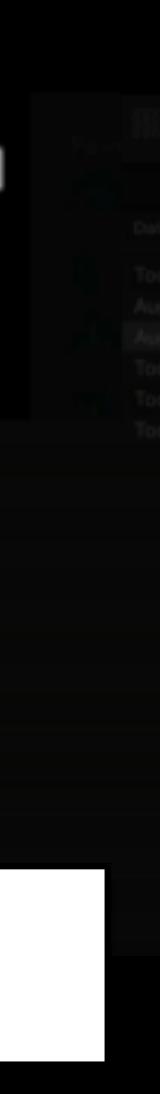
### Check Signature Against similar benign PCAP

pyorre@Joshs-MacBook-Pro test\_signatures % python3 test\_signature.py benign\_exe\_download.pcap {'filename': 'flowoutputs/benign\_exe\_download\_0.cap', 'percent of times in between': [10, 1, 28]}] atio: flowoutputs/benign\_exe\_download\_0.cap: emotetGET\_20220707, 36 artial\_ratio: flowoutputs/benign\_exe\_download\_0.cap: emotetGET\_20220707, <mark>57</mark> pyorre@Joshs-MacBook-Pro test\_signatures % |

Notes for the Viewer: It doesn't match too well to the emotet dropper download, which is good!









Multiple Flows in a PCAP

yorre@Joshs-MacBook-Pro test\_signatures % |

••												20	22-03	-20-6	motet-4	ipoch4	-with-(	Cobalt-	Strike_	http.pcap									
1		0	1.00	100	<b>D R</b>			-		<u>х</u> л				9															
		9		m v l		2	、 ~	~		r y	-				S. 1														
Αρρί																													
No.		Tin	ne				Source			Dest	ination		P)	otocol	Length	t Info													
		1 20	22-83-2	9 07:1	7:49.1	189583	10.3.25	1.101		104.	161.12	7.22	H	TTP	5.88	GET	/wp-co	intent/	Elw3k	Pv0sZxM5/	HTTP/1	1							
		2 28	22-83-2	9 87:1	7:49.3	313841	104.161	1.127.7	22	10.3	3.29.18	1	T	CP	1415	i 80 →	56389	[PSH,	ACK]	Seq=1 Ac	k=447 M	n=64248	Len=136	51 [TC	P segn	ent of	fare	assembl	ed PDU)
		3 20	22-83-2	9 87:1	7:49.3	313918	104.161	1.127.7	22	10.3	3.29.18	1	T	CP	1415	i 80 -	56389	[PSH,	ACK]	Seq=1363	Ack=447	Min=642	48 Len-	=1361	[TCP :	segment	t of a	reasse	mbled PDU
		4 28	22-83-2	9 87:1	7:49.3	314278	104.161	1.127.7	22	10.3	3.29.18	1	T	CP	1415	i 80 →	56389	[PSH,	ACK]	Seq=2723	Ack=447	Min=642	48 Len	=1361	[TCP 1	segment	t of a	reasse	mbled PDU
		5 28	22-83-2	9 87:1	7:49.3	314494	104.161	1.127.2	22	10.3	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=4884	Ack=44	Min=642	48 Len	=1361	[TCP 1	segment	tofa	reasse	mbled PDU
		6 28	22-83-2	9 87:1	7:49.3	314711	104.161	1.127.3	22	10.3	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=5445	Ack=44	Min=642	40 Len	=1361	[TCP 1	egment	t of a	reasse	mbled PDU
		7 28	22-83-2	9 87:1	7:49.3	314939	104.163	1.127.3	22	10.3	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=6886	Ack=44	Min=642	40 Len	=1361	[TCP 1	egment	t of a	reasse	mbled PDU
		8 28	22-83-2	9 87:1	7:49.3	315151	104.163	1.127.3	22	10.3	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=8167	Ack=44	Min=642	40 Len	=1361	[TCP 1	egment	t of a	reasse	mbled PDU
		9 28	22-83-2	9 07:1	7:49.3	315647	104.167	1.127.7	22	10.3	8.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=9526	Ack=44	Win=642	40 Len	=1361	[TCP 1	egment	t of a	reasse	mbled PDU
	1	0 20	22-83-2	9 07:1	7:49.3	315893	104.167	1.127.7	22	10.3	8.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=1088	9 Ack=4/	7 Win=64	240 Ler	n=1361	[TCP	segner	nt of a	a reass	embled PD
	1	1 20	22-83-2	9 07:1	7:49.3	316113	104.167	1.127.7	22	10.7	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=1225	8 Ack=4/	7 Win=64	240 Ler	n=1361	[TCP	segner	it of a	a reass	embled PD
	1	2 20	22-83-2	9 07:1	7:49.4	431163	104.167	1.127.7	22	10.7	3.29.18	1	T	CP															embled PD
	1	3 20	22-83-2	9 07:1	7:49.4	431384	104.167	1.127.7	22	10.7	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=1497	2 Ack=4/	7 Win=64	240 Ler	n=1361	[TCP	segner	it of a	a reass	embled PD
	1	4 20	22-83-2	9 07:1	7:49.4	431724	104.167	1.127.7	22	10.7	3.29.18	1	T	CP	1415	80 -	56389	[PSH,	ACK]	Seq=1633	3 Ack=4/	7 Win=64	240 Ler	n=1361	[TCP	segner	it of a	n reass	embled PD
	1	5 20	22-83-2	9 87:1	7:49.4	431975	104.167	.127.7	22	10.7	3.29.18	1	T	CP	1415	i 80 -	56389	(PSH,	ACK]	Seq=1765	4 Ack=4/	17 Win=64	248 Ler	n=1361	[TCP	segner	it of a	a reass	embled PD
> Fra	me 1: 50	ið byt	tes on v	wire (+	1888 b	111 00	00 20	e5 2a	b6 93	f1 00	08 02	16 47 4	se 88	ee 45	00			G···E·											
> Eth	ernet II	, Sre	: Hewl	ettP_1	:47:0							19 0a 0																	
> Int	ernet Pr	otace	al Vers	ion 4,	Sre: :							30 2e 0 20 2f 7					Pow 0												
> Tra	nsmissio	in Car	strol P	rotoco	l, Src	PI						33 6b 5						/wp-co ikPv0sZ											
> Hyp	ertext T	rans!	fer Pro	tocol		00						2f 31 2						1.1											
							68 61	73 74	3a 20	66 6b	6c 2e	63 6f 2	2e 6b	65 Ød	0a	esti	fkl.c	o.ke··											
												6e 3a 2						: keep											
												70 67 7						grade-											
						00						52 65 7 72 2d 4						equest -Agent											
												21 35 2						5.0 (1											

#### **Notes for the Viewer:** Running a PCAP containing a GET request for an Emotet dropper to a compromised wordpress account.

03 78 74 21 08 74 00 DC 2C 01 78 78 0C 09 03 01 ext/html ,applica

	< > test_signal	tures E
AirDrop	Name	
	📑 1_emotet_get.pcap	
	2022-03-29-Emote	t-epocith-Cobalt-Strike,
	> flowoutputs	



