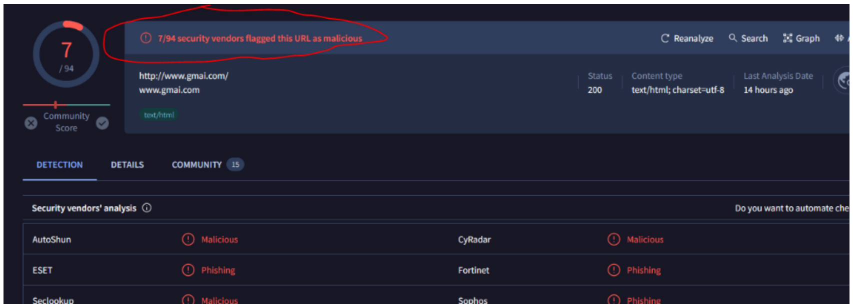
MS Defender Endpoint – Threat Hunting

Problem: a user clicked on a Phishing URL

Goal: triage and remediate alert

Process:

- Static URL analysis
    - check reputation of URL on VirusTotal



7/94 security vendors flagged this URL as malicious

http://www.gmai.com/
www.gmai.com
text/html

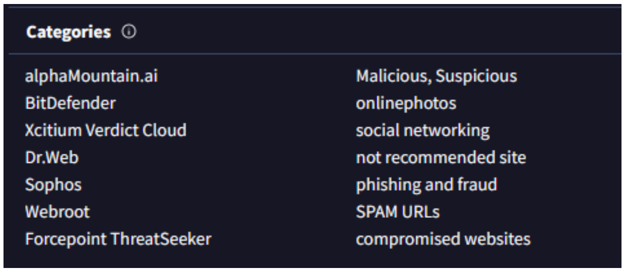
Status	Content type	Last Analysis Date
200	text/html; charset=utf-8	14 hours ago

Security vendors' analysis

Do you want to automate che

AutoShun	Malicious	CyRadar	Malicious
ESET	Phishing	Fortinet	Phishing
Seclookup	Malicious	Sophos	Phishing

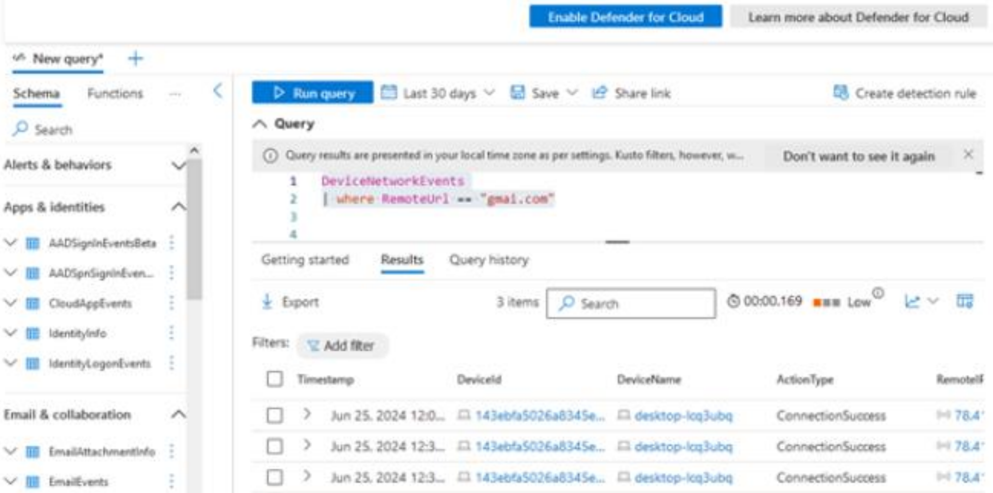
- check the category of the URL: found phishing and SPAM



Categories

alphaMountain.ai	Malicious, Suspicious
BitDefender	onlinephotos
Xcitium Verdict Cloud	social networking
Dr.Web	not recommended site
Sophos	phishing and fraud
Webroot	SPAM URLs
Forcepoint ThreatSeeker	compromised websites

