PURPLE TEAMING

Demystifying purple teaming, emulating our first threat for better defenses

Samuel Rossier
BlackHat.971 Chapter Meet Up
27.07.2022, Dubai

(SAM㉿BHMEA.971)-[~]
$ WHOAMI

- Samuel Rossier
- SOC Lead, SANS Teaching Assistant ICS515
- Twitter: @sam0x90

┌──(SAM㉿BHMEA.971)-[~]
└─$ WHO

- How many work in SOC? DFIR?
- How many work in CTI? Or malware analysis?
- How many Red Teamer/Pentester?
- Who already did a purple teaming/adversary emulation exercise?

AGENDA

1 Today’s context – Red ⚔ Blue

2 New mindset – Red 💗 Blue

3 Threat Management – How to improve?

4 Cyber Threat Intelligence - The glue between both worlds

5 Purple Teaming - How does it work?

6 Walkthrough – Our first purple teaming exercise

1. TODAY'S CONTEXT

Red ⚔ Blue

1. TODAY'S CONTEXT – RED VS. BLUE

- Pentest is not the real world #scope
- Objectives are not aligned
- The success of one makes the other one's failure
- Lack of collaboration and feedback
- Lack of visibility on controls' efficiency
- What's my ROI?

2. PURPLE TEAMING

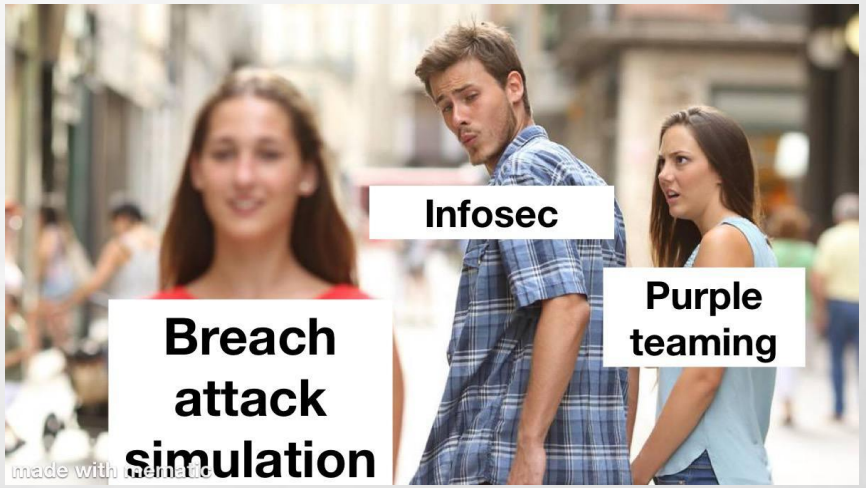
Red ♥ Blue

2. NEW MINDSET – PURPLE TEAMING CONCEPT

- No official definition
- **Virtual team**, not yet another new dedicated team
- 4 Roles: Coordinator, CTI, Red and Blue
- **CTI is the bridge between Red and Blue**
- **Collaborative** and transparent in nature, as everyone sit at the same table
- **Same goal, train and improve organization's defenses**

2 PURPLE TEAMING – OTHER RELATED CONCEPTS

- Breach Attack Simulation
- Adversary simulation vs. Adversary emulation
- Threat-informed defense

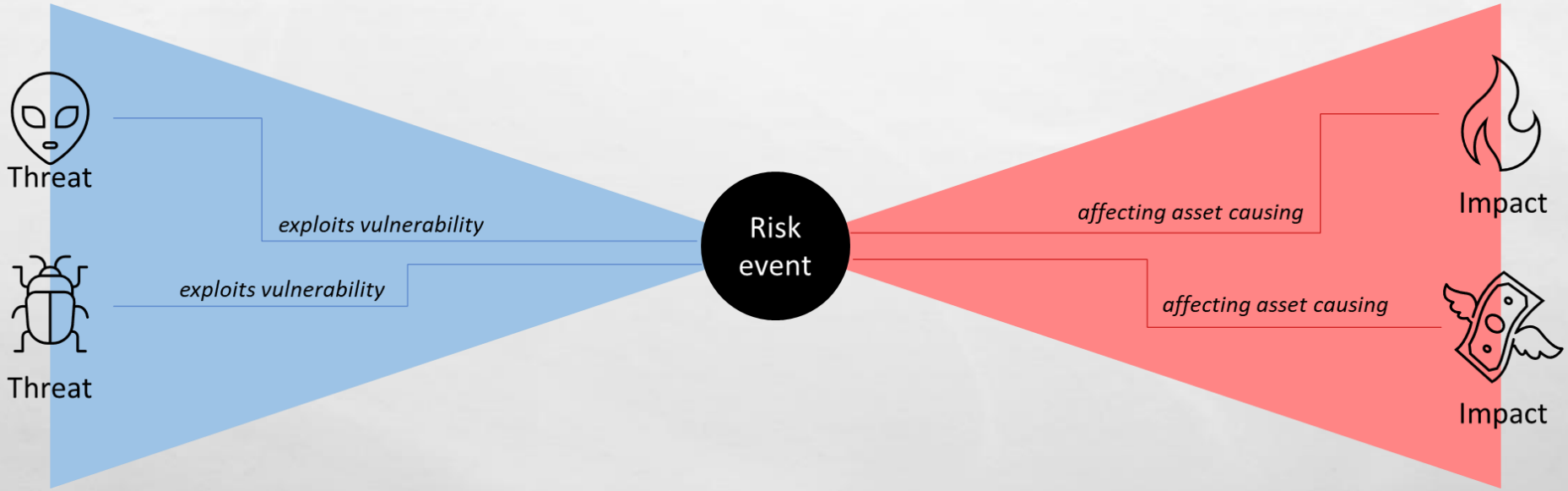


3. THREAT MANAGEMENT

How to improve?

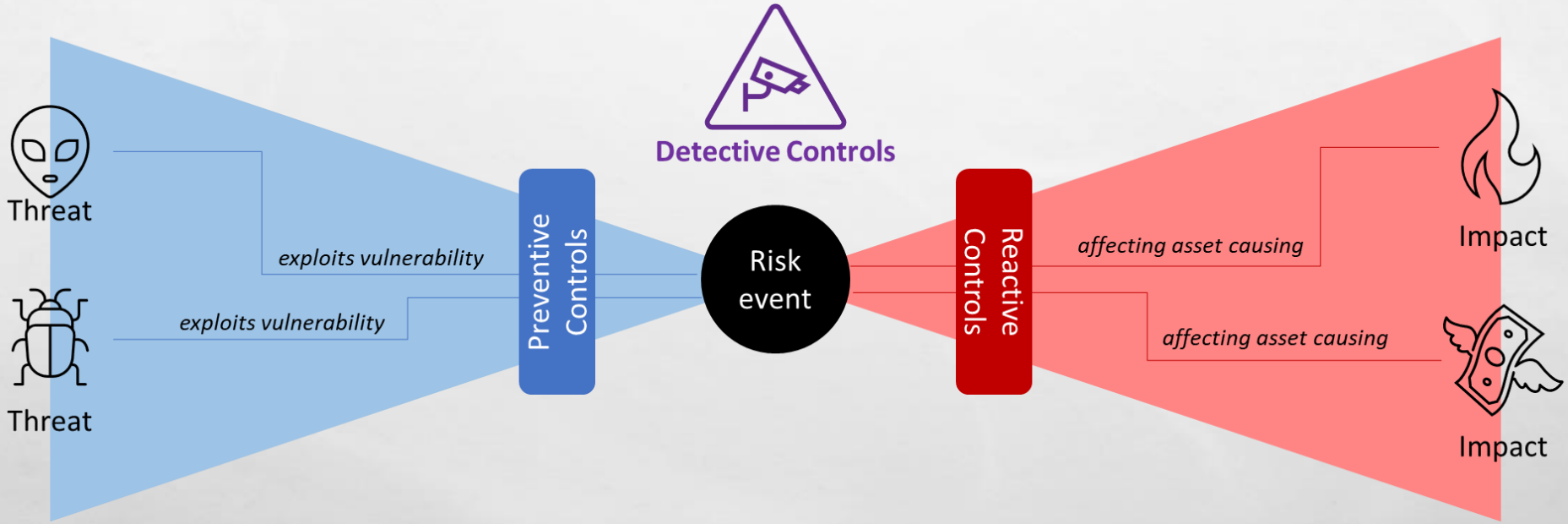
3. THREAT MANAGEMENT

Bow Tie view of a risk event



3. THREAT MANAGEMENT

Bow Tie view of a risk event **with security controls**



3. THREAT MANAGEMENT

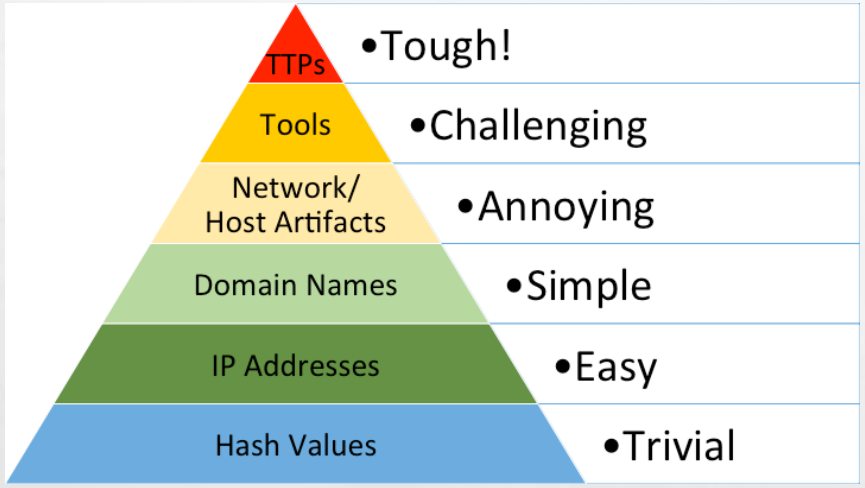
Some resources to help us cherry pick tips and improvements

Prevention	Detection	Response
• **MITRE ATT&CK Mitigation** • CIS Benchmark • ATC Mitigation • Vendor’s hardening guidelines	• **TaHiTI methodology** • Threat Hunter Playbook • **MaGMa framework** • **DeTT&CT** • Palantir Alerting and Detection Strategies Framework • **Sigma** • MITRE CAR • **Github** (Elastic, Splunk, Microsoft, Google Chronicles, FalconForce, TheDFIRReport, etc.)	• NIST Computer Security Incident Handling Guide • SANS Incident Handler's Handbook • **ATC RE&CT**

Honorable mention: MITRE D3FEND, MITRE Engage

4. CYBER THREAT INTELLIGENCE

The glue between both worlds



- Why CTI?
  - So many threats, how to prioritize defenses?
  - Focus on what matters, what will likely hit us
- Pyramid of pain
- STIX and MITRE ATT&CK as a common language between Red and Blue
- 3 types: Strategic, Operational, Tactical
- TTP
  - Tactic, why?
  - Technique, what?
  - **Procedure, how?**

