CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

EMILIEN LE JAMTEL, TEAM LEADER, FIRST RESPONSE

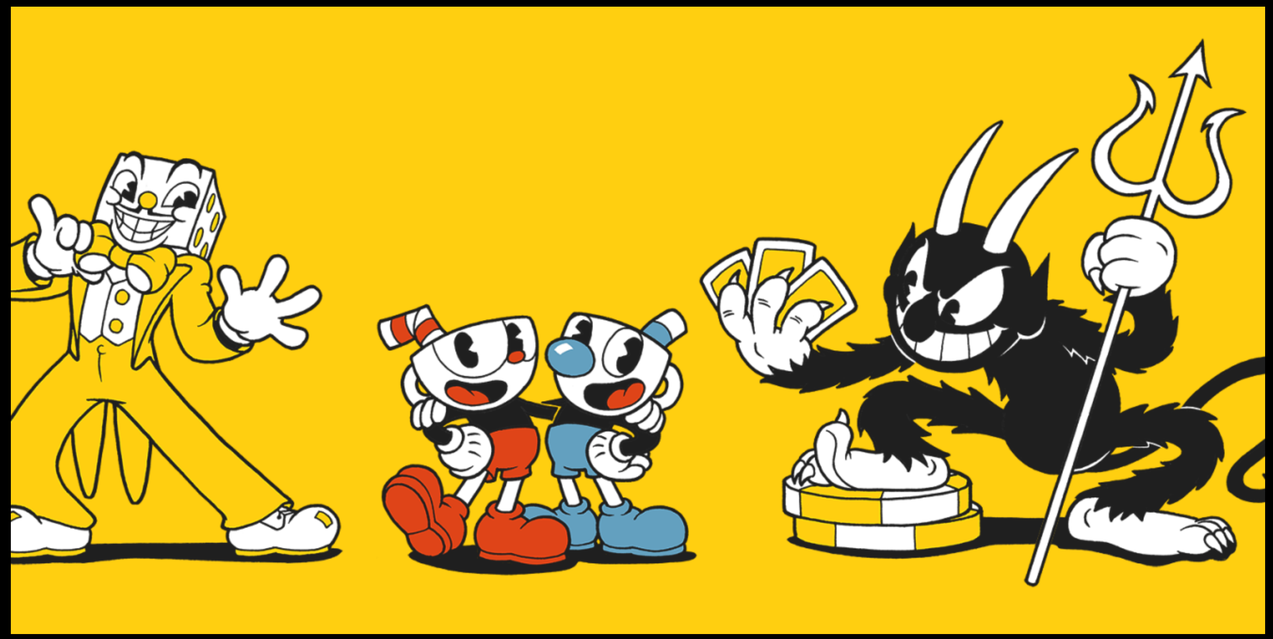
3RD MITRE ATT&CK EU USER WORKSHOP / 2019-05-10

TLP:WHITE

PRACTICAL THREAT HUNTING USING MITRE ATT&CK

What are we going to hunt ?

Threat Hunting is time-consuming, choose wisely!