		Dut
		Yes
_http.pc	ap.	Oe
		Too

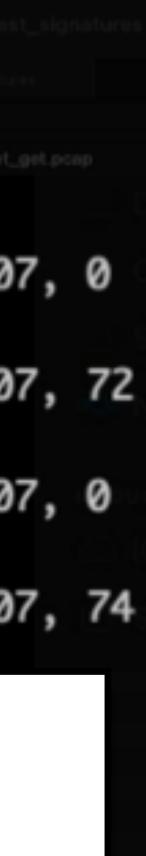


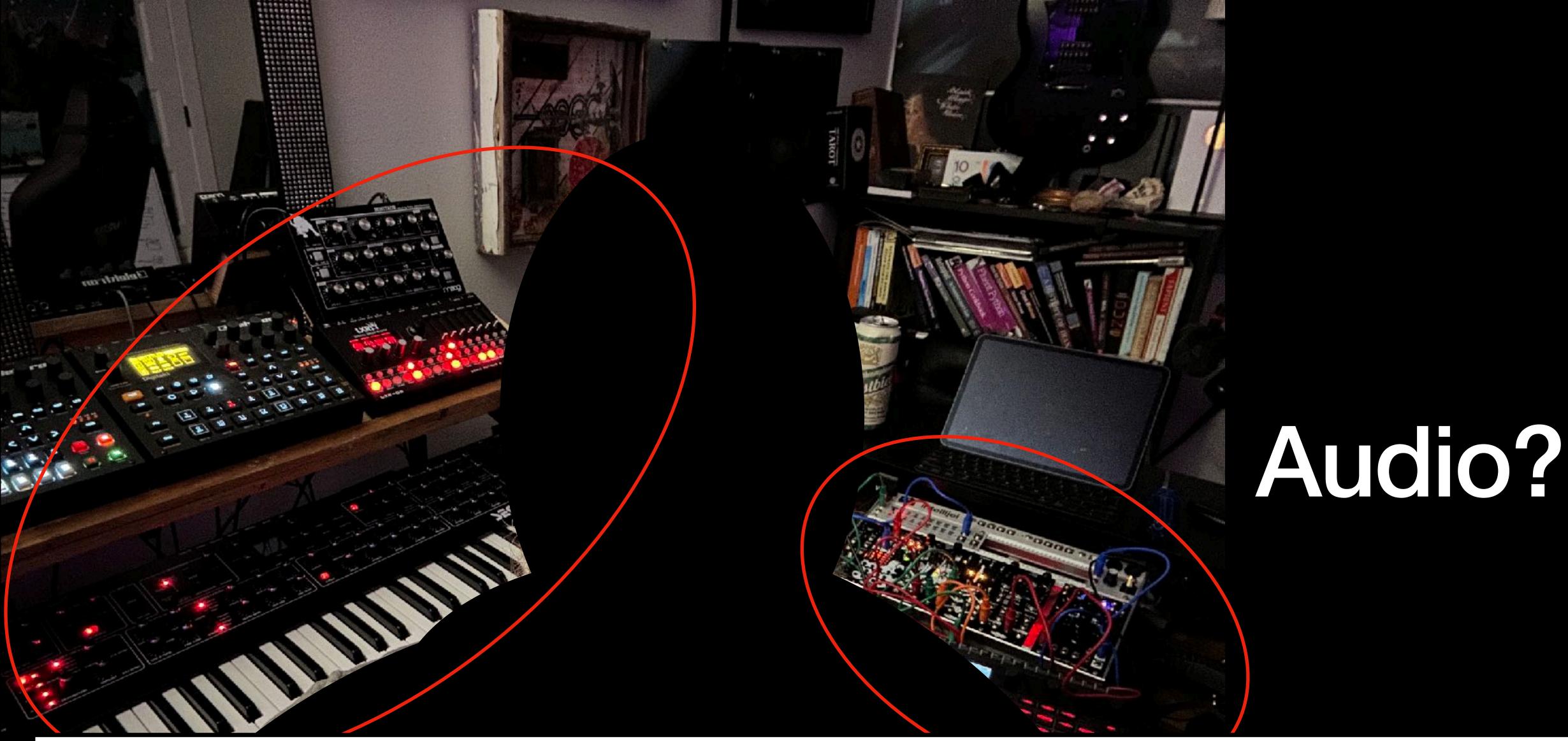


ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_1.cap: emotetGET\_20220707, 0 partial\_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_1.cap: emotetGET\_20220707, 0 ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_0.cap: emotetGET\_20220707, 68 partial\_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_0.cap: emotetGET\_20220707, 72 ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt[2.cap: emotetGET\_20220707, 0 partial\_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_2.cap: emotetGET\_20220707, 0 ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_3.cap: emotetGET\_20220707, 67 partial\_ratio: flowoutputs/2022-03-29-Emotet-epoch4-with-Cobalt-Strike\_htt\_3.cap: emotetGET\_20220707, 74 invorre@loshs\_MacRook\_Pro test signatures %

**Notes for the Viewer:** 

Each flow is separated from the PCAP and the signature is run against them, one at a time. Higher matches are shown. The PCAPs with partial ratios of 72 and 74 are a match for Emotet Dropper downloads





**Notes for the Viewer:** 

This image shows that music is another thing I do, and security is a creative process. Just to think outside the box, can we convert time to audio and use something to identify it, much like the app 'Shazam' is used to identify a song by listening to part of it?





 $\rightarrow$  C

⊠ ±

# **Audio Fingerprinting** with Python and Numpy

### November 15, 2013

The first day I tried out Shazam, I was blown away. Next to GPS and surviving the fall down a flight of stairs, being able to recognize a song from a vast corpus of audio was the most incredible thing I'd ever seen my phone do. This recognition works though a process called audio fingerprinting. Examples include:

- Shazam
- SoundHound / Midomi

https://willdrevo.com/fingerprinting-and-audio-recognition-with-python/

# **Notes for the Viewer:**

### E README.md

 $\mathbf{C}$ 

### dejavu

Audio fingerprinting and recognition algorithm implemented in Python, see the explanation here: How it works

Dejavu can memorize audio by listening to it once and fingerprinting it. Then by playing a song and recording microphone input or reading from disk, Dejavu attempts to match the audio against the fingerprints held in the database, returning the song being played.

Note: for voice recognition, Dejavu is not the right tool! Dejavu excels at recognition of exact signals with reasonable amounts of noise.

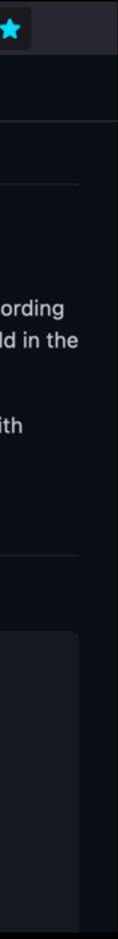
### **Quickstart with Docker**

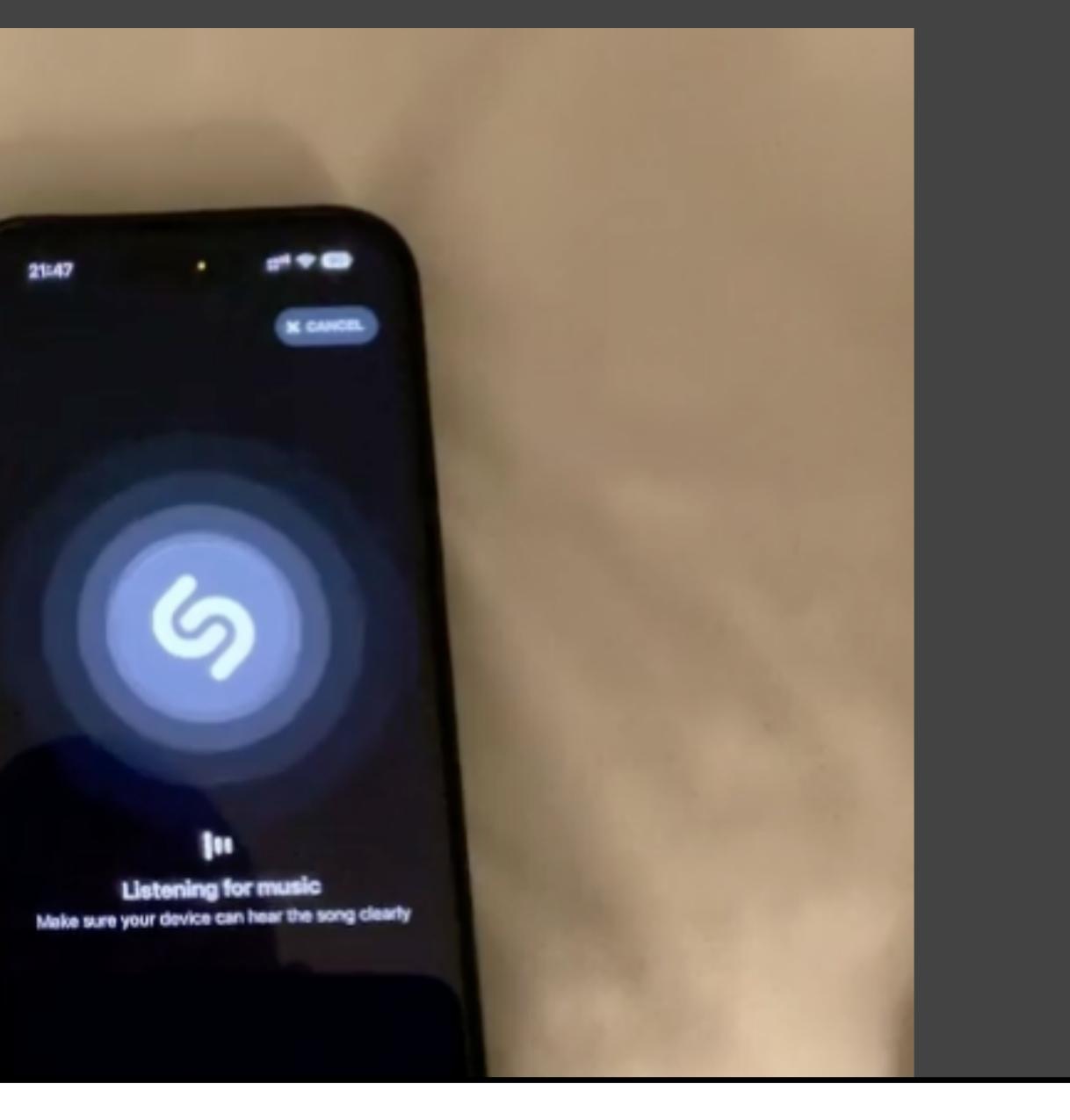
First, install Docker.

```
# build and then run our containers
$ docker-compose build
$ docker-compose up -d
# get a shell inside the container
$ docker-compose run python /bin/bash
Starting dejavu_db_1 ... done
root@f9ea95ce5cea:/code# python example_docker_postgres.py
Fingerprinting channel 1/2 for test/woodward_43s.wav
Fingerprinting channel 1/2 for test/sean_secs.wav
```