4. CTI – THE GLUE BETWEEN BOTH WORLDS

4. CTI – THE GLUE BETWEEN BOTH WORLDS

CTI is not a tool or just IoCs, **it is a process**

1. PLANNING AND TARGETING

2. PREPARATION AND COLLECTION

3. PROCESSING AND EXPLOITATION

4. ANALYSIS AND PRODUCTION

5. DISSEMINATION AND INTEGRATION

6. EVALUATION AND FEEDBACK

4. CTI – THE GLUE BETWEEN BOTH WORLDS

SOME RESOURCES TO GET STARTED

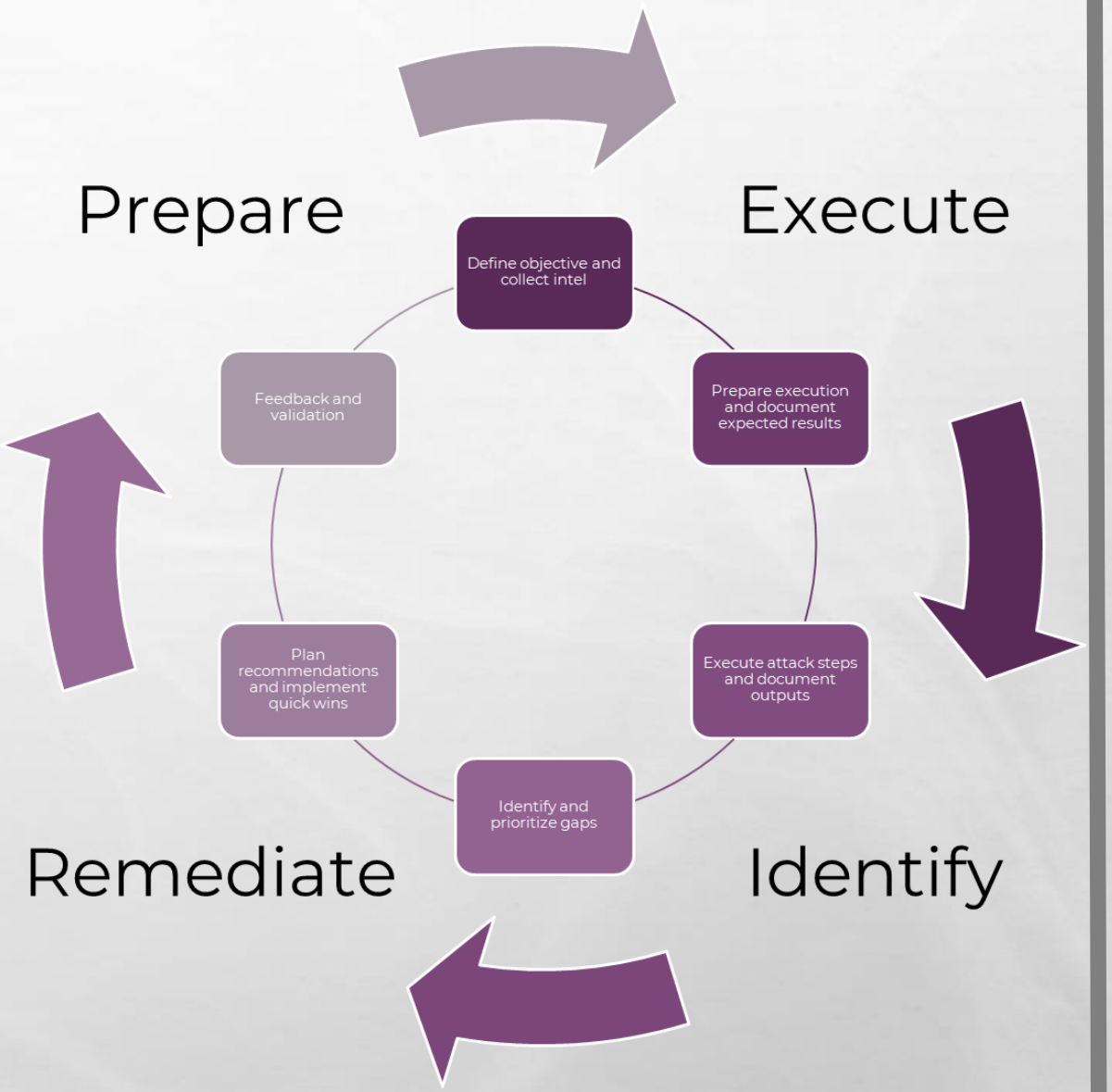
Topic	Collection source	Link
Overall trends/Various	Checkpoint Weekly Intelligence Report Avertium weekly threat report Anomali Weekly Cyber Watch Threat Source newsletter Weekly NCSC TheHackerNews TheRecord SecureList This Week/Month in 4n6	https://research.checkpoint.com/category/threat-intelligence-reports/ https://www.avertium.com/resources https://www.anomali.com/blog/category/anomali-cyber-watch https://blog.talosintelligence.com/search/label/Threat%20Source%20newsletter https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/wochenrueckblicke.html https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports https://thehackernews.com/ https://therecord.media/ https://securelist.com/ https://thisweekin4n6.com/
TTP	MITRE ATT&CK TheDFIRReport RedCanary Intelligence Insights Unit42 ATOMs Trellix monthly threat report	https://attack.mitre.org/ https://thedfirreport.com/ https://redcanary.com/blog/ https://unit42.paloaltonetworks.com/atoms/ https://www.trellix.com/en-ca/threat-center/threat-reports.html
Vulnerabilities	CISA CVETrends	https://www.cisa.gov/known-exploited-vulnerabilities-catalog https://cvetrends.com/
Malware	Malware Hunters AnyRun Hatching Triage Malpedia	https://malwarehunters.org/ https://any.run/malware-trends/ https://hatching.io/blog/ AND https://tria.ge/kb/ https://malpedia.caad.fkie.fraunhofer.de/
Vendors	Mandiant, PAN Unit42, Crowdstrike, Kaspersky...	-

5. PURPLE TEAMING

How does it work?

5. PURPLE TEAMING – PROCESS

1. Define objective and collect intel
2. Prepare execution and document expected results
3. Execute attack steps and document outputs
4. Identify gaps and prioritize
5. Plan recommendations and implement quick wins
6. Feedback and validation



5. PURPLE TEAMING – OTHER RESOURCES

- Framework
  - Scythe – Purple Teaming Exercise Framework
- Emulation Libraries
  - Scythe - Community Threats Library
  - Center for threat-informed Defense - Adversary Emulation Library
- Courses
  - MITRE ENGENUITY - MITRE ATT&CK Defender™ (MAD) - Adversary Emulation Methodology
  - AttackIQ Academy
  - SANS SEC599 and SEC699 (Purple Summit)

6. WALKTHROUGH

Our first purple teaming exercise – Qakbot

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

Internal

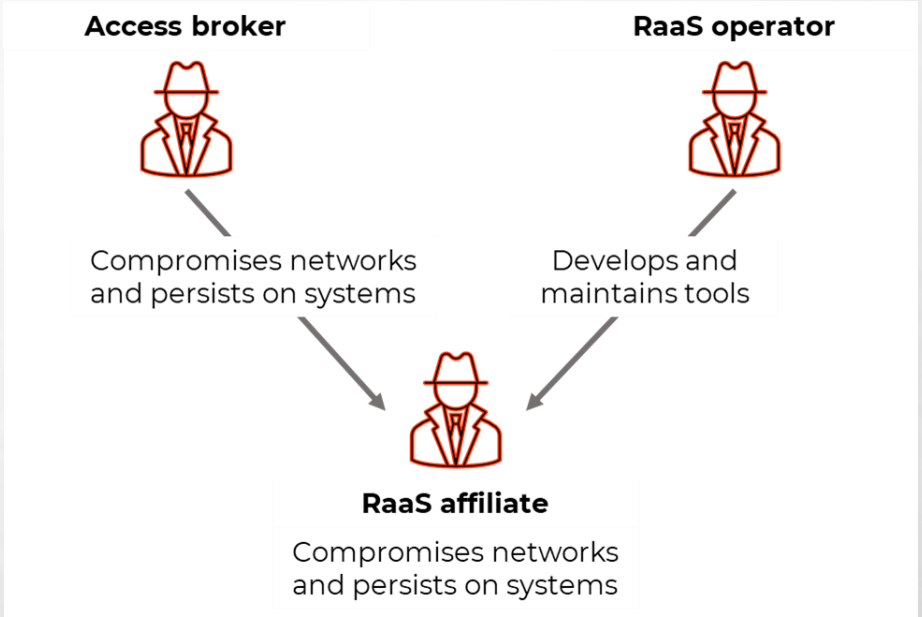
- Our Management is worried about ransomware
- Our CTI briefed us on a recent intel on RaaS from MS (mixed kill chain)
- Asset owner remembers a Qakbot incident

External

- AB use Qakbot, and it seems trendy
- All those AB malwares shared lots of common techniques (Trickbot, IcedId, Emotet, etc.)

Decision

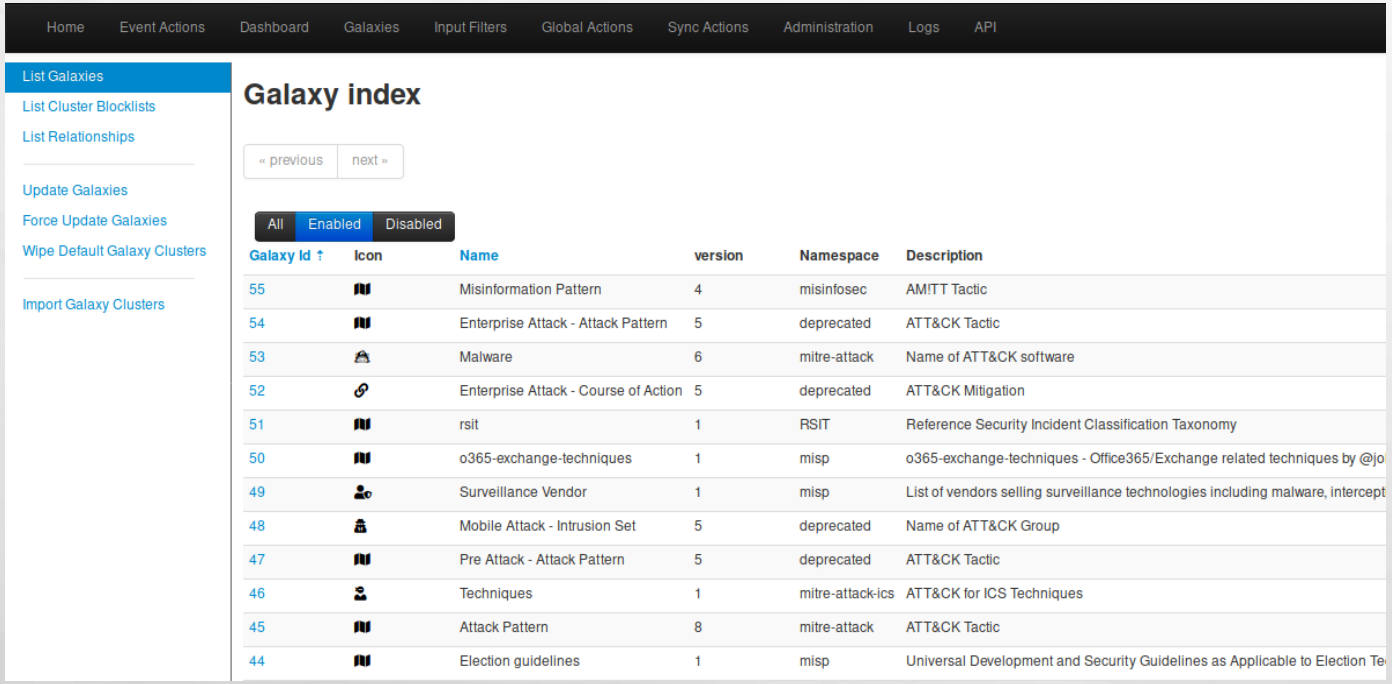
- Evaluate, fix and improve defenses against typical AB malware
- Focus on a malware instead of a threat actor as they are changing affiliation
- Focus is de facto on the beginning of the kill chain, simpler to emulate but ignoring half of the kill chain