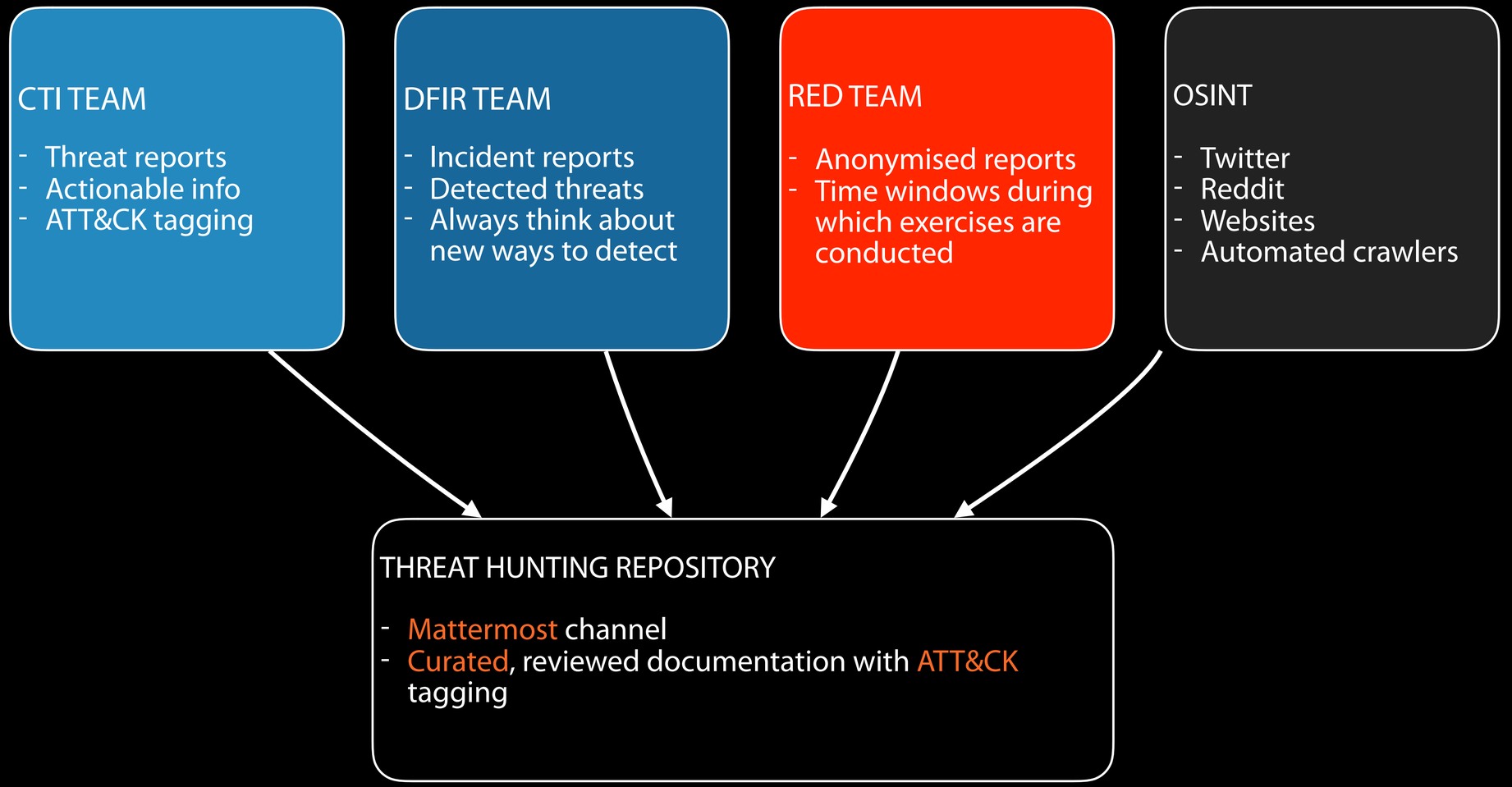


Threat Hunting starts and finishes with technology

WHERE TO HUNT? USING WHICH TECH?

- Use the logs Luke! Get a SIEM, leverage SIGMA
- Network sensors such as Snort & Suricata are still a thing
- Learn the dark arts of live scanning using YARA and EDR (or EDPR as the cool kids & girls say these days)