https://github.com/worldveil/dejavu

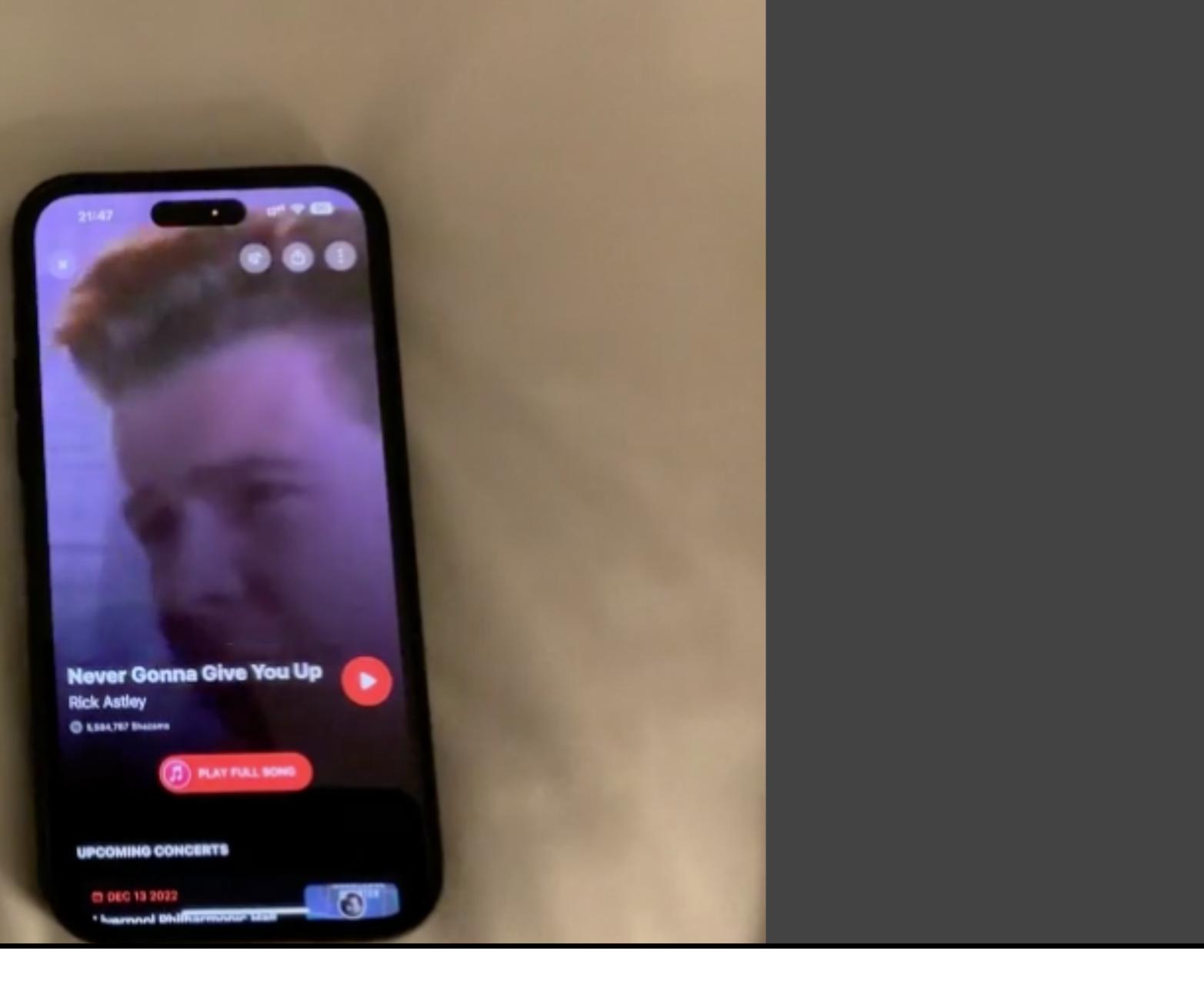
## I found a great post about fingerprinting audio, along with a framework I could modify/play with.





**Notes for the Viewer:** Stills from a video showing how Shazam identifies music.





**Notes for the Viewer:** Stills from a video showing how Shazam identifies music.



33, 72, 77, 62, 348, 6047, 75, 3054, 72, 3861, 71, 164, 70, 2817, 69, 75, 2966, 71, 168, 85, 50, 2753, 69, 120, 140, 2788, 119, 46, 4388, 70, 3035, 118, a71, 87, 2842, i118, 169, -109, 2825, 118, i72, 149, 8415, 117, 69, 130, e126, i2653, 120, e120, 134, i9117, e123, 78, 2506, 71, 165, 63, 2820, 69, 75, 2963, 123, 35, 9215, 122, 8780, 76, 3032, 58, 30018, 123, 2909, 69, 129, 86, 2826, 71, 118 , 2920, 66, 69, 19514, 118, 34, 2947, 69, 170, 10638, 122, 8939, 112, 2974, 71, 122, 3651, 119, 33, 2968, 72, 3034, 68, 165, 48, 2821, 71, 164, 81, 127, 2702, 71, 117, 2915, 118, 72, 127, 55, 2752, 72, 121, 2915, 121, 66, 130, 120, 24, 144, 7685, 124, 2962 , 68, 121, 129, 128, 123, 122, 175, 7102, 68, 121, 141, 2783, 122, 72, 126, 117, 130, 123, 169, 6882, 103, 74, 8857, 58, 4909, 1 18, 71, 149, 2737, 170, 34, 2953, 121, 28123, 70, 9852, 118, 10003, 78, 13889, 69, 79, 14458, 122, 2928, 73, 10876, 52, 10914, 7 1, 3018, 73, 6807, 71, 6927, 75, 4953, 123, 2984, 120, 2976, 71, 3031, 118, 34, 2962, 87, 2973, 27, 111, 100, 2910, 76, 3025, 11 9, 41, 2944, 75, 3025, 71, 165, 49, 2951, 72, 3012, 118, 71, 181, 2756, 120, 6602, 68, 121, 145, 2790, 109, 35, 4619, 69, 120, 8, 2833, 118, 72, 127, 118, 216, 2478, 133, 2967, 119, 4494, 74, 1766, 13189, 145, 8882, 72, 3026, 73, 11744, 121, 13932, 72, 49 56, 74, 8923, 71, 165, 45, 2834, 71, 194, 54, 52, 2753, 118, 69, 96, 2835, 122, 33, 8594, 118, 32, 2971, 71, 164, 84, 174, 68, 1, 106, 118, 124, 124, 173, 71, 128, 84, 1685, 69, 120, 177, 35, 2729, 118, 72, 127, 60, 8047, 72, 164, 71, 2804, 69, 118, 82, 851, 71, 168, 73, 2809, 69, 118, 132, 165, 76, 185, 34, 2372, 73, 8540, 119, 47, 2949, 71, 164, 50, 2834, 70, 165, 84, 114, 2695 , 68, 118, 133, 42, 2770, 118, 34, 8289, 72, 12838, 122, 2978, 120, 21792, 72, 3014, 121, 10742, 119, 33, 13984, 74, 3009, 124, 12744,76,4968,72,11883,121,3881,202,7797,72,11847,122,12975,122,15887,121,10802,72,10932,120,10934,78,1488 5, 72, 9921, 121, 8857, 122, 7816, 118, 7892, 123, 5906, 125, 4948, 90, 7917, 92, 9839, 121, 6847, 117, 6926, 119, 6912, 74, 693 1, 77, 12963, 121, 10815, 72, 13903, 74, 4935, 75, 3028, 71, 3800, 120, 5879, 121, 6884, 70, 13945, 74, 10916, 131, 2812, 232, 9 388, 221, 3750, 158523, 102, 518, 8392, 52958, 120072, 2775, 88, 716, 2824, 175514, 155465, 113794, 84, 60724, 223924, 46940, 15 542, 124961, 93668, 179892, 500224, 170839, 172608, 130, 327996, 177188, 4764, 70169, 102, 552, 82322, 16174, 76, 6003, 72854, 9 1, 834, 125699, 522332, 133, 11213, 75, 2723, 67, 165, 48, 2743, 68, 117, 105, 2820, 118, 112, 2894, 63, 56736, 130, 2741, 117, 59, 86, 2738, 71, 140, 2888, 118, 68, 102, 2819, 118, 72, 168, 2766, 80, 78, 14312, 77, 3009, 69, 118, 99, 2776, 117, 121, 32860 , 79, 3029, 77, ∞67, ∞2714, 79, ∴3010, 71, 171, 74, 173, 2529, 73, 68, 2968, 119, 71, 107, 2821, 79, 3021, 71, 172, 67, 81, 2738, € 3. 121. 150. 2784. 118. 71. 187. 77. 2672. 71. 122. 2919. 119. 34. 2922. 140. 2993. 118. 71. 181. 88. 2669. 70. 75. 2963. 119. 3

### **Notes for the Viewer:** I take the microseconds in between and make them a frequency in an audio file using wavio and pydub

58, 42,×2439, 1113, 645, 2354, 149, 535, 11752, 135, 60, 13047, 3099, 42, 69, 3056, 1408, 184, 11131, 3099, 59, 5197, 3364, 48, a1 76. 18. 91. 42758. 3741. 68. 111. 2507. 58. 5880. 2265. 2251