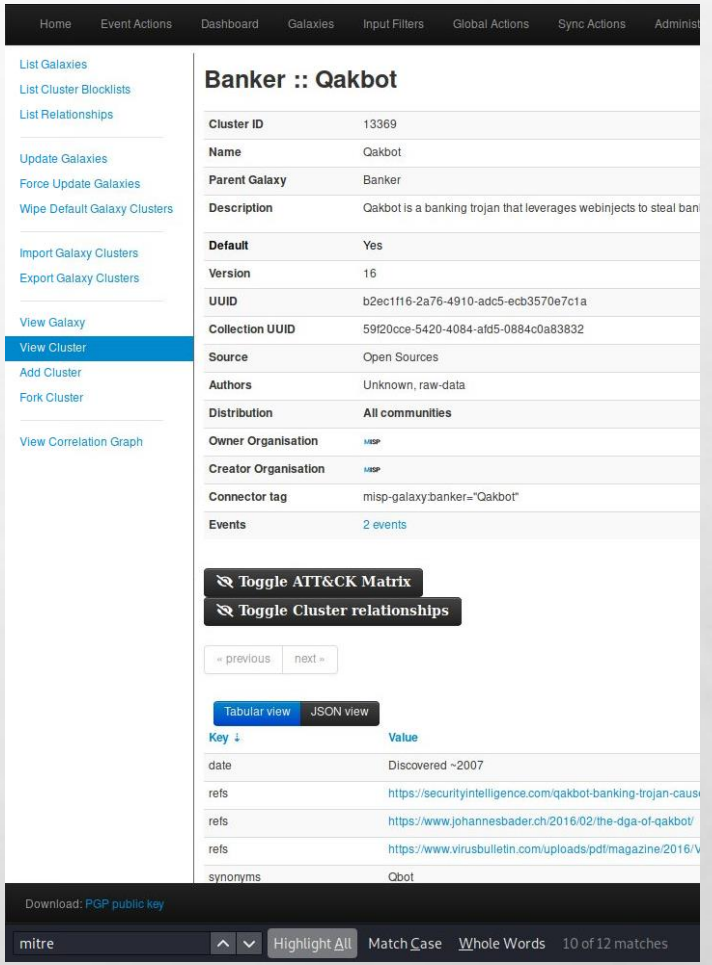


Simplified figure from: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

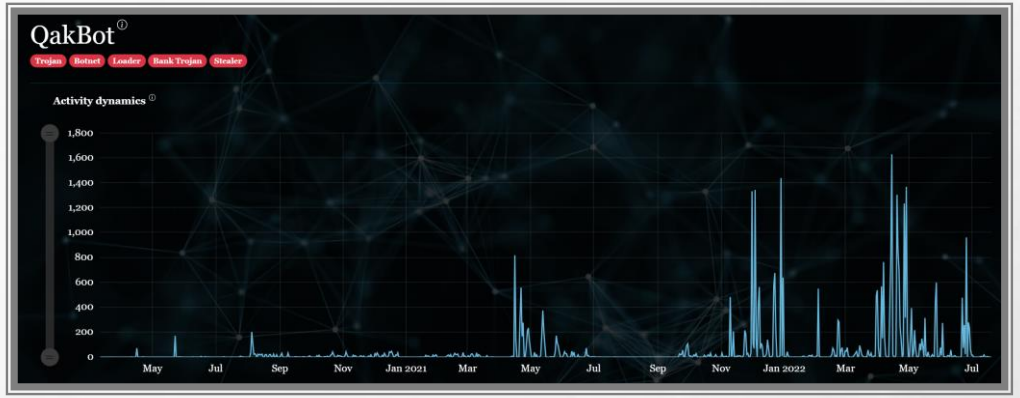
6.1 DEFINE OBJECTIVE AND COLLECT INTEL

Only 2 old MISP events, not trendy…



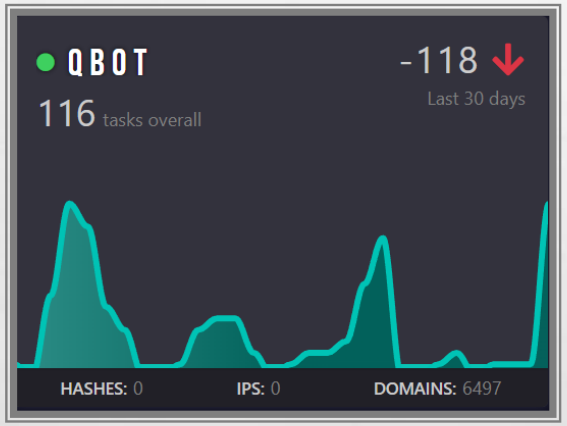


6.1 DEFINE OBJECTIVE AND COLLECT INTEL



https://malwarehunters.org/infographics/malware%3Dqakbot/

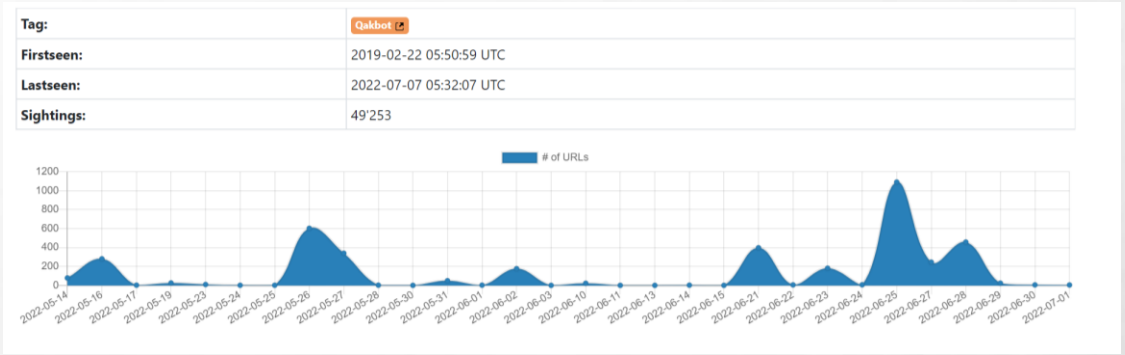
...wow, here it seems trendy!



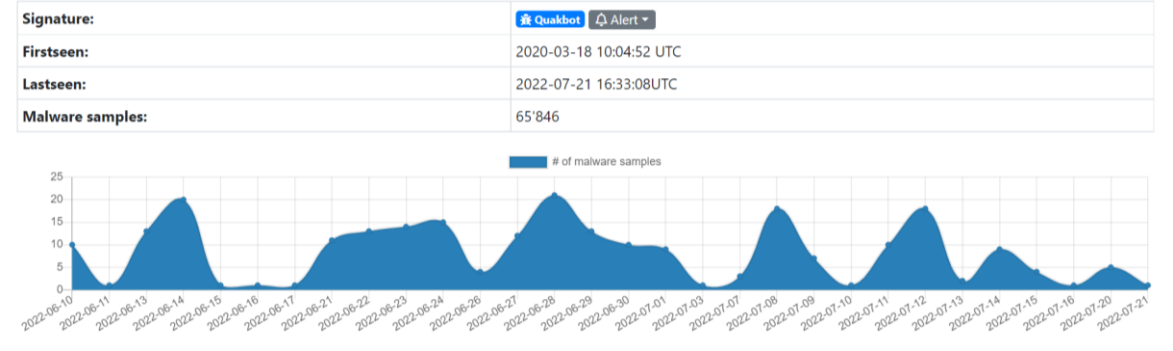
https://any.run/malware-trends/

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

What about here?
Trendy? Not trendy?



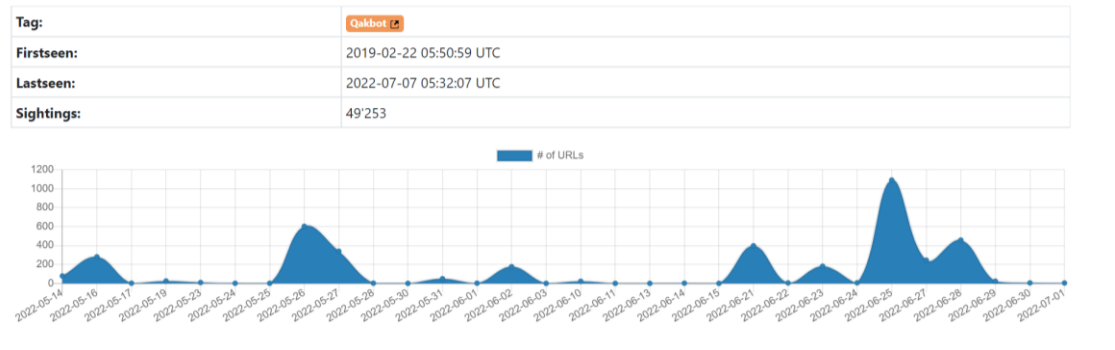
https://urlhaus.abuse.ch/browse/tag/Qakbot



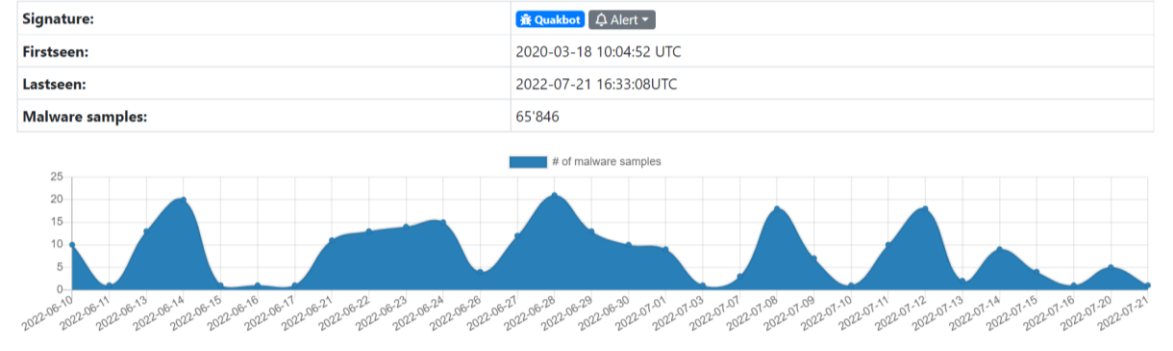
https://bazaar.abuse.ch/browse/signature/Quakbot/

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

What about here?
Trendy? Not trendy?



https://urlhaus.abuse.ch/browse/tag/Qakbot



https://bazaar.abuse.ch/browse/signature/Quakbot/

Beware the collection bias!