DOCUMENTATION IS OF THE ESSENCE



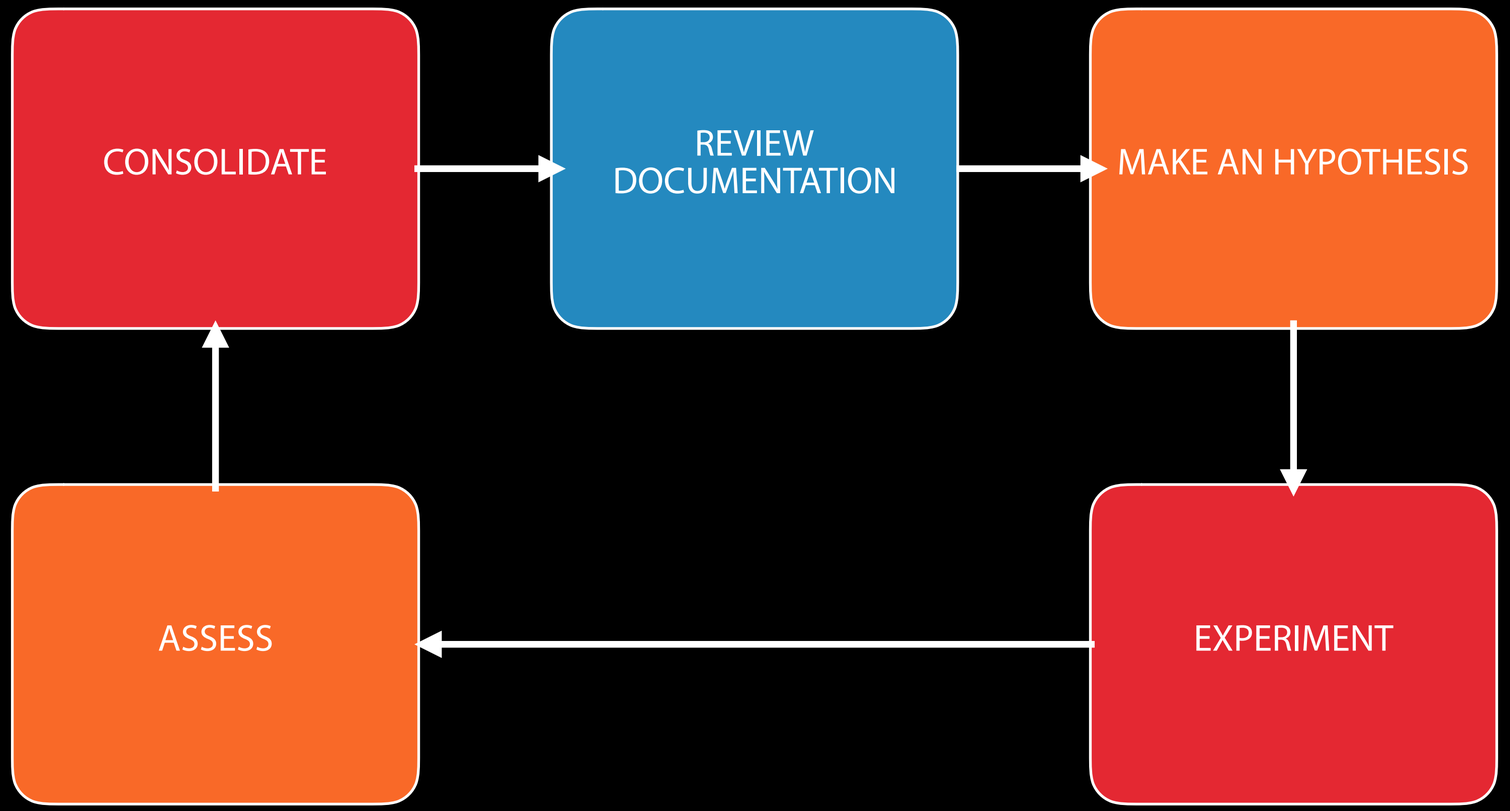
PRIORITISATION - EXAMPLE: APT10

Initial Access	Execution	Persistence	Privilege escalation	Defensive Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfil	C2
Spearphishing Attachment	Command-Line Interface	DLL Search Order Hijacking	DLL Search Order Hijacking	Deobfuscate/ Decode Files or Information	Credential Dumping	Account Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Compressed	Connection Proxy
Trusted Relationship	PowerShell	Scheduled Task	Scheduled Task	DLL Search Order Hijacking		Network Service Scanning	Remote File Copy	Data Staged		Remote File Copy
Valid Accounts	Scheduled Task	Valid Accounts	Valid Accounts	DLL Side-Loading		Remote System Discovery	Remote Services			
	Scripting			File Deletion		System Network Configuration Discovery				
	User Execution			Obfuscated Files or Information		System Network Connections Discovery				
	WMI			Process Hollowing						
				Scripting						
				Valid Accounts						