wavio 0.0.4 pip install wavio 🕒

https://github.com/WarrenWeckesser/wavio

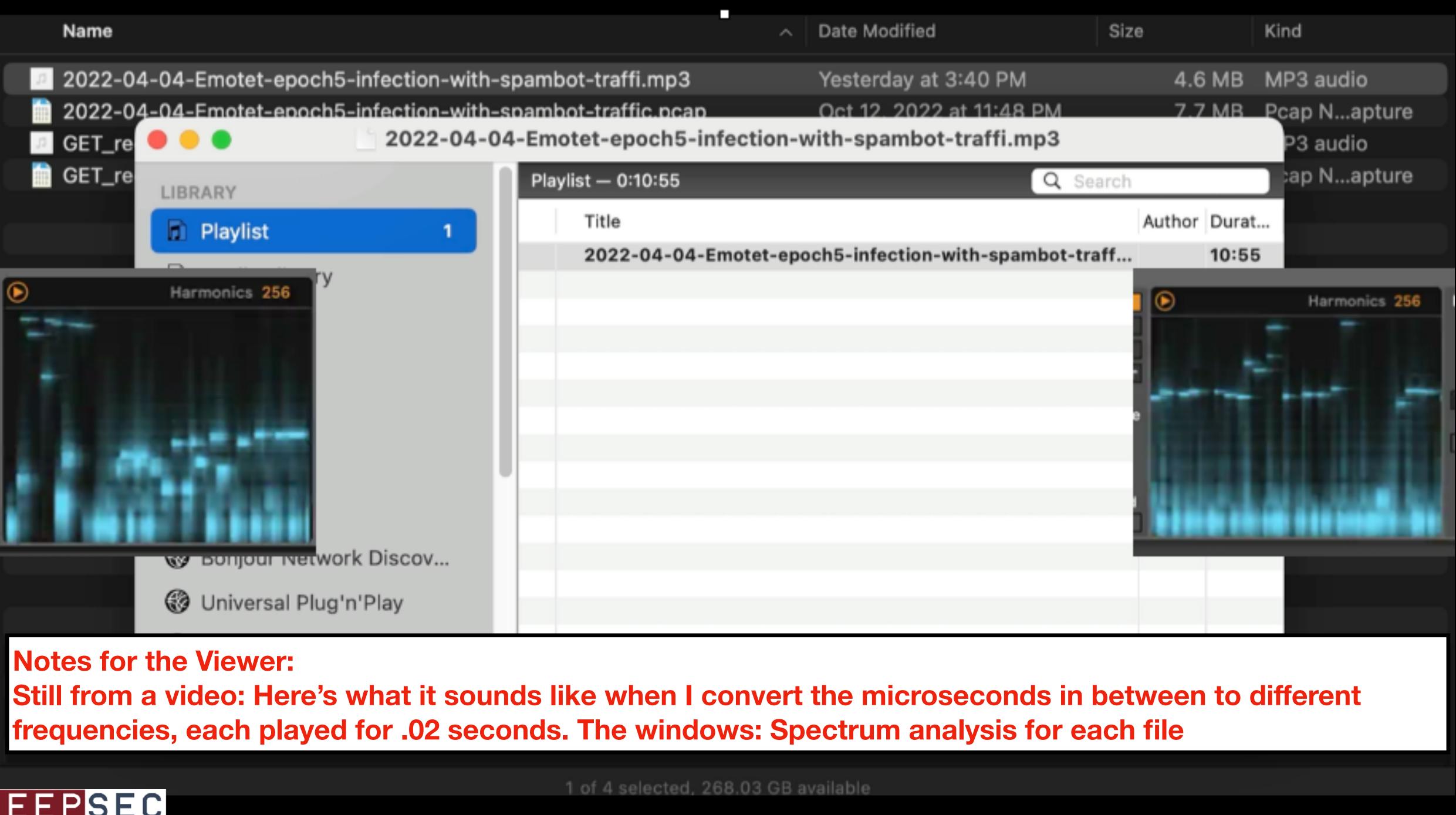
DEEPSEC

### pydub 0.25.1

pip install pydub 🕒

http://pydub.com/





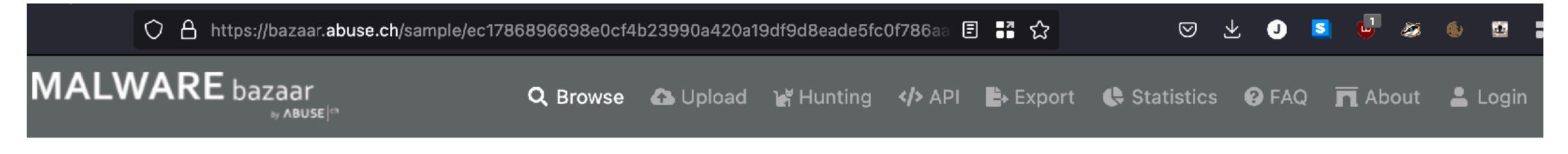
## DEEPSEC

# Same Malware Sample/ **Different Environments**

**Notes for the Viewer:** Let's see what happens when malware is run in different environments, where bandwidth might make the timing differ. Will we still see a signature match?





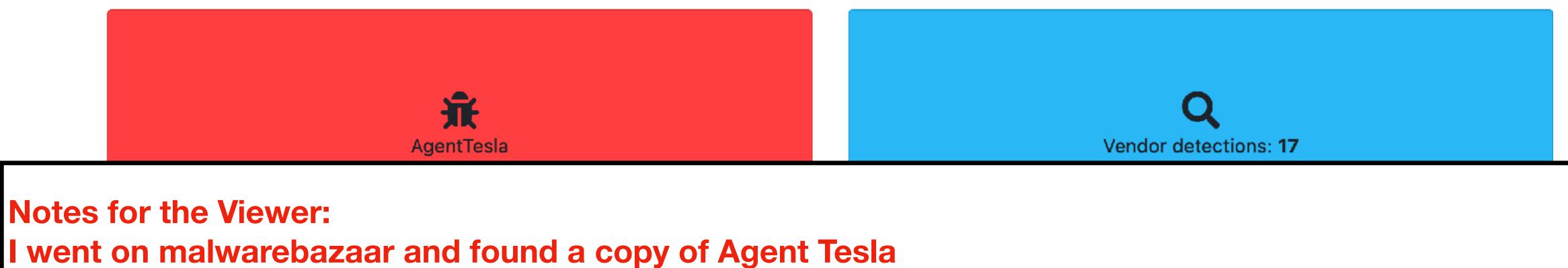


Browse / Malware sample

# MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for SHA256 ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

## **Database Entry**



Intelligence 17	IOCs	YARA 3	File information	Comments 1	Actions -



C ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f

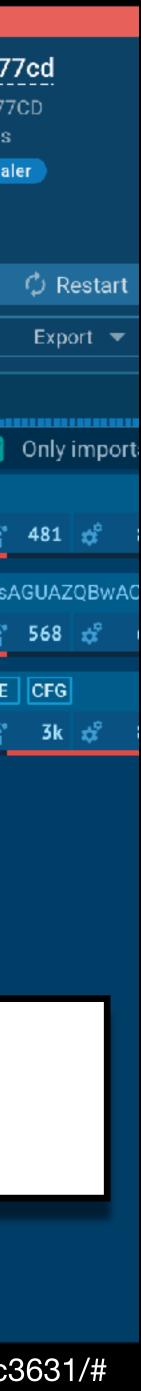


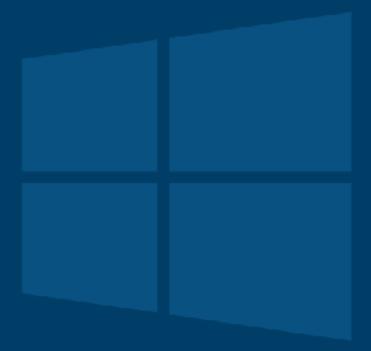


## **Notes for the Viewer:** and then I found that someone had already run it on any.run

DEE	<b>PSEC</b> mple/ed	c1786896698e0cf4b23990a420a19df9c	l8eade5fc0f786aa980d50b026ac13f/	https://app.any.run/	tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3
59731 ms	POST   200: OK	👌 2944 ad244b8ab0e31636cd 🗖	opendir http://80.85.156.9/fe33l/inc/0docbb2f367788.php	9.27 Kb 🕇 text 200 b 🕂 ini	
59729 ms	POST   200: OK	👌 2944 ad244b8ab0e31636cd 🗖	opendir http://80.85.156.9/fe33l/inc/0dccbb2f367788.php	200 b <b>↓ in</b> i	

	🚽 🖗 Malicio	ous activity	
a a	d244b8ab0e316	36cdc93dca27a	1777
	ID5: AD244B8AB0E3 tart: 11.11.2022, 20:		
Win7 32 bit Complete	trojan rat agen	ttesla opendir	steale
Indicators: 🚸 🗶	re 💠 🖳 🕞	Tracker: <u>Agent Tes</u>	la
보 Get sample	E 10C	MalConf	
Text report	Process graph	ATT&CK <sup>™</sup> matrix	
	СРИ		
Processes Filter b	y PID or name		
▼ 2672 ad244b8a	ab0e31636cdc93dca	27a777cd.exe PE	]
←→ 🕮 🛱		📄 1k	
3360 powe	ershell.exe -enc UwB	0AGEAcgB0AC0AUv	wBsA(
		📄 1k	1
2944 ad24	4b8ab0e31636cdc93	3dca27a777cd.exe	PE
愛ち妻。	* 💿	enttesla 📔 1k	1