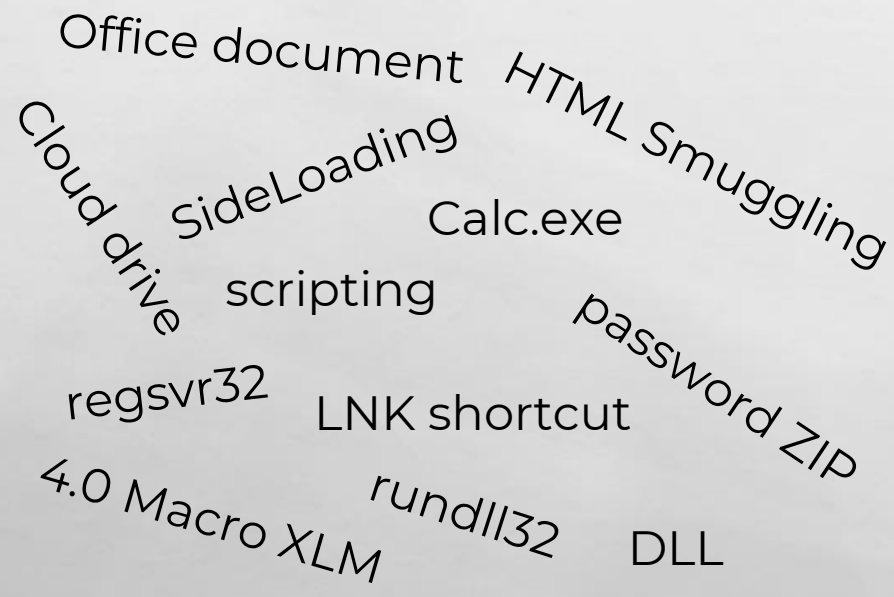
6.1 DEFINE OBJECTIVE AND COLLECT INTEL

To emulate Qakbot, now **we need the P from TTP...**

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

To emulate Qakbot, now **we need the P from TTP...**

... which comes in different flavors with **Qakbot** (TR and Obama)



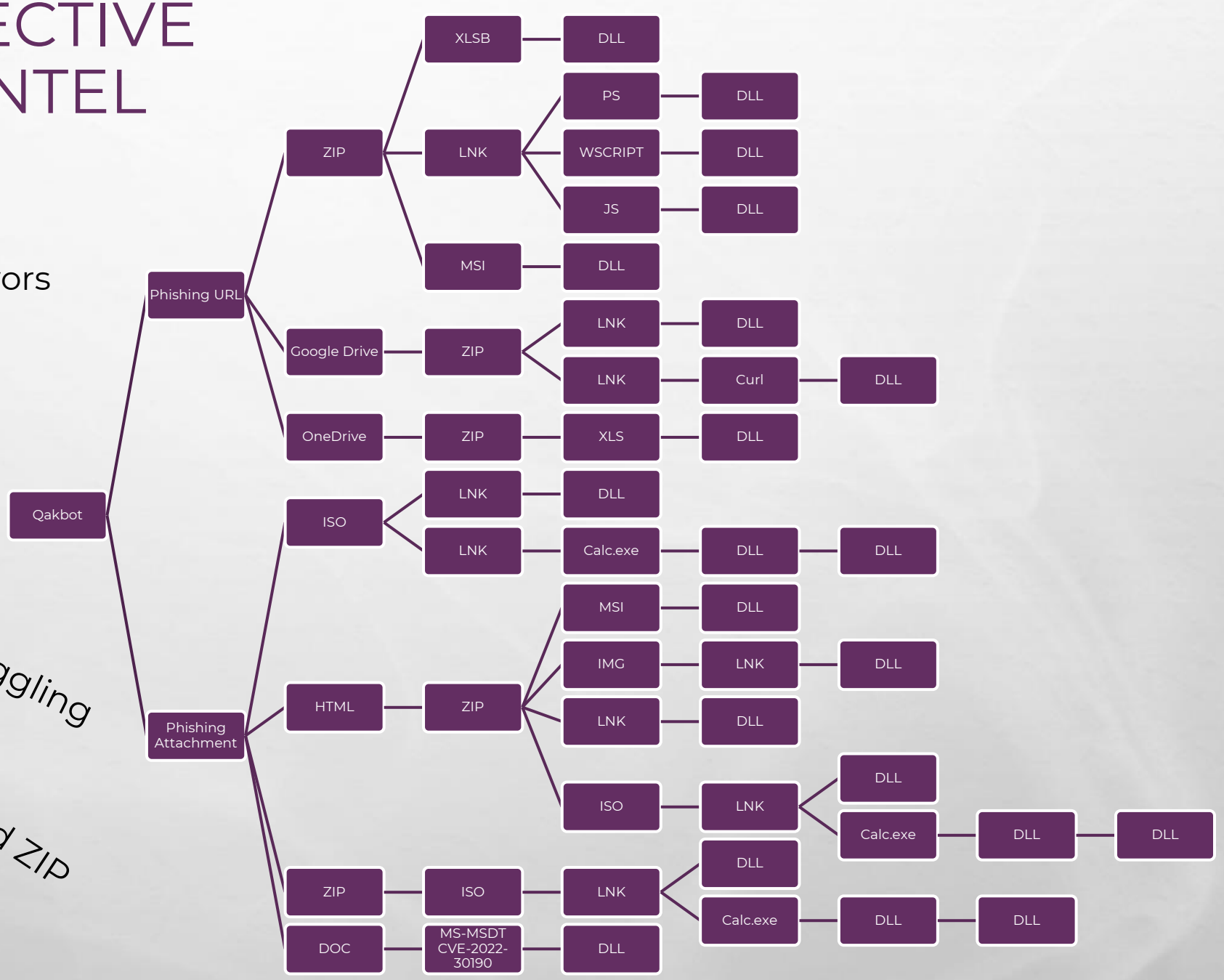
https://twitter.com/Sam0x90/status/1552011547974696960

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

To emulate Qakbot, now **we need the P from TTP...**

... which comes in different flavors with **Qakbot** (TR and Obama)

Office document
HTML Smuggling
Cloud drive
SideLoading
Calc.exe
scripting
password ZIP
regsvr32
LNK shortcut
4.0 Macro XLM
rundll32
DLL

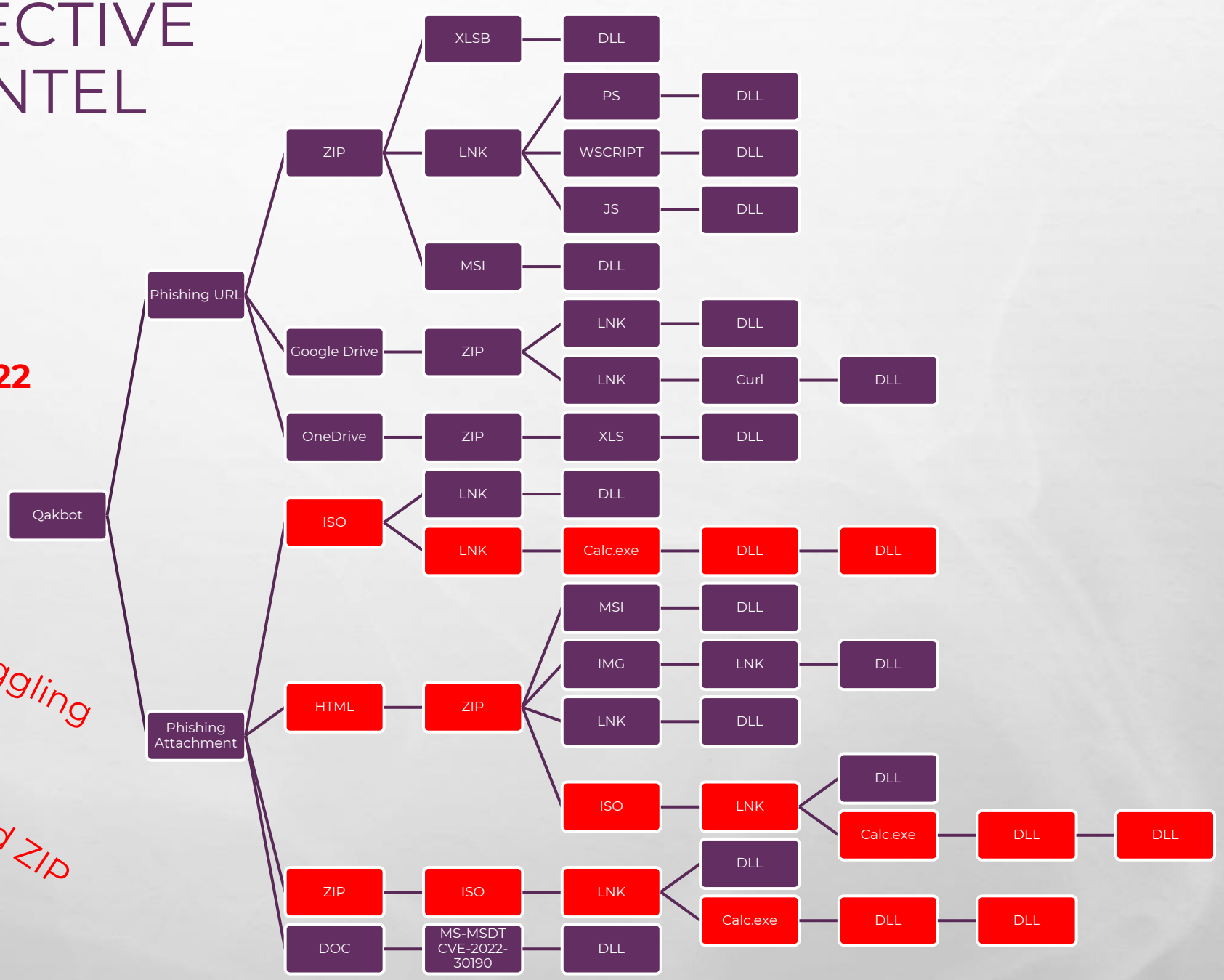


https://twitter.com/Sam0x90/status/1552011547974696960

6.1 DEFINE OBJECTIVE AND COLLECT INTEL

Latest TTPs from Mid-July 2022

Office document
HTML Smuggling
Cloud drive
SideLoading
Calc.exe
scripting
password ZIP
regsvr32
LNK shortcut
4.0 Macro XLM
rundll32
DLL



https://twitter.com/Sam0x90/status/1552011547974696960

6.2 PREPARE EXECUTION AND DOCUMENT EXPECTED RESULTS

So,

- we selected the **latest TTP from Qakbot**
- We obtained **procedure-level** intel

It's our first exercise, **keep it simple**

Let’s prepare the steps!