PRIORITISATION - EXAMPLE: APT10

Initial Access	Execution	Persistence	Privilege escalation	Defensive Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfil	C2
Spearphishing Attachment	Command-Line Interface	DLL Search Order Hijacking	DLL Search Order Hijacking	Deobfuscate/ Decode Files or Information	Credential Dumping	Account Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Compressed	Connection Proxy
Trusted Relationship	PowerShell	Scheduled Task	Scheduled Task	DLL Search Order Hijacking		Network Service Scanning	Remote File Copy	Data Staged		Remote File Copy
Valid Accounts	Scheduled Task	Valid Accounts	Valid Accounts	DLL Side-Loading		Remote System Discovery	Remote Services			
	Scripting			File Deletion		System Network Configuration Discovery				
	User Execution			Obfuscated Files or Information		System Network Connections Discovery				
	WMI			Process Hollowing						
				Scripting						
				Valid Accounts						

BREAKING IT DOWN INTO MICRO-PROJECTS



REVIEW DOCUMENTATION

- Documentation repository
- Incidents, Red Team exercises & CTI reports
- OSINT

MAKE AN HYPOTHESIS

EXAMPLE: COMMAND-LINE OBFUSCATION

- What is it doing?
  - Use Obfuscation to hide its true purpose

```
C:\Users\emilien>p^o^w^ers^he^ll w^ho^a^mi
desktop-88fdg9t\emilien
```

- Where and when can I find traces?
  - Executed command lines & running processes
- How can I have access to it?
  - Sysmon logs? PowerShell logs? Strings in memory?

EXPERIMENT

ASSESS

- Test in a lab environment if possible
- Design detection mechanisms

SPLUNK | SIGMA | SNORT | SURICATA | YARA

DASHBOARDS | STATISTICAL ANALYSIS

- False positives vs. True negatives

CONSOLIDATE

- What have we learned?
- Have we identified any gaps?
- Can we use the detection mechanisms we've built in production?
- Did we come up with new ideas for future hunts?

REVIEW DOCUMENTATION

HUNTING APT10 THROUGH ACCOUNT DISCOVERY (T1087)

Source	Info
Operation Cloud Hopper PwC / BAE systems	csvde.exe is a legitimate Microsoft administration command line tool used to import and export data from Active Directory (AD) Services.19It is of note that this binary requires elevated permissions as well as the AD Services (alternative AD Lightweight Directory Services) role to execute correctly. APT10 has been observed using it to export region specific AD data via the following command: **cmd /c "csvde -f C:\windows\web\[REGION].log"** This was run multiple times and resulted in the actor likely mapping out User and Host Names for the network.
Expel blogpost	https://expel.io/blog/how-to-hunt-for-reconnaissance/
CSVDE documentation	https://social.technet.microsoft.com/wiki/contents/articles/2113.comma-separated-value-directory-exchange-csvde-utility.aspx
JPCERT blog	https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

MAKE AN HYPOTHESIS

HUNTING APT10 THROUGH ACCOUNT DISCOVERY (T1087)

Question	Possible Answers
What?	Call to **csvde.exe -f** from command-line Requires **elevated permissions** and **AD Services** (alternative AD Lightweight Directory Services) role.
Where?	- Endpoint logs on compromised workstation/servers. - csvde.exe need to be installed (RSAT Active Directory Tools) - Usage of privileged accounts
When?	Process creation time **Get-WindowsFeature RSAT-AD-Tools** (PowerShell)
How?	- Sysmon logs (Execution) - Powershell Logs (Get-WindowsFeature) - Windows Security Logs (Process creation)

EXPERIMENT

ASSESS

HUNTING APT10 THROUGH ACCOUNT DISCOVERY (T1087)

- We found activity related to csvde.exe
  - Sysmon logs (EventID = 1)
  - Windows security logs (EventCode = 4688)
- Legitimate operation. The 'APT' was… CERT-EU's infrastructure team
- Activities related to RSAT-AD-Tools
  - No hit in PowerShell or Sysmon logs
  - Verified in lab environment
  - Activities in Registry events (to be investigated)