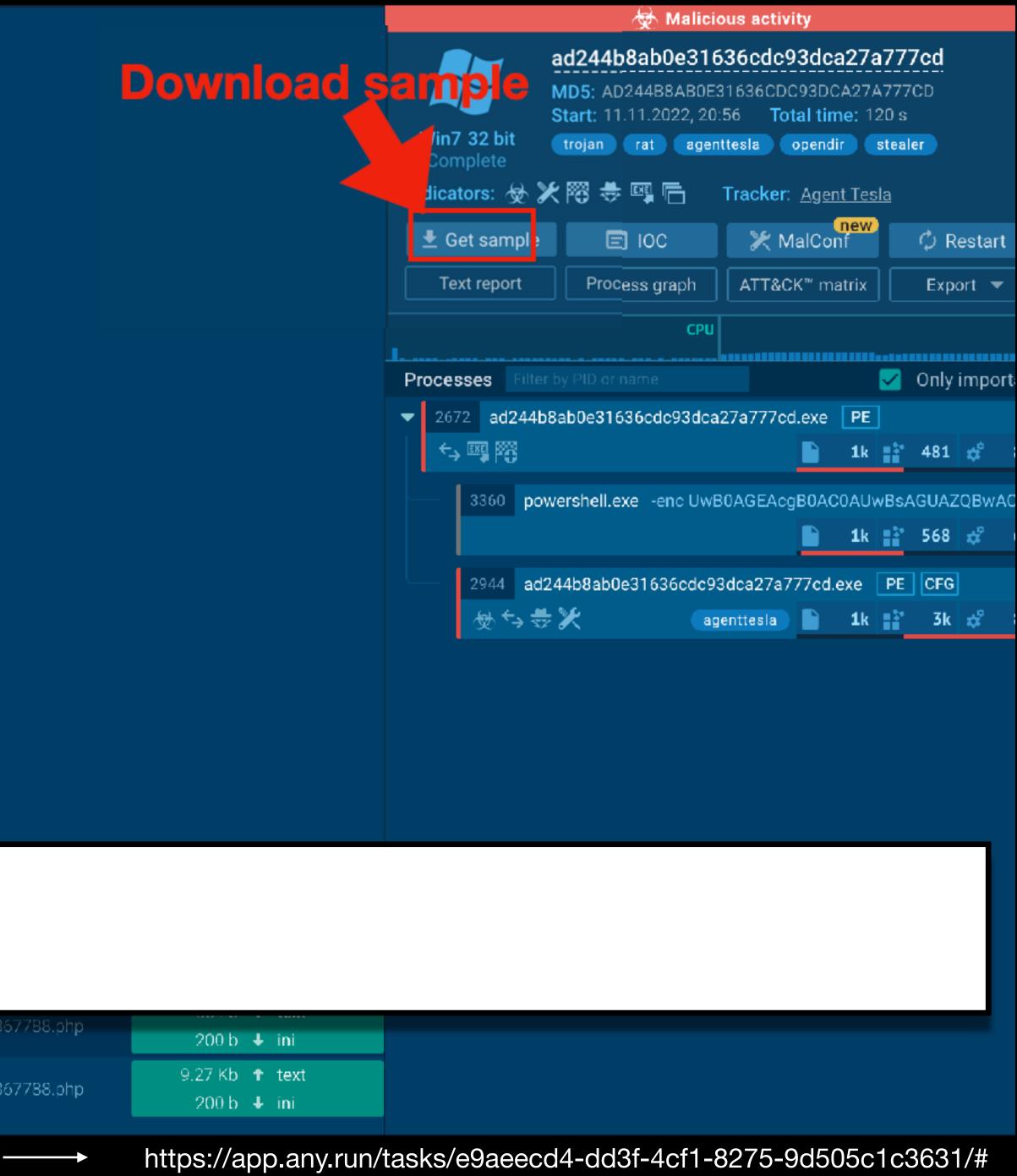




# Notes for the Viewer: I downloaded the sample

		c178	6896698e0cf4b239	990a420a19	df9d8	eade5fc0f786aa980d50b026ac13f/	https://app.anv.run/	/tasks/e9aeecd4-dd3f-4cf1-8	8275-9d505c1c3
59731 ms	POST   200: OK	6	2944 ad244b8ab0e	e31636cd		opendir http://80.85.156.9/fe33l/inc/0docbb2f367788.php	9.27 Kb ↑ text 200 b ↓ ini		
59729 ms	POST   200: OK	Ø	2944 ad244b8ab0e	e31636cd		opendir http://80.85.156.9/fe33l/inc/0dccbb2f367788.php	200 b 🕹 ini		

DEEPSEC mple/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac

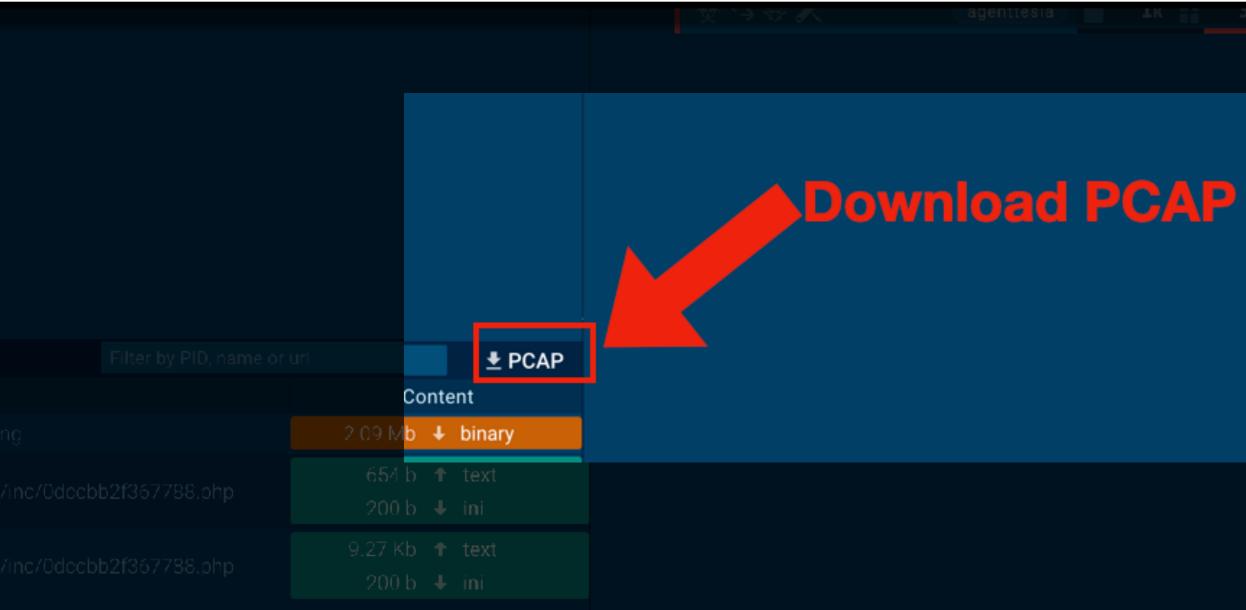


## Notes for the Viewer: And I downloaded the PCAP

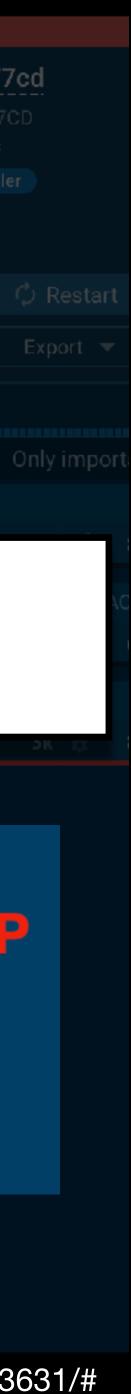
HTTP Reque	sts 3	Connections		DNSI	Requests		Threats		
Timeshift	Head	lers	Rep	PID	Process na	ame	C	N.	URL
	GET I	200: OK						)	
	POST I	200: OK					)6cd	-	opendir http://80.85.156.9/fe33l/i
	POST	200: OK					36od		opendir http://80.85.156.9/fe33l/i

DEEPSEC mple/ec1786896698e0cf4b23990a420a19df9d8eade5fc0f786aa980d50b026ac13f/

	😓 Malici	ous activity	
		536cdc93dca27a7 31636CDC93DCA27A77 :56 Total time: 120 nttesla opendir ste	
Indicators: 🕁 🗶	19 💠 🖳 🗖	Tracker: <u>Agent Tesla</u>	
生 Get sample		MalConf	
Text report	Process graph	ATT&CK <sup>™</sup> matrix	
Processes Filter b			
▼ 2672 ad244b8a	ab0e31636cdc93dca	27a777cd.exe PE	



https://app.any.run/tasks/e9aeecd4-dd3f-4cf1-8275-9d505c1c3631/#



# any.run: 192.168.100.82 -> 80.85.156.9 POST /fe33l/inc/0dccbb2f367788.php

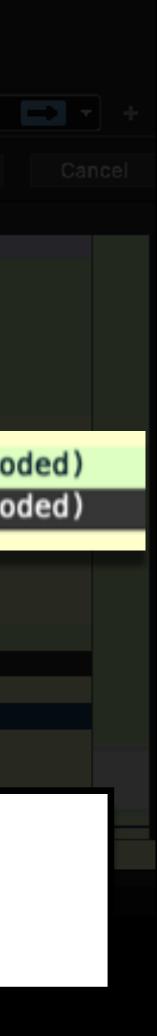
17 2022-11-11 2843 2022-11-11 2849 2022-11-11 2868 2022-11-11 2750 2022-11-11	20:58:50.762534 20:56:53.121078 20:57:51.669902 20:57:51.918734 20:57:52.044996 20:56:54.330841	192.168.100.82 80.85.156.9 80.85.156.9 80.85.156.9 80.85.156.9 37.139.128.94	Destination 192.168.100.82 37.139.128.94 192.168.100.82 192.168.100.82 192.168.100.82 192.168.100.82	Protoc TLSv1 HTTP HTTP HTTP HTTP HTTP	85 132 79 79 252 1119	Encrypt GET /fx HTTP/1. HTTP/1. HTTP/1. HTTP/1.	/Lqmslu 1 100 C 1 100 C 1 200 C 1 200 C
		80.85.156.9	192.168.100.82 192.168.100.255 HTTP	HTTP BROWS 7		HTTP/1. Hest. An	nqiw cer
192.168.10	0.82	80.85.156.9	НТТР	11	L00	POST	/fe3
2869       2022-11-11         2871       2022-11-11         2844       2022-11-11         2865       2022-11-11         2791       2022-11-11         2792       2022-11-11         2793       2022-11-11	20:57:51.443489         20:57:52.184260         20:57:52.934253         20:57:51.670159         20:57:51.942289         20:57:23.121850         20:57:23.871729         20:57:24.621708	192.168.100.82 192.168.100.82 192.168.100.82 192.168.100.82	<b>255</b> 192.168.100.255 192.168.100.255 80.85.156.9 80.85.156.9 192.168.100.255 <b>192.168.100.255</b> 192.168.100.255 192.168.100.255	NBNS NBNS HTTP HTTP NBNS NBNS NBNS	92 92 708 1100 110 110 110	Rame in Name qu Name qu POST /f POST /f Registr Registr Registr	ery NB ery NB e33l/in e33l/in ation N ation N ation N

## **Notes for the Viewer:** Here is just the traffic from that machine to any hosts



<01><02> MSBROWSE <02><01>

rt Joi.png HTTP/1.1 Continue Continue W	
)K (image/png) )K (text/html)	
31/inc/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-u	urlence
3l/inc/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-u	urlenco
jon NR <01 <02 > MSRROWSE <02 <01 >	
USER-PC<1c> USER-PC<1c>	
<pre>ic/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-urlencoded) ic/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-urlencoded)</pre>	
c/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-urlencoded) HB <01><02>MSBROWSE<02><01>	