6.2 PREPARE EXECUTION AND DOCUMENT EXPECTED RESULTS

(Simplified) Qakbot Emulation Plan, Excel-style

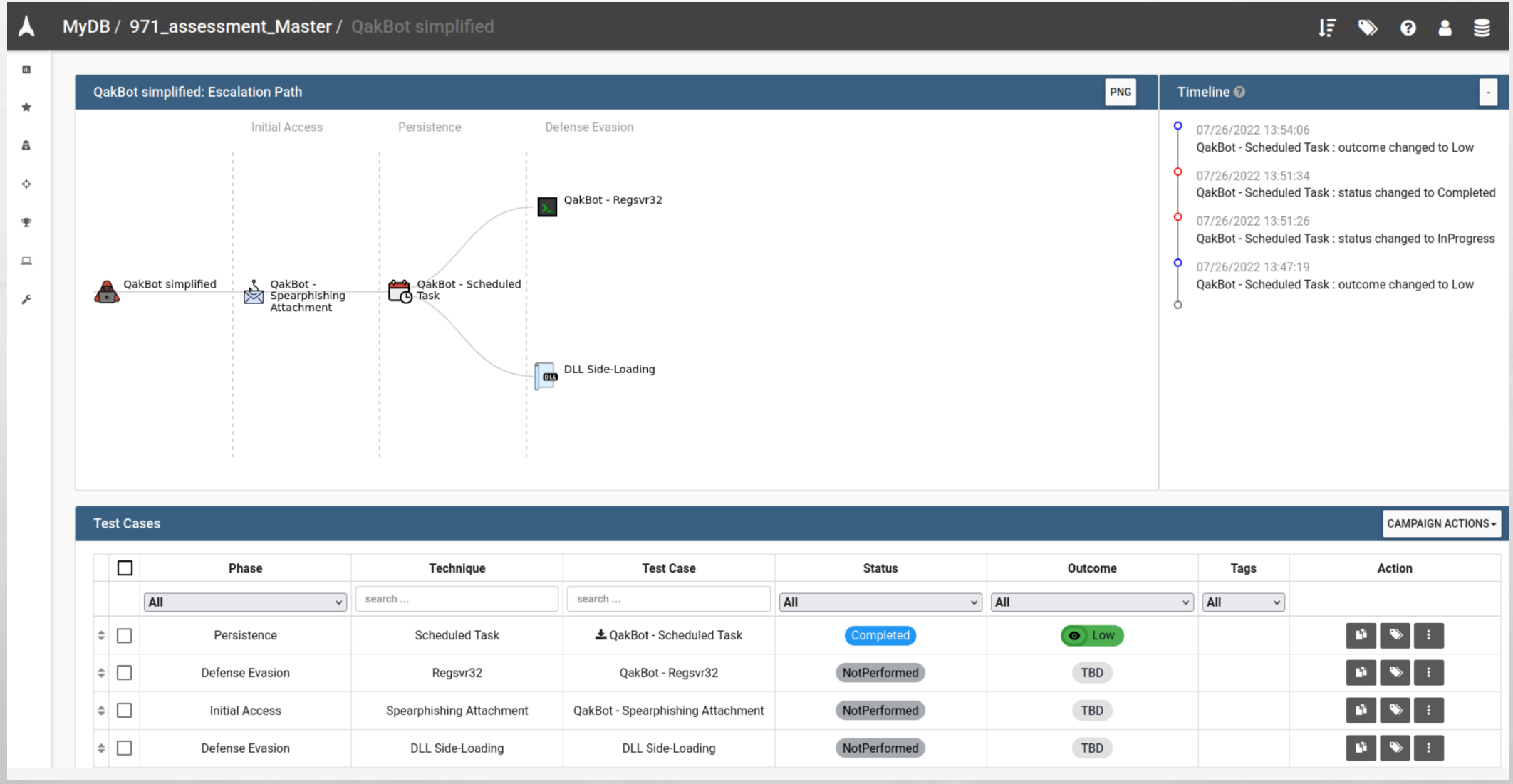
Emulation Plan

CTI Team		CTI and Red Team	Red Team	Red & Blue Team	Blue Team		ALL
Tactic	**Technique**	**Procedure description**	**Procedure replay**	**Control/Mitigation**	**Type**	**Effectiveness**	**Comment**
TA0001 Initial Access	T1566 Phishing	Email containing password-protected ZIP file	1. Copy LNK, calc.exe and side-loaded DLL into an ISO file (payload not included) 2. ZIP with password the ISO file 3. Send email with password in email body and ZIP as attachment	Mail GW antispam	Prevention		Final payload not included which could biased the test
				Mail GW password archive decryption	Prevention		
				Mail GW sandbox	Prevention		
				Outlook warning banner	Prevention		
TA0005 Defense Evasion	T1574.002 Hijack Execution Flow: DLL Side-Loading	LNK file looking like a PDF will execute cmd.exe, which will execute calc.exe. The latter will side load a hidden DLL within the same folder	1. Replacing WindowsCodecs.dll by legit DLL (URLMon.dll for example) 2. Use same LNK as malware sample 3. Use Win7 calc.exe (same as malware sample) 4. Double click the LNK	Antivirus/EPP HIPS engine	Telemetry		Emulation could be improved to include creation of shell. Objective here is mainly to see if telemtry exist
				Sysmon	Telemetry		
				EDR	Detection		
TA0002 Execution TA0003 Persistence	T1053.005 Scheduled Task	Qakbot creates schedule tasks to maintain persistence	1. Run the following command in a cmd.exe *schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /Z /ST 22:43 /tn heyjijua /ET 22:54 /tr "powershell.exe -encodedCommand cgBlAGcAcwB2AHIAMwAyAC4AZQB4AGUAIAAiAEMAOgBcAFUAcwBlAHIAcwBcAEEAZABtAGkAbgBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwAXABUAGUAbQBwAFwAbwB1AHQAXAAxADAAMgA3ADUANQ*	SIEM use case #34	Detection		
				Windows Log 4688 / Sysmon 1	Telemetry		
				Windows Log 4698	Telemetry		
				SIEM use case #23	Detection		

https://github.com/PacktPublishing/Purple-Team-Strategies/blob/main/Chapter-11/Purple_Teaming_Report_v1.0.xlsx

6.2 PREPARE EXECUTION AND DOCUMENT EXPECTED RESULTS

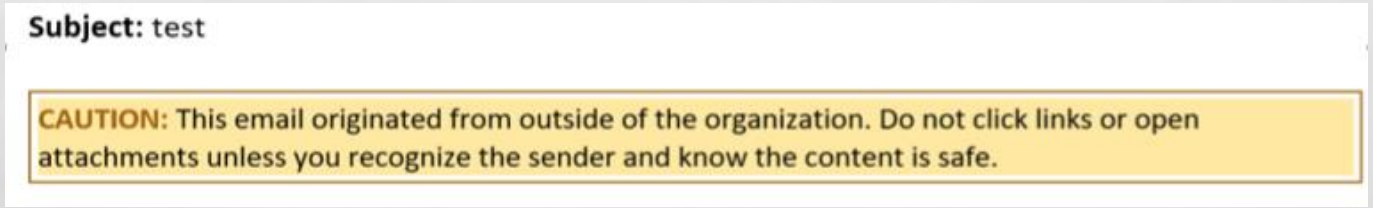
(Simplified) Qakbot Emulation Plan, Vectr-style



6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

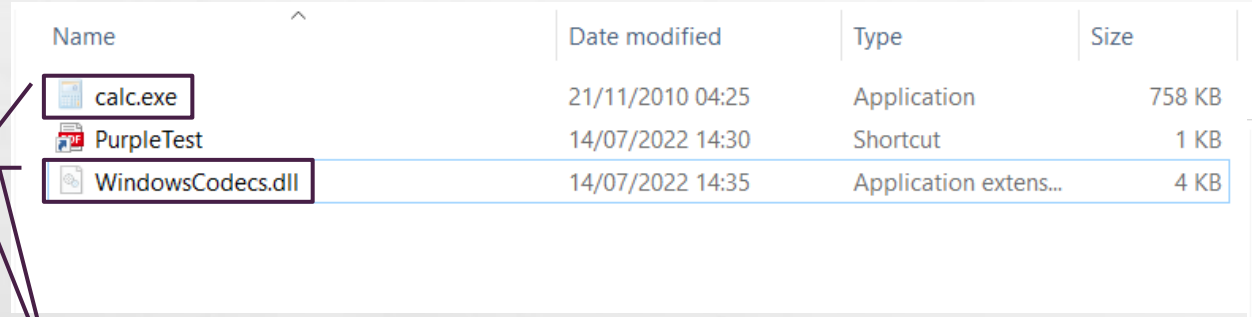
T1566.001: Spearphishing Attachment

- Mail GW was able to decrypt but antivirus failed
- We confirmed that the Outlook Banner is there on the email