CONSOLIDATE

HUNTING APT10 THROUGH ACCOUNT DISCOVERY (T1087)

- SIGMA rules to generate the right alerts using Splunk
- Future hunt: WinRegistry logs for tool installation
- Gap analysis: monitor accounts granted with new AD services role

```
title: Execution of csvde.exe
description: Detection for
csvde.exe
author: Emilien Le Jamtel
tags:
    - attack.discovery
    - attack.t1087
logsource:
    category: process_creation
    product: windows
level: high
detection:
    selection1:
        CommandLine:
            - '*csvde -f*'
            - '*csvde.exe -f*'
    selection2:
        Image:
            - '*powershell.exe'
        CommandLine:
            - '*RSAT-AD-Tools*'
    condition:
selection1 or selection2
```

REVIEW DOCUMENTATION

HUNTING APT10 VIA WMI (T1087) & REMOTE FILE COPY (T1105)

Source	Info
Operation Cloud Hopper PwC / BAE systems	We have encountered the following script, t.vbs, which research has shown to be a modified version of the pentesting script known in open source as wmiexec.vbs.16 In single command mode, the script logs the user into the remote machine using Windows **Management Instrumentation (WMI)**, and **creates a Server Message Block (SMB) share**, which is usually set to C:\Windows or C:\Windows\TEMP.
Wmiexec.vbs source code	https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs
SIGMA rule example	https://github.com/Neo23x0/sigma/blob/master/rules/apt/apt_cloudhopper.yml
JPCERT analysis of wmiexec	https://jpcertcc.github.io/ToolAnalysisResultSheet/details/wmiexec-vbs.htm
FLARE report on WMI Fireeye	https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

REVIEW DOCUMENTATION

HUNTING APT10 VIA WMI (T1087) & REMOTE FILE COPY (T1105)

Source	Info

CreateShare function of wmiexec.vbs	Function CreateShare()
	'create share
	Set objNewShare = objWMIService.Get("Win32_Share")
	intReturn = objNewShare.Create _
	(FilePath, "WMI_SHARE", 0, 25, "")
	If intReturn <> 0 Then
	WScript.Echo "WMIEXEC ERROR: Share could not be created." & _
	vbNewLine & "WMIEXEC ERROR: Return value -> " & intReturn
	Select Case intReturn
	Case 2
	WScript.Echo "WMIEXEC ERROR: Access Denied!"
	Case 9
	WScript.Echo "WMIEXEC ERROR: Invalid File Path!"
	Case 22
	WScript.Echo "WMIEXEC ERROR: Share Name Already In Used!"
	Case 24
	WScript.Echo "WMIEXEC ERROR: Directory NOT exists!"
	End Select
	If intReturn <> 22 Then WScript.Quit 1
	Else
	WScript.Echo "WMIEXEC : Share created sucess."
	WScript.Echo "WMIEXEC : Share Name -> WMI_SHARE"
	WScript.Echo "WMIEXEC : Share Path -> " & FilePath
	End If
	End Function

MAKE AN HYPOTHESIS

HUNTING APT10 VIA WMI (T1087) & REMOTE FILE COPY (T1105)

Question	Possible Answers
What?	- Creation of new SMB share - Specific WMI command (objWMIService.Get, objNewShare.Create) - Specific strings (WMI_SHARE, WMIEXEC, Twi1ight@T00ls.Net …)
Where?	- Endpoint logs on compromised workstation/servers. - Network devices
When?	- Process creation time - Tool download - SMB share creation time
How?	- Sysmon logs (Execution) - WMI Logs (Get-WindowsFeature) - Snort/Suricata rule - YARA scanning - Proxy logs (VBS)