- Threat Hunting: searched for the number of users who clicked the URL - 3



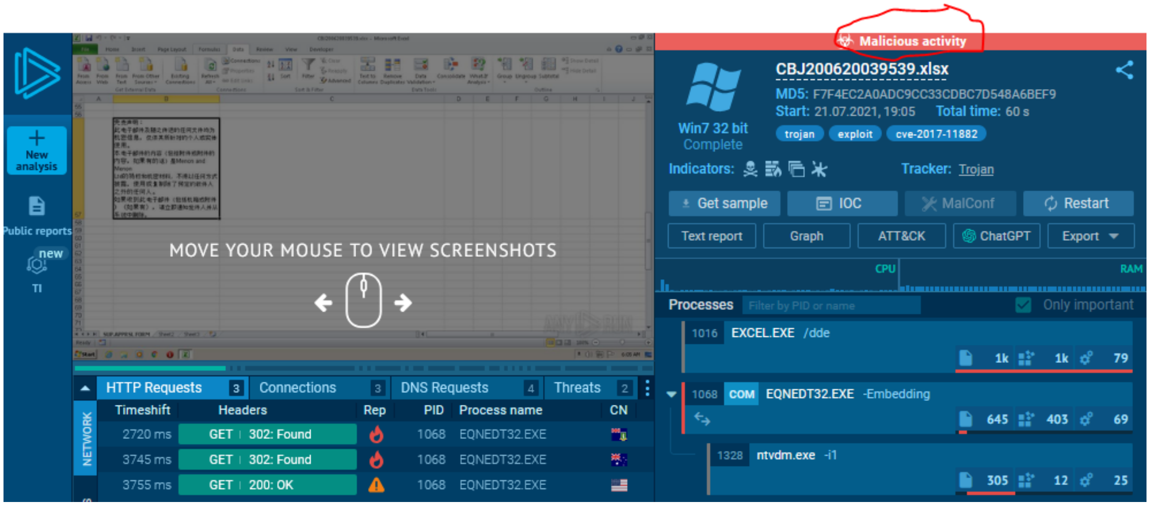
Query results are presented in your local time zone as per settings. Kusto filters, however, w...

```
DeviceNetworkEvents
| where RemoteUrl == "gmai.com"
```

Timestamp	DeviceId	DeviceName	ActionType	RemoteIP
Jun 25, 2024 12:0...	143ebfa5026a8345e...	desktop-lcq3ubq	ConnectionSuccess	78.4'
Jun 25, 2024 12:3...	143ebfa5026a8345e...	desktop-lcq3ubq	ConnectionSuccess	78.4'
Jun 25, 2024 12:3...	143ebfa5026a8345e...	desktop-lcq3ubq	ConnectionSuccess	78.4'

- **Actions**:
    - Isolate devices -> Run anti-virus -> Release device

- Dynamic URL analysis- use Any Run to interact with a malicious URL https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83
    - URL Classification - malicious



CBJ200620039539.xlsx

MD5: F7F4EC2A0ADC9CC33CDBC7D548A6BEF9

Start: 21.07.2021, 19:05 Total time: 60 s

Tracker: Trojan

1016 EXCEL.EXE /dde — 1k 1k 79

1068 COM EQNEDT32.EXE -Embedding — 645 403 69

1328 ntvdm.exe -i1 — 305 12 25

HTTP Requests 3 | Connections 3 | DNS Requests 4 | Threats 2

Timeshift	Headers	Rep	PID	Process name	CN
2720 ms	GET | 302: Found	🔥	1068	EQNEDT32.EXE	
3745 ms	GET | 302: Found	🔥	1068	EQNEDT32.EXE	
3755 ms	GET | 200: OK	⚠	1068	EQNEDT32.EXE	

- The malicious file is CBJ200620039539.xlsx
- The SHA 256 hash for the file is 5F94A66E0CE78D17AFC2DD27FC17B44B3FFC13AC5F42D3AD6A5DCFB36715F3EB
- I found the following malicious domains:
    - hxxp[://]www[.]biz9holdings[.]com
    - hxxp[://]www[.]findresults[.]site
- I found the following malicious IP addresses:
    - 204[.]11[.]56[.]48
    - 103[.]224[.]182[.]251
    - 75[.]211[.]242
- This malicious attachment attempts to exploit the CVE vulnerability.