Incident Report

Customer: Scenario Client CPM SEN-571

Priority	High
Status	Open
Incident Category	Phishing
Incident Description	Three workstations were compromised via phishing attack

Incident Handler	
Name	Abdurr Patel
Contact	Abdurrpatel2@gmail.com

Affected Host System or Systems	The Affected Service or Services
WS-029 WS-032 WS-073	

Incident Findings

This report provides an initial assessment; further analysis is required to validate timeline, execution, C2 presence, and potential persistence or lateral movement.

What is known:

- The multiple threat intelligence hits from a high-confidence feed indicate potential malicious activity that may have moved across the network.
- Three workstations (WS-029, WS-032, WS-073) accessed eight suspicious TLDs (.ml, .gq, .tk, .ga). known for hosting and distributing malware.
- These TLDs are often used by attackers since there is no financial commitment, making them ideal for malware hosting and phishing campaigns.
- Virus Total has classified each link with at least being one of phishing, malware or spyware.

What Can be Deduced:

- Initial access technique is likely a phishing campaign given that multiple users were affected with supporting classification from Virus Total.
- Given the reputation of the TLD and that eight different domains were accessed by only three workstations, it's possible some of the links were used as a beacon to download additional tools and / or establish a C2 channel from the other domains. A common tactic used is the Ingress Tool Transfer (T1105)
- Suspicious activity has been reported across the network, indicating the possibility of lateral movement from those endpoints in a reasonable timeframe.

Investigation Recommendations

Verify Initial Access **|** Confirm and identify the scope of the phishing campaign unearthing any unreported entities:

- Query email logs for links containing .ml, .gq, .tk, .ga domains and pivot to identify the sender addresses and list of recipient clients.
- From those senders find evidence of internal phishing to rule out the possibility of lateral movement using this technique. (T1534)
- Analyse patterns in targeted client roles or privileges to determine if this was a targeted attack.

Identify Execution & C2 Communication **|** Correlate system events that show evidence execution and discovery commands:

- Hunt for file creation events on