### analysis1

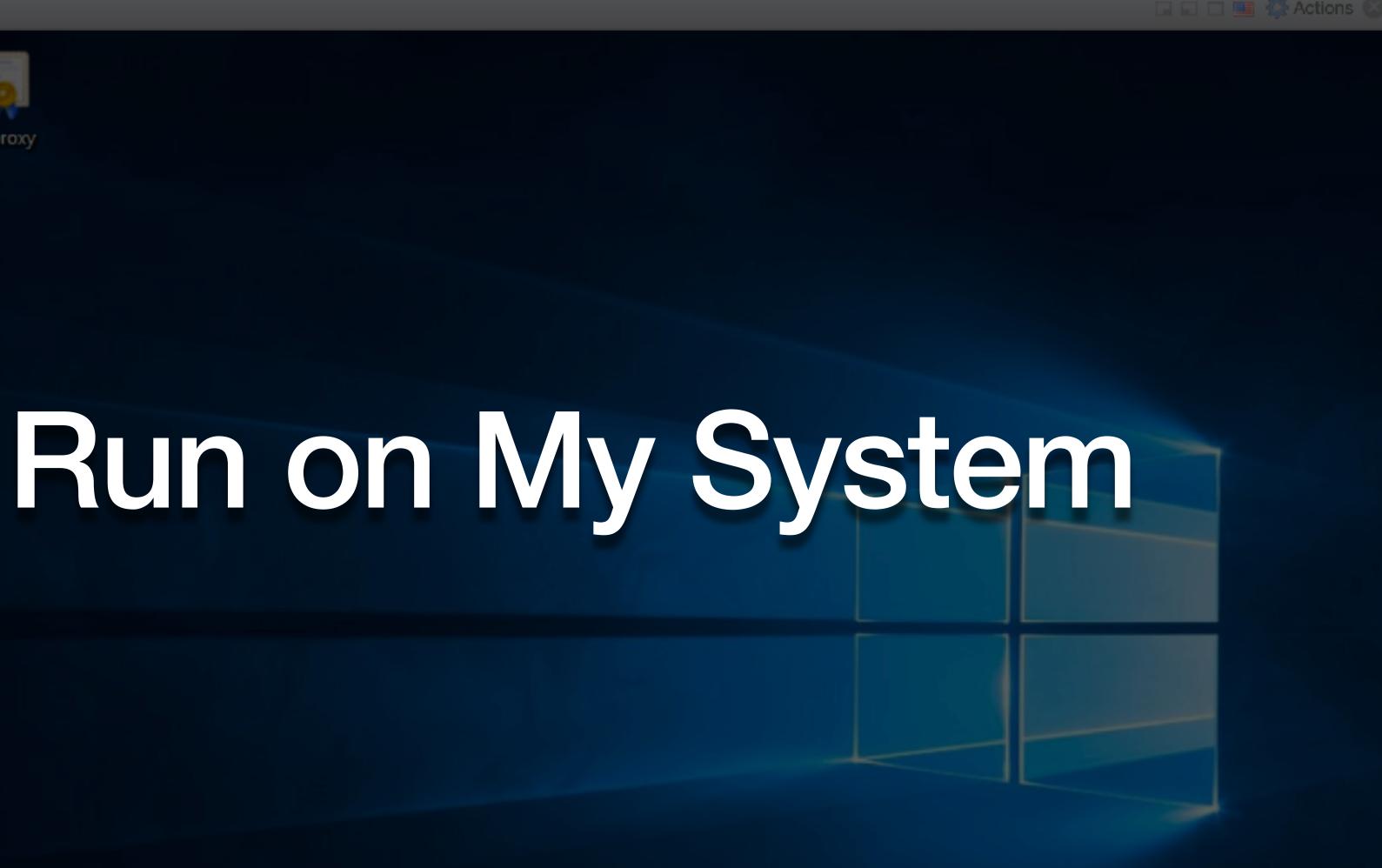








Doc30644101







📰 🔎 🛱 🧲 🔚 💼 🕋 🍪 🚄





		Recy	cle Bin
RR	^ 도 48	8:13 AM 11/12/2022	, ,

# VE: 192.168.1.99 -> 80.85.156.9

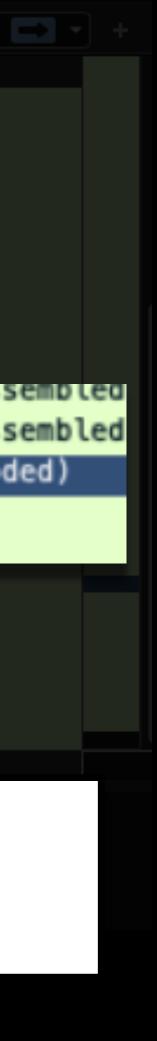
### POST /fe33l/inc/0dccbb2f367788.php

	2022-11-12 00:16:41.052871	80.85.156.9	192.168.1.99			80 → 49719	[A
17	2022-11-12 00:16:41.053645	80.85.156.9	192.168.1.99			<b>80 → 49719</b>	[A
18	2022-11-12 00:16:41.054304	80.85.156.9	192.168.1.99			<b>80 → 49719</b>	[A
19	2022-11-12 00:16:41.054829	80.85.156.9	192.168.1.99			<b>80</b> → <b>49719</b>	[AI
20	2022-11-12 00:16:41.055996	80.85.156.9	192.168.1.99			<b>80</b> → <b>49719</b>	[A
21	2022-11-12 00:16:41.056680	192.168.1.99	80.85.156.9		1506	49719 → 80	[A
. 22	2022-11-12 00:16:41.056680	192.168.1.99	80.85.156.9		1506	49719 → 80	[A
• 23	2022-11-12 00:16:41.056680	192.168.1.99	80.85.156.9		1506	49719 → 80	[A
• 24	2022-11-12 00:16:41.056680	192.168.1.99	80.85.156.9		1506	49719 → 80	[A(
• 25	2022-11-12 00:16:41.056680	192.168.1.99	80.85.156.9		1506	49719 → 80	[A
	2022-11-12 00:16:41.056726		80.85.156.9	TCP		49719 → 80	
192	.168.1.99	80.85.156.9	ICP	1:	990	49/19 →	-
192	.168.1.99	80.85.156.9	TCP	15	506	49719 →	8
192	.168.1.99	80.85.156.9	нття	<b>)</b> 1	178	POST /f	e:
80.	85.156.9	192.168.1.99	TCP		60	80 → 49	71
80.	85.156.9	192.168.1.99	TCP		60	80 → 49	71
	2022-11-12 00:16:41.284304	80.85.156.9	192.168.1.99			80 → 49719	
- 55	2022-11-12 00:16:41.349047	00.03.130.3	192.168.1.99	HTTP		HTTP/1.1 20	
	2022-11-12 00:16:41.403414		80.85.156.9			49719 → 80	
	2022-11-12 00:16:46.838844		192.168.1.99			80 → 49719	
	2022-11-12 00:16:46.843653		80.85.156.9			49719 → 80	
	2022-11-12 00:18:21.353694		80.85.156.9			49719 → 80	
∟ 40	2022-11-12 00:18:21.578559	80.85.156.9	192.168.1.99			80 → 49719	

### **Notes for the Viewer:** Seeing the same type of traffic



```
Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU]
         9 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU]
           Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled PDU]
                    =262656 Len=1452 [TCP segment of a reassembled PDU]
80 [ACK] Seq=26413 ACK=26 W1N=262656 Len=1452 [ICP segment of a reassembled
80 [ACK] Seq=27865 Ack=26 Win=262656 Len=1452 [TCP segment of a reassembled
331/inc/0dccbb2f367788.php HTTP/1.1 (application/x-www-form-urlencoded)
'19 [ACK] Seq=26 Ack=20605 Win=132096 Len=0
19 [ACK] Seg=26 Ack=26413 Win=132096 Len=0
  Seq=29441 Ack=281 Win=262400 Len=0
  ACK] Seq=29441 Ack=281 Win=262400 Len=0
  Seq=281 Ack=29442 Win=132096 Len=0
```







# Shazam it!

# Create an audio file from the any.run PCAP

Name
Any_run_e9aeecd4-dd3f-4cf1-8
myrun_justthepost.pcap
signature_g
iCloud
E Shared
. iPad P ≜
Network



## 3275-9d505c1c3631.pcap

# Create an audio file from my PCAP

			て#2	-zsh	¥1 .
		jpyor	re@jair	pcaps %	6
	< >				
Favorites					
🧑 AirDrop	Nan				
🙏 Applicati	Any				
Desktop	Any				
🖨 DATA	📄 myr				
AUDIO	sigr				
🚞 signature					
Ownloads					
😭 jpyorre					
iCloud					
🛆 iCloud Dri					
😁 Shared					