EXPERIMENT

ASSESS

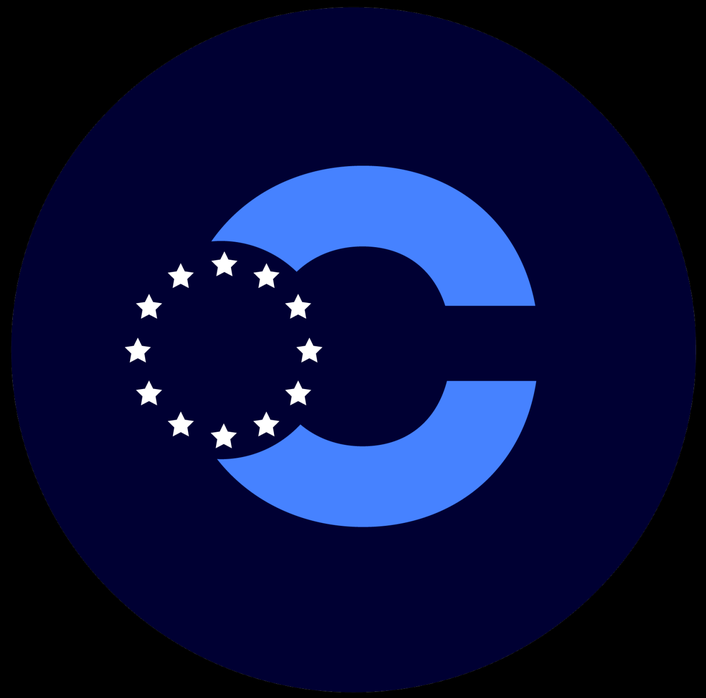
HUNTING APT10 VIA WMI (T1087) & REMOTE FILE COPY (T1105)

- Relevant activities found on existing logs
  - VBS downloaded over HTTP
- SMB share creation (EventID = 5142): too many FPs
- SMB share deletion (EventID = 5144): good indicator
- Execution in sandboxes with full logging
  - Not enough information in WMI logs
  - Process execution (4688 or Sysmon EventID =1)
  - WMI logging (EventID 4624), may be suspicious
- YARA rule for specific string is working fine

CONSOLIDATE

HUNTING APT10 VIA WMI (T1087) & REMOTE FILE COPY (T1105)

- SIGMA rules to generate the right alerts from Splunk
  - VBS download over HTTP
  - WMI remote logging
  - SMB share deletion
- Future hunt: Make statistical analysis on Process_name in 4624 events
- New YARA rule added to our repository



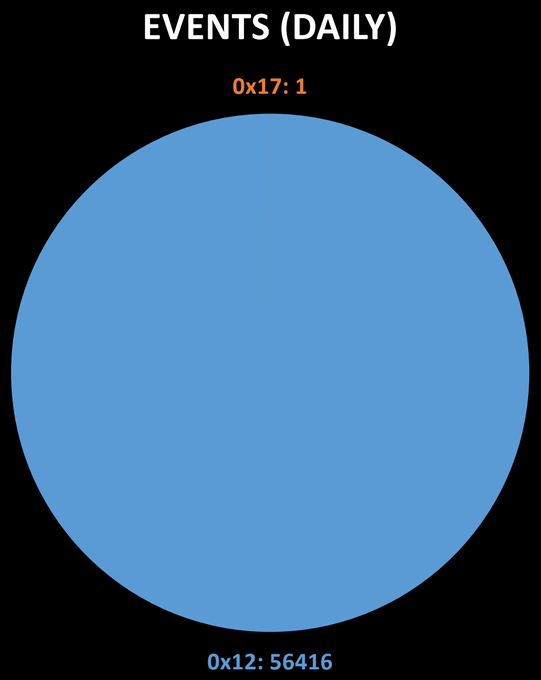
EXTRA SLIDES

… IF I MANAGED TO SPEAK FAST ENOUGH

RED VS. BLUE

- Red Team exercises are a good opportunity to assess practical threat hunting capabilities
- Red Team reports are an excellent source for performing retro-hunts
- Feedback to the Red Team is mandatory to continuously improve their future engagements, which will help you improve your threat hunting capabilities