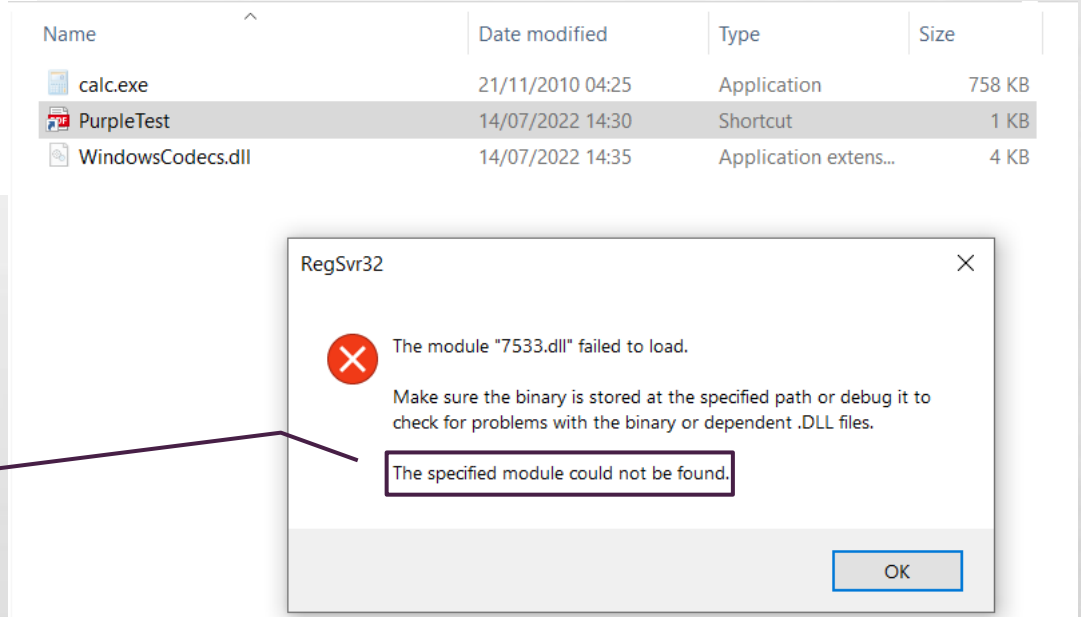


6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

T1574.002 Hijack Execution Flow: DLL Side-Loading



Hidden files



We could/should have loaded a legit DLL to emulate properly #Improvement

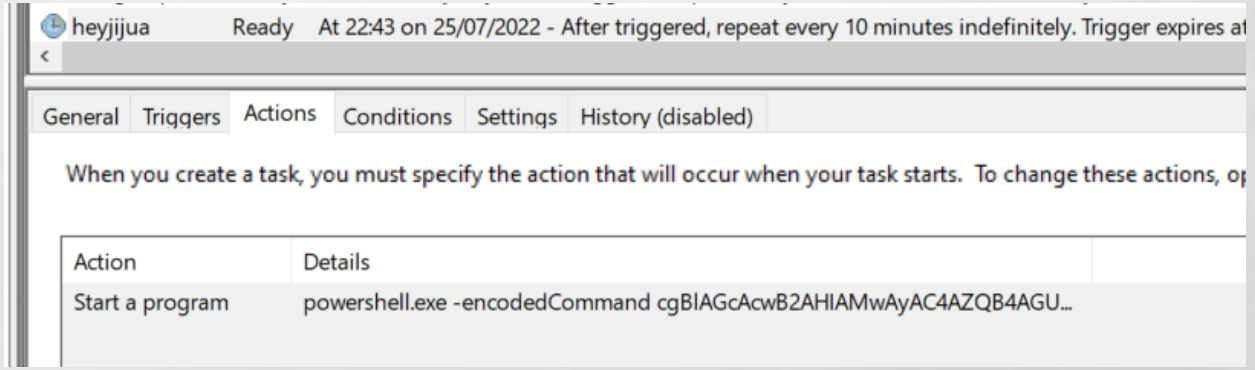
6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

T1053.005 Scheduled Task/Job: Scheduled Task

```
C:\WINDOWS\system32>schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /Z /ST 22:43 /tn heyjijua /ET 22:54 /tr "powershell.e
xe -encodedCommand cgBlAGcAcwB2AHIAMwAyAC4AZQB4AGUAIAAiAEMAOgBcAFUAcwBlAHIAcwBcAEEAZABtAGkAbgBcAEEAcABwAEQAYQB0AGEAXABMA
G8AYwBhAGwAXABUAGUAbQBwAFwAbwB1AHQAXAAxADAAMgA3ADUANQAuAGQAbABsACIA" /SC ONCE
SUCCESS: The scheduled task "heyjijua" has successfully been created.

C:\WINDOWS\system32>
```

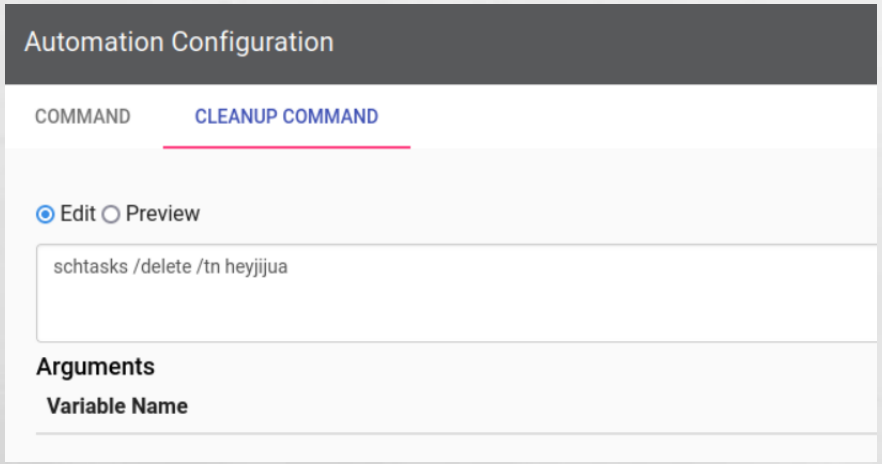
Manual execution

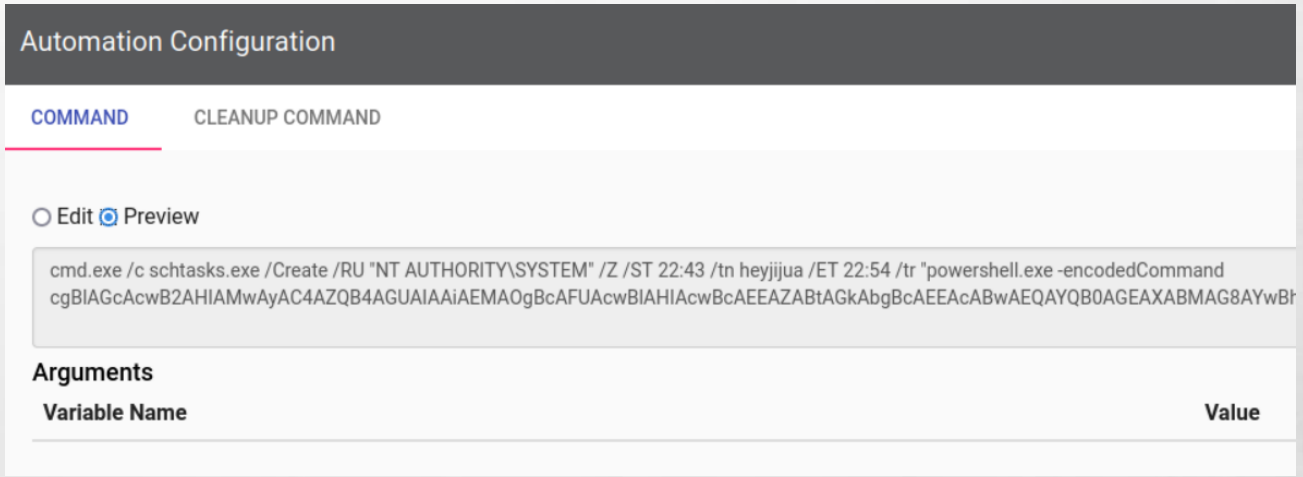


6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

T1053.005 Scheduled Task/Job: Scheduled Task

Vectr allows for automation, execution and cleanup





We could/should have leveraged Atomic Red Team

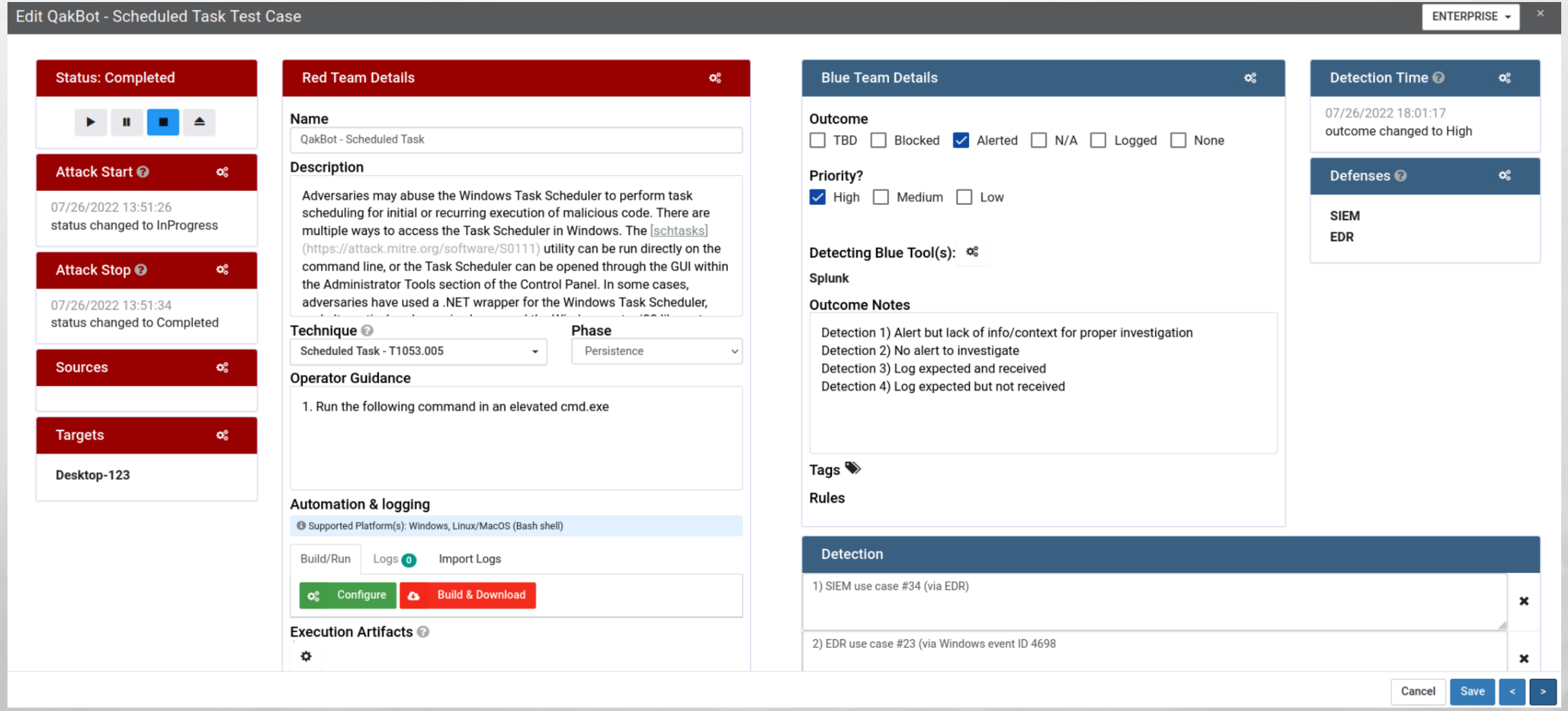
6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