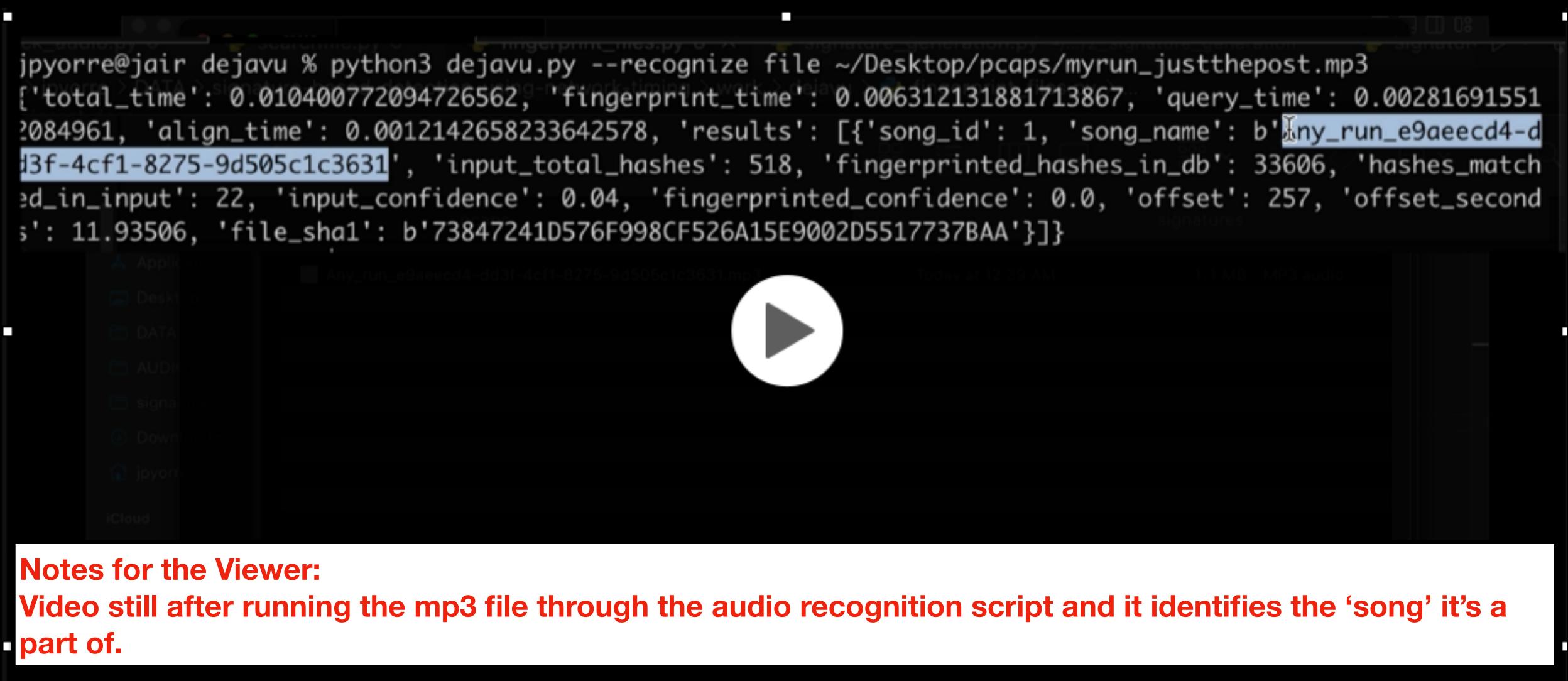




89 100 100   00 00	research: ~ (-zsh)	earch: ~ (mariadb)	жз jo	josh@ids: ~ (-zsh) #4					
A Date Modified Size Kind   A Date Modified Size Kind   B Today at 12:39 AM 1 TIMB MP3 audio   ap Yesterday at 11:40 PM 2.4 MB Pcap Niapture   Today at 12:32 AM 33 KB Pcap Napture									
N3       Today at 12:39 AM       1 TIMB       MP3 audio         ap       Yesterday at 11:40 PM       2:4 MB       Peap Niapture         Today at 12:32 AM       33 KB       Peap Napture									
N3Today at 12:39 AM1 TIMBMP3 audioapYesterday at 11:40 PM2.4 MBPeap NiaptureToday at 12:32 AM33 KBPeap Napture									
	з 👔 Т								



# Identify Threat (AKA Shazam it)





# Same, but signature method based off percentages

**Notes for the Viewer:** Repeating this process, but using the quicker and more practical signature method we've been building during this presentation.





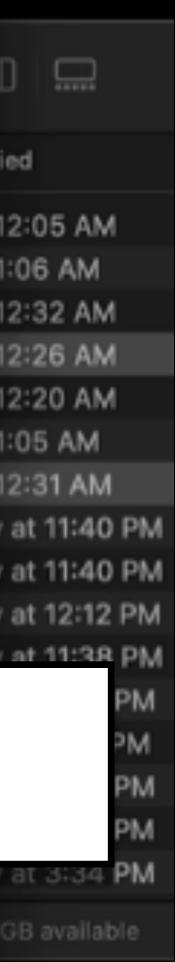
## jpyorre@jair 2\_signature\_generation %

•••	> 2_signature_generation
Favorites	2_signature_generation
💎 AirDrop	Name
🐴 Applicati	anyrun_justthepost.pcap
🚍 Desktop	my_run_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631.pca
📛 DATA	signature_generation.py
audio	
🚞 signature	
Ownloads	
😭 jpyorre	
iCloud	
iCloud Dri	
🖿 Shared	

## Notes for the Viewer: Video Still: We have both PCAPs, one from the any.run analysis and one from my own.

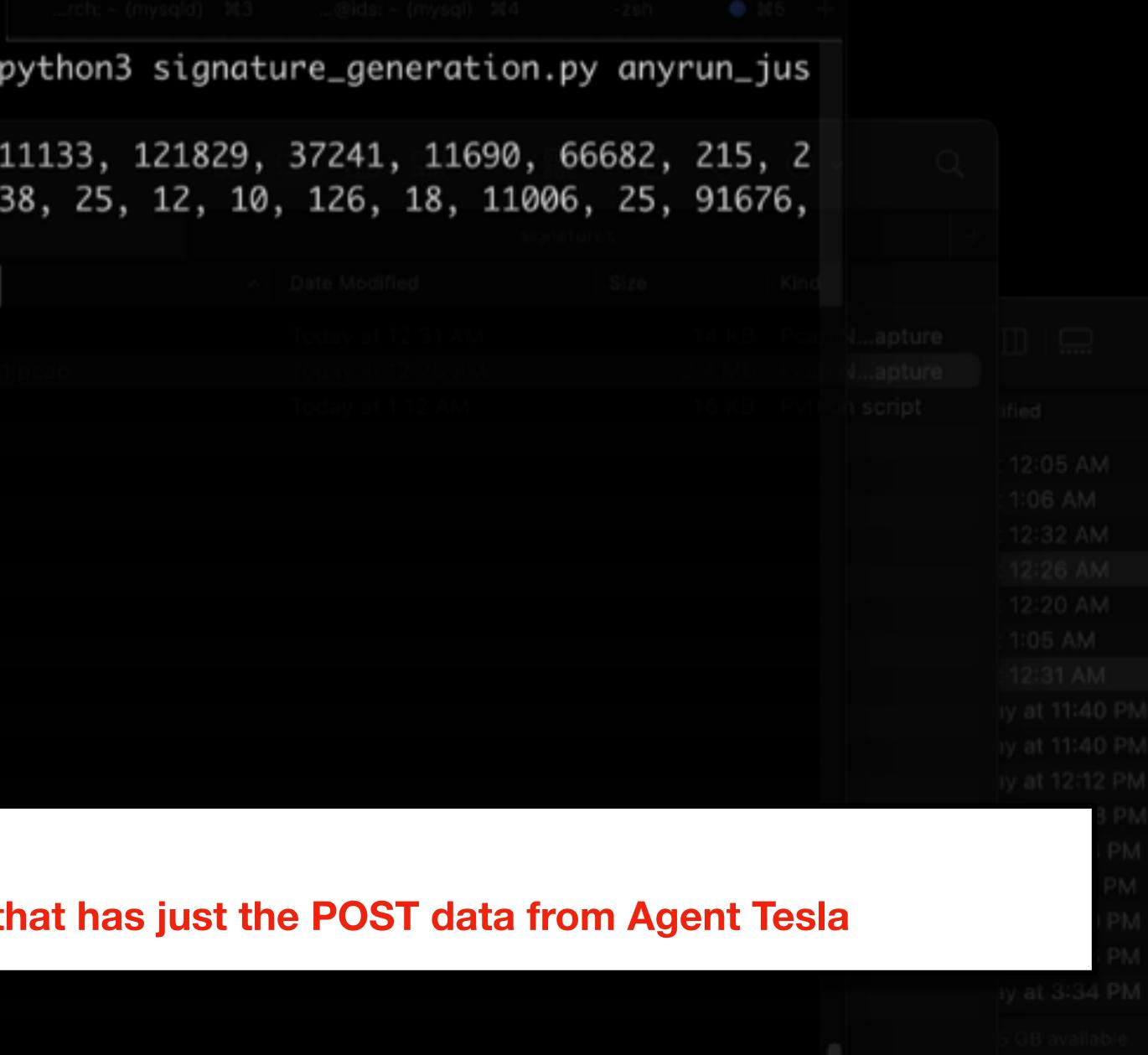


	88 ☷ Ш		oo v ⊂ C	,
			0.	`
		signatures		+
	A Date Modified	Size	Kind	
	Today at 12:31 AM	14 KB	Pcap Napture	
ар	Today at 12:26 AM	2.4 MB	Pcap Napture	
	Today at 1:12 AM	16 KB	Python script	



jpyorre tthepos	-	-	iture_g	eneratio	n%p
-				32776, 2 6, 5, 4,	
		995, 181		re_generation	
			_	eneratio	n %
				Ī	