RED VS. BLUE — RED ALERT! UNUSUAL TICKET ENCRYPTION TYPE

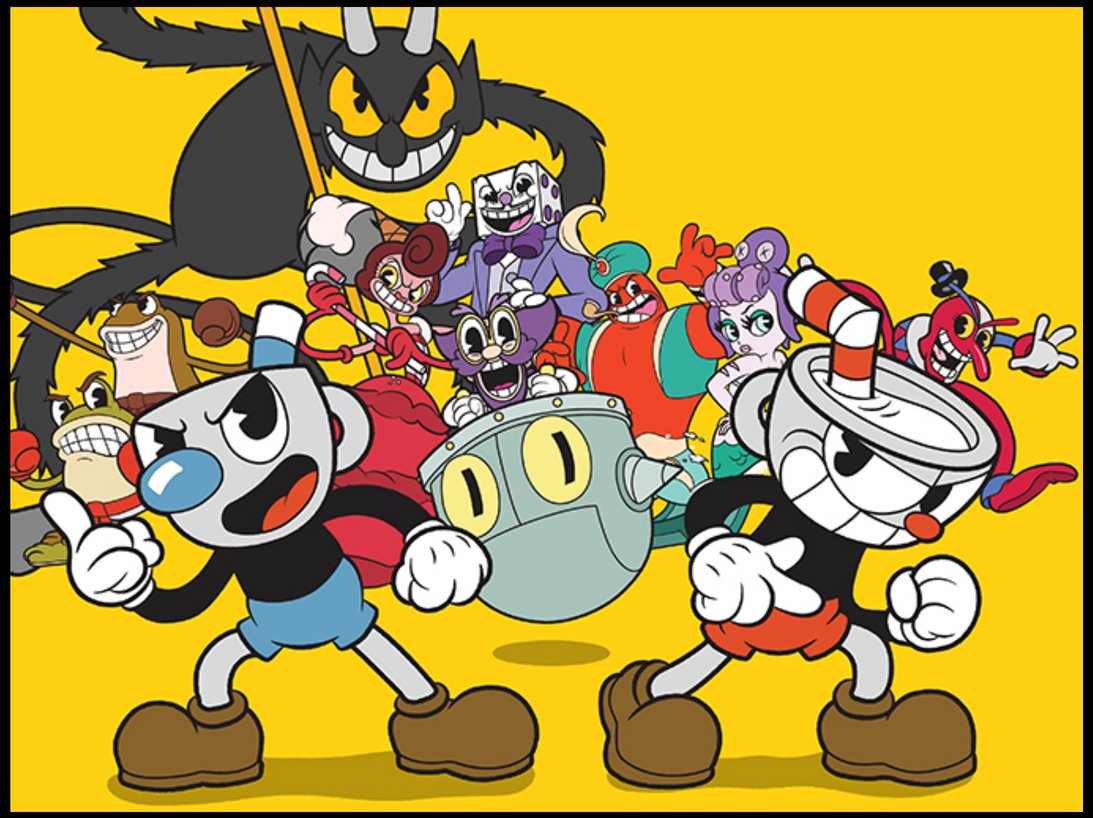


- **Ticket Encryption Type**: [Type = HexInt32]: the cryptographic suite that was used for issued TGS.

Type	Type Name	Description
0x1	DES-CBC-CRC	Disabled by default starting from Windows 7 and Windows Server 2008 R2.
0x3	DES-CBC-MD5	Disabled by default starting from Windows 7 and Windows Server 2008 R2.
0x11	AES128-CTS-HMAC-SHA1-96	Supported starting from Windows Server 2008 and Windows Vista.
0x12	AES256-CTS-HMAC-SHA1-96	Supported starting from Windows Server 2008 and Windows Vista.
0x17	RC4-HMAC	Default suite for operating systems before Windows Server 2008 and Windows Vista.
0x18	RC4-HMAC-EXP	Default suite for operating systems before Windows Server 2008 and Windows Vista.
0xFFFFFFFF or 0xffffffff	-	This type shows in Audit Failure events.

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4769

WUT?!? (A SHORT STORY OF THE LIFE OF A BLUE TEAM)



- I started working on an incident
- I wasn't aware of any ongoing Red Team exercise
- So I asked my Red Team devilish friends for advice
- What kind of tool was used by this sophisticated, advanced, next-generation, cyber-earth chattering, probably not flexitarian threat actor?
- Oh… wait… it was us

THINK CONSTITUENT

CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CREATE VALUE