LET'S DOCUMENT THE RESULTS, EXCEL-STYLE

Red & Blue Team	Blue Team	
Control/Mitigation	**Type**	**Effectiveness**
Mail GW antispam	Prevention	Expected, ineffective
Mail GW password archive decryption	Prevention	Expected, effective
Mail GW sandbox	Prevention	Expected, ineffective
Outlook warning banner	Prevention	Expected, effective
Antivirus/EPP HIPS engine	Telemetry	Expected, ineffective
Sysmon 7	Telemetry	Expected, ineffective
Sysmon 11	Telemetry	Not-expected, effective
EDR	Detection	Expected, ineffective
SIEM use case #34	Detection	Expected, partially effective
Windows Log 4688 / Sysmon 1	Telemetry	Expected, effective
Windows Log 4698	Telemetry	Expected, ineffective
SIEM use case #23	Detection	Expected, ineffective

6.3 EXECUTE ATTACK STEPS AND DOCUMENT OUTPUTS

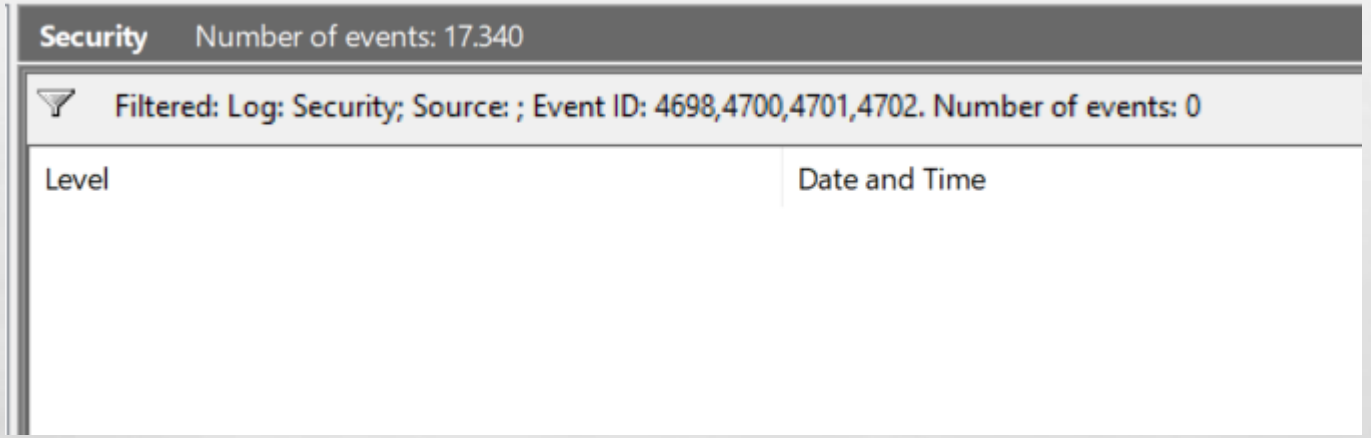
Let’s document the results, Vectr-style



6.4 IDENTIFY GAPS AND PRIORITIZE

Quick win #1:

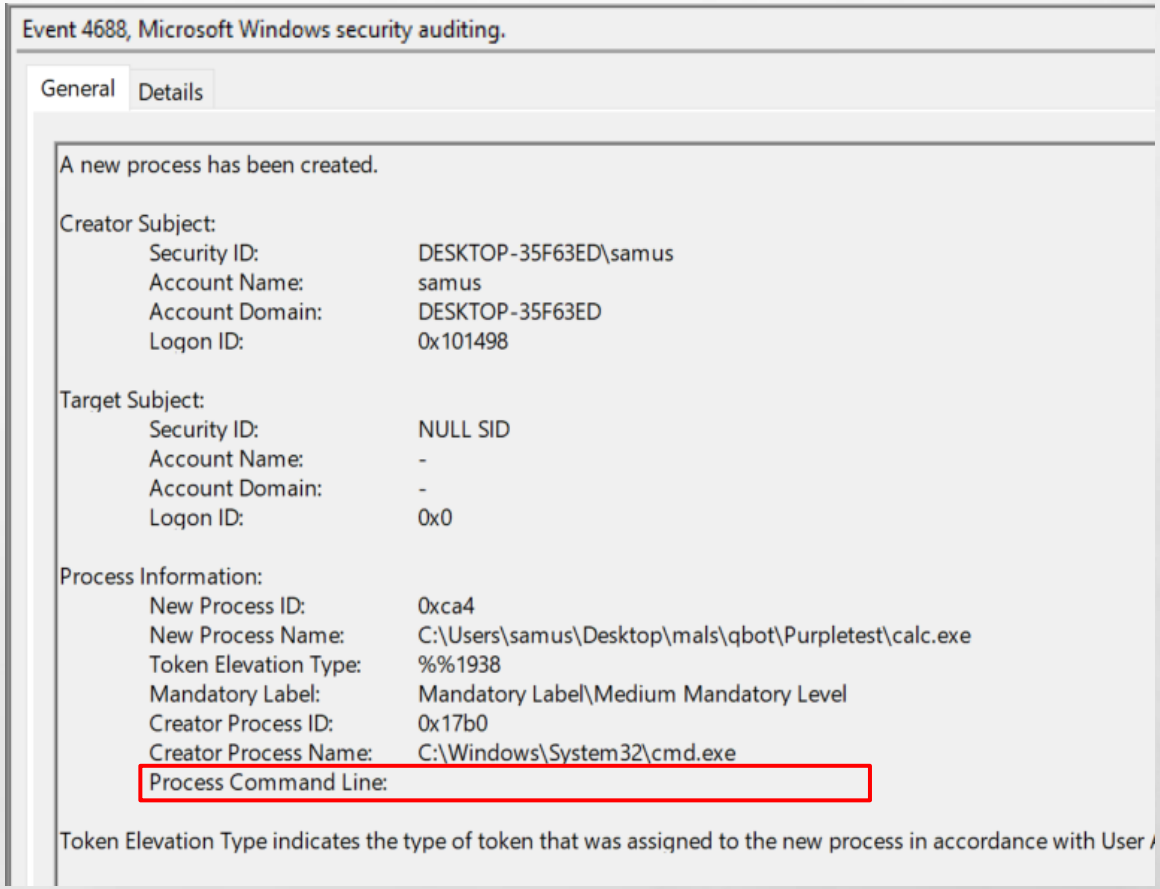
Audit policy to improve, no logging of schedule task creation, update and deletion



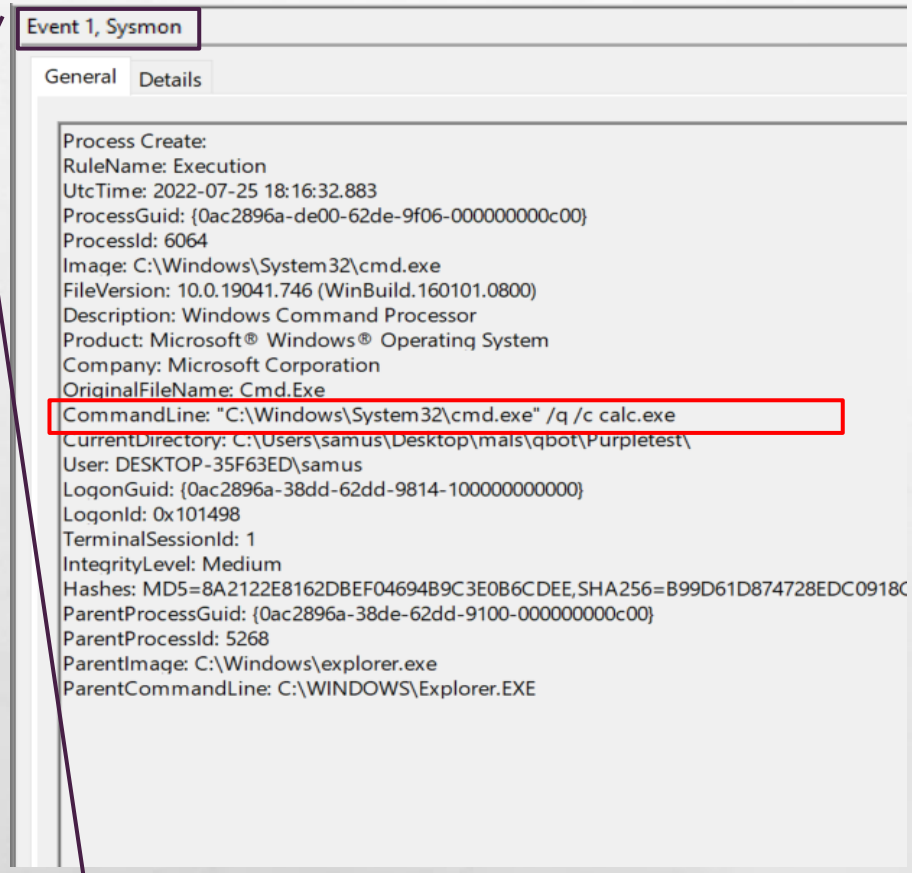
6.4 IDENTIFY GAPS AND PRIORITIZE

Quick win #2:

No command line auditing enabled

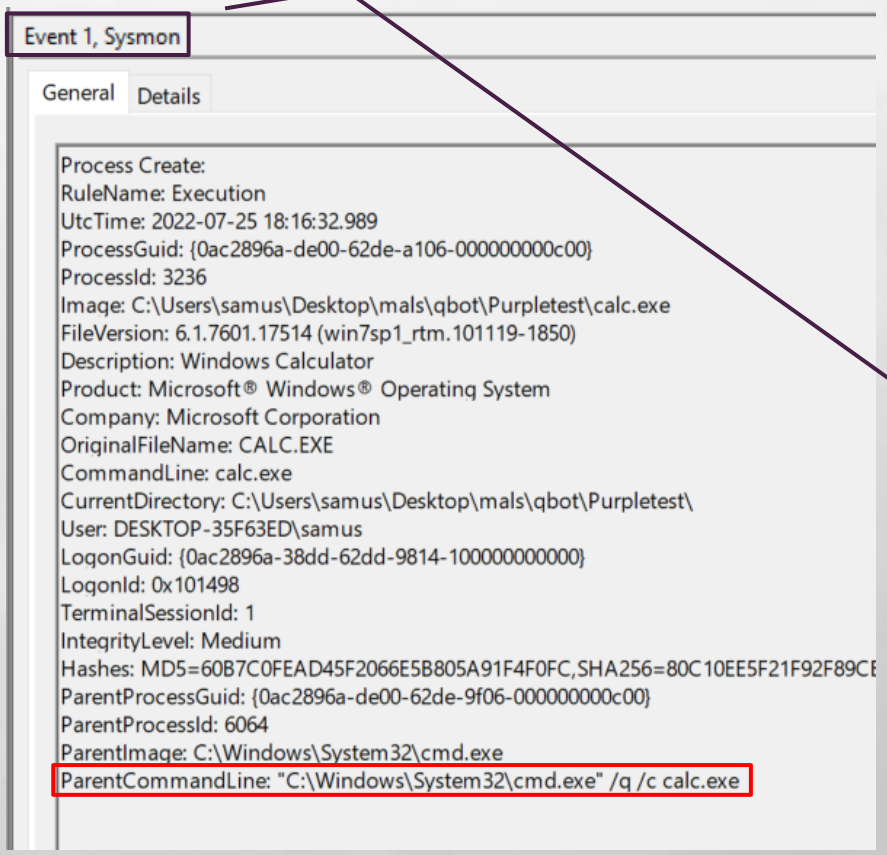


6.4 IDENTIFY GAPS AND PRIORITIZE



Parent cmd.exe process creation

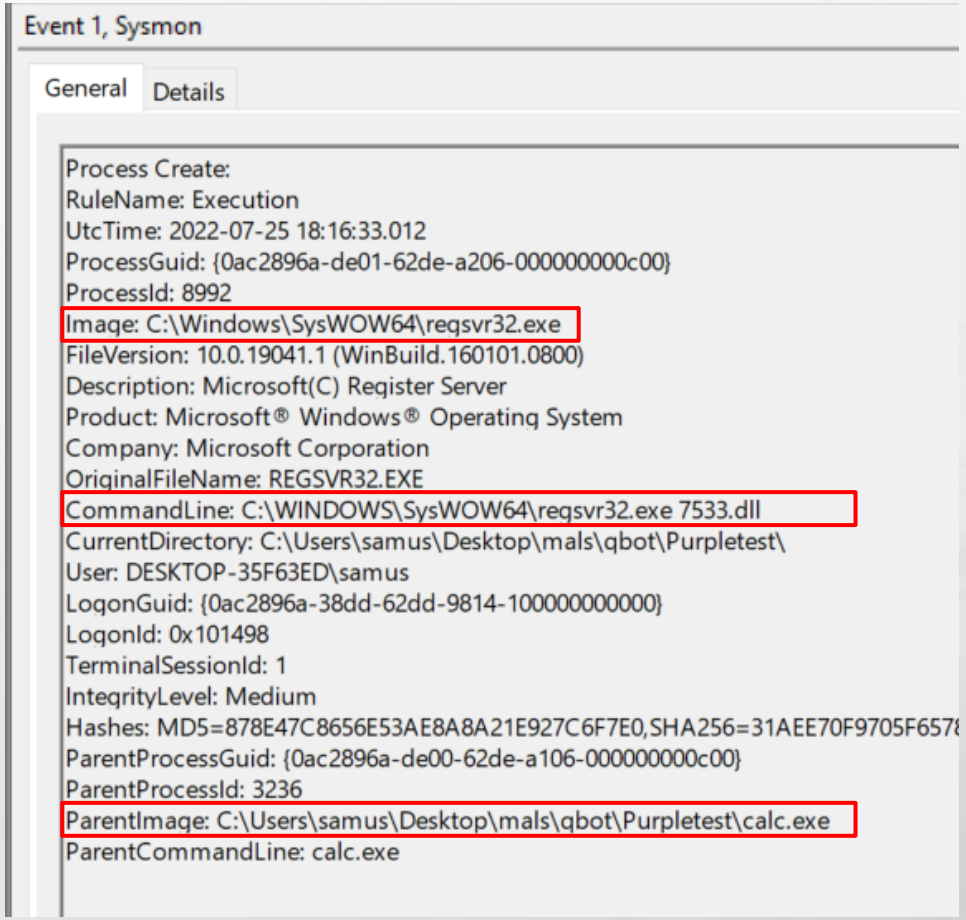
Detection opportunity #1:
Process cmd.exe creating process calc.exe with /q /c parameters



Child calc.exe process creation

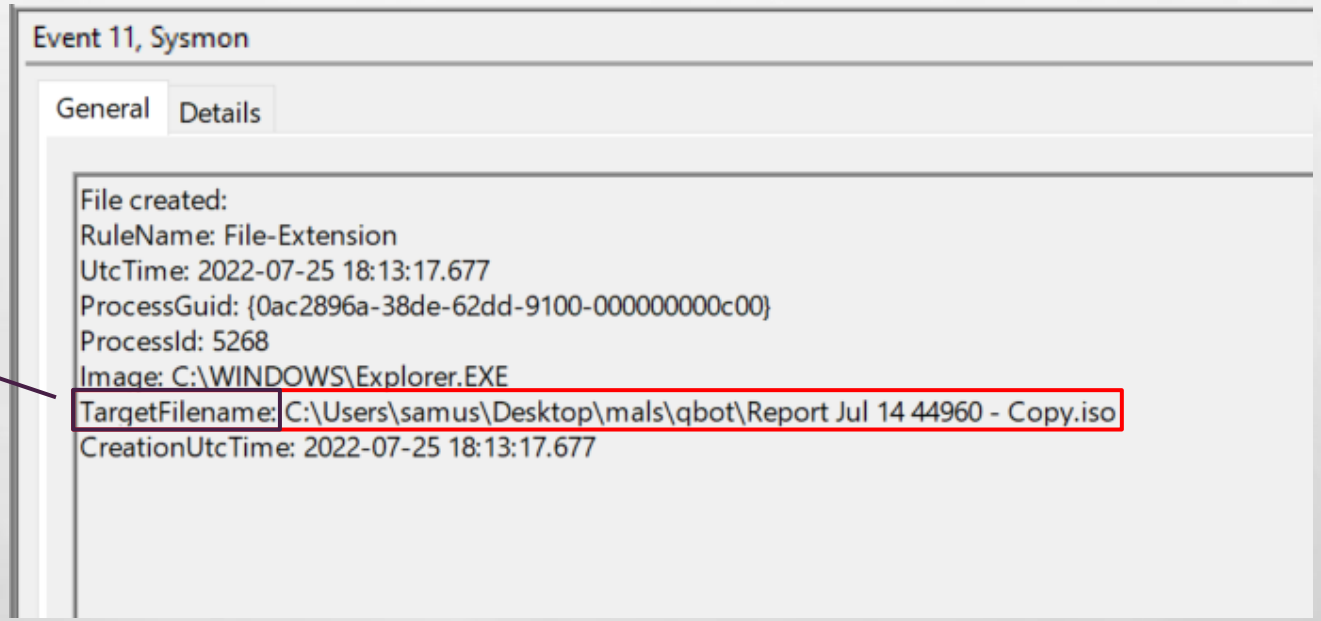
6.4 IDENTIFY GAPS AND PRIORITIZE

Detection opportunity #2:
Process calc.exe creating a process regsvr32.exe



6.4 IDENTIFY GAPS AND PRIORITIZE

Detection opportunity #3:
Creation of ISO file in specific folder Content.Outlook, Download and C:\Users\<username>\AppData\Local\Temp*.zip*.iso



zip extracted instead of double-clicked #Improvement

6.4 IDENTIFY GAPS AND PRIORITIZE

Detection opportunity #4:
Detection of DLL sideloading using Sysmon Event ID 7 ImageLoad. Process calc.exe loading an image outside of legit paths C:\Windows\System32 and/or C:\Windows\SysWOW64

procmon

20:05:29,7360383	calc.exe	6628	Thread Create	
20:05:29,7371794	calc.exe	6628	Load Image	C:\Windows\SysWOW64\shlwapi.dll
20:05:29,7382947	calc.exe	6628	Load Image	C:\Windows\SysWOW64\msvcrt.dll
20:05:29,7441598	calc.exe	6628	Load Image	C:\Windows\SysWOW64\advapi32.dll
20:05:29,7453594	calc.exe	6628	Load Image	C:\Windows\SysWOW64\sechost.dll
20:05:29,7464238	calc.exe	6628	Load Image	C:\Windows\SysWOW64\rpcrt4.dll
20:05:29,7474286	calc.exe	6628	Load Image	C:\Windows\SysWOW64\oleaut32.dll
20:05:29,7485098	calc.exe	6628	Load Image	C:\Windows\SysWOW64\combase.dll
20:05:29,7498147	calc.exe	6628	Load Image	C:\Windows\SysWOW64\ole32.dll
20:05:29,7530037	calc.exe	6628	Load Image	C:\Windows\SysWOW64\uxtheme.dll
20:05:29,7579254	calc.exe	6628	Load Image	C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf
20:05:29,7611055	calc.exe	6628	Load Image	C:\Windows\SysWOW64\winmm.dll
20:05:29,7634041	calc.exe	6628	Load Image	C:\Windows\SysWOW64\version.dll
20:05:29,7718583	calc.exe	6628	Load Image	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b
20:05:29,7764589	calc.exe	6628	Load Image	C:\Windows\SysWOW64\imm32.dll
20:05:29,8378102	calc.exe	6628	Load Image	C:\Users\samus\Desktop\mals\qbot\test\WindowsCodecs.dll
20:05:29,8547162	calc.exe	6628	Process Create	C:\WINDOWS\SysWOW64\regsvr32.exe
20:05:29,8547307	regsvr32.exe	324	Process Start	
20:05:29,8547787	regsvr32.exe	324	Thread Create	
20:05:29,8628345	calc.exe	6628	Load Image	C:\Windows\SysWOW64\apphelp.dll
20:05:29,8694634	regsvr32.exe	324	Load Image	C:\Windows\SysWOW64\regsvr32.exe
20:05:29,8709016	regsvr32.exe	324	Load Image	C:\Windows\System32\ntdll.dll
20:05:29,8730115	regsvr32.exe	324	Load Image	C:\Windows\SysWOW64\ntdll.dll

6.4 IDENTIFY GAPS AND PRIORITIZE

- Powershell encoded command…
- … and many others

Don’t reinvent the wheel, **leverage existing resources**!

Time to level up!

- Implement quick wins before re-testing
- Define roadmap for medium- and long-term improvements
  - #**Red** – Emulation
  - #**Blue** – Prevention, Telemetry and Detection
  - #**CTI** – Intel and TTPs

6.5 PLAN RECOMMENDATIONS AND IMPLEMENT QUICK WINS

6.6 FEEDBACK AND VALIDATION

To fix and improve defenses

Lots of rabbit's holes, so keep it simple

Basic detections but efficient

Mature the process

- Think **automation**...
  - Vectr + ART, SOAR?, Others*
- ... but keep in mind that **collaboration is key**, so talk, teach, learn and have fun!

*Caldera, SafeBreach, PurpleAD, PurpleSharp, Plumhound, C2Matrix, Infection Monkey, Unfetter, ATTPwn, Metta, APT Simulator, FlightSim, Scythe, Picus Security, etc.

THANK YOU

@sam0x90