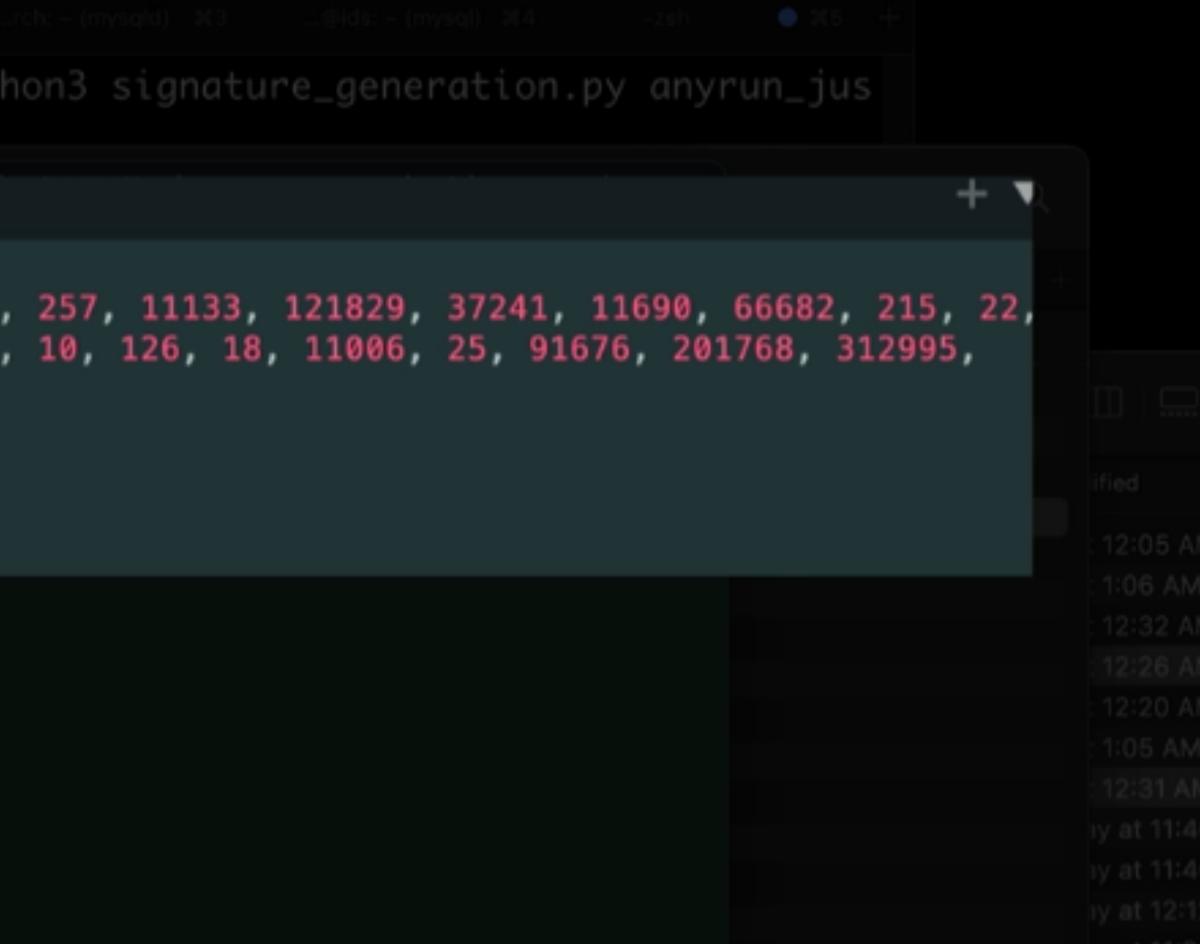
## **Notes for the Viewer:** Video Still: We generate a signature from a PCAP that has just the POST data from Agent Tesla



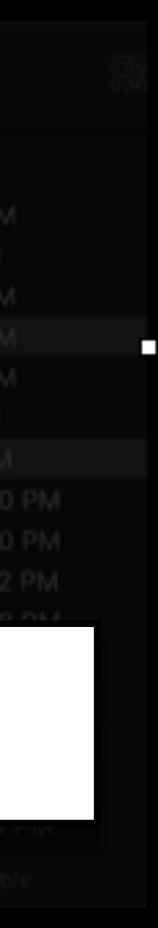
	jpyorre@jair tthenost nca					
signat	ures.json 🛛 🔍					
{ }	'Agent Tesla POST": 8, 10996, 25, 181 <u>]</u>	:[11407, 1 128, 17,	50, 139, 6, 5, 4,	12029, 11938,	1327 25,	776 12

## Notes for the Viewer: Video Still: and we put that signature in our signatures.json file.

Red
 Orange
 Yellow



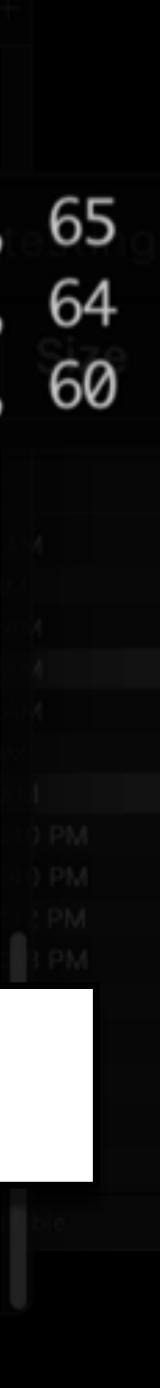




# 'my\_run\_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631\_0.cap: Agent Tesla POST, 65 /my\_run\_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631\_1.cap: Agent Tesla POST, 64 /my\_run\_e9aeecd4-dd3f-4cf1-8275-9d505c1c3631\_2.cap: Agent Tesla POST, 60

# **Notes for the Viewer:** from the malware run on my system.





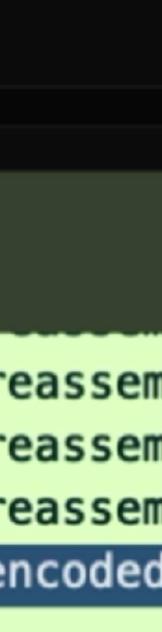
																dd3f-4									
				٢			×	C																	
No.		Time				S	ource			Destin	ation	Pro	otoc Le	eng Info	0										
	18 19 20	2022-1 2022-1 2022-1	1-12 1-12 11-12	00:16: 00:16: 00:16:	41.0530 41.0543 41.0548 41.0559 41.0566	304 80 829 80 996 80	0.85.15 0.85.15 0.85.15	6.9 6.9 6.9		192.16 192.16 192.16 192.16 192.16 80.85.	8.1.99 8.1.99 8.1.99	TCI TCI TCI TCI TCI	> > >	60 80 60 80 60 80	<ul> <li>→ 49719</li> <li>→ 49719</li> <li>→ 49719</li> </ul>	[ACK] 5 [ACK] 5 [ACK] 5	Seq=26 / Seq=26 / Seq=26 /	Ack=11893 Ack=14797	Win=1320 Win=1320 Win=1320	96 Len=0 96 Len=0 96 Len=0	2 [TCP segmen	it of a reassemb	led PDU]		
	23 24	2022-1 2022-1 2022-1 2022-1	1-1 1-1																			segment			
	27 28	2022-1 2022-1 2022-1 2022-1	1-1 1-1																			segment			
	30	2022-1	1-1	1	78	P0	ST	/fe	2	l/inc	/0d(	ccbb2	f36	7788	3.ph	рΗ	TTP/	1.1	(ap	plic	ation/	x-www-fo	rm-	urle	n
	32	2022-1 2022-1 2022-1	1-1		60	80	<b>→</b>	497	/19	[ACK	] Se	eq=26	Ac	k=20	0605	Wi	n=13	32096	6 Ler	<b>1=0</b>					
		2022-1			60	80	-	497	/19	[ACK	] Se	eq=26	Ac	k=26	5413	Wi	n=13	32096	5 Ler	<b>)=0</b>					
	36 37	2022-1 2022-1 2022-1	1-1 1-1		60					[ACK		eq=26	Ac	k=29	9441	Wi	n=13	32096	6 Ler	<b>0=</b>					

## Notes for the Viewer: Video Still: Opening these files gives me the same network POST traffic pattern.

Transmission Control Protocol, Src Port: 49719, Dst Port: 80, Seq: 0, Len: 0



0040 04 02



# Going Further

- Using Third Party API's
  - Domain/IP Reputation & Relationships
  - Analysis of Components within the PCAPs



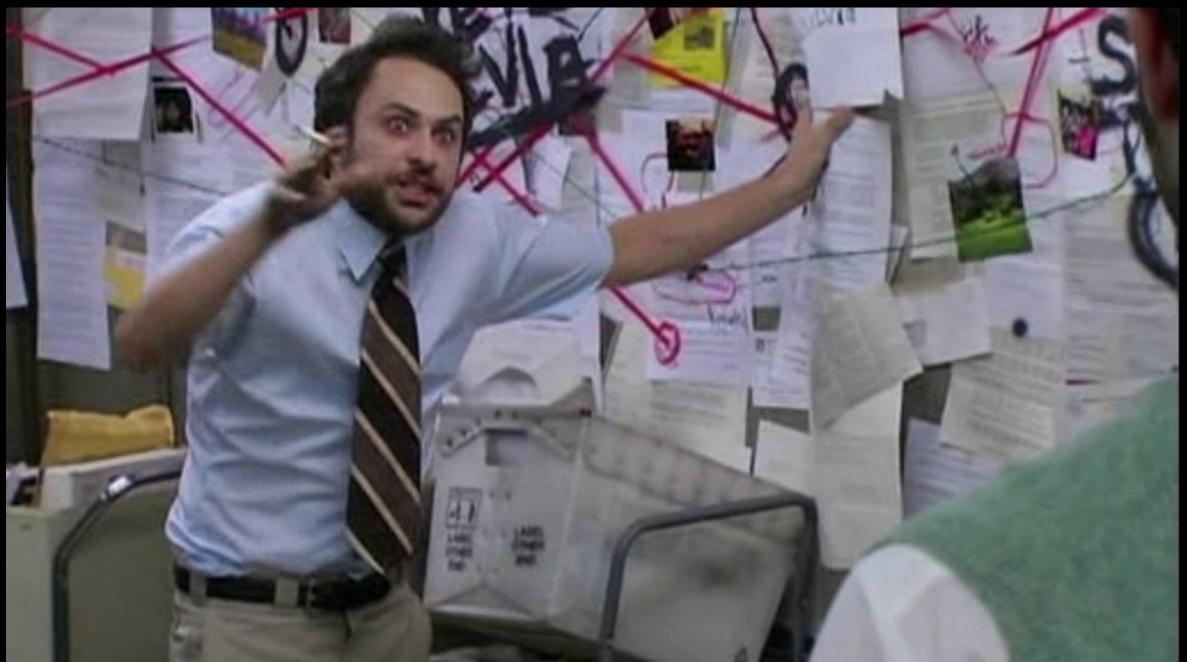


# The Future

- Run on streaming traffic
- Learn to program in something faster
- Build a web or API service to send PCAPs







# https://github.com/jpyorre/

Website: https://pyosec.com DEEPSEC

Twitter: @joshpyorre

# Code

Mastodon: @joshpyorre@infosec.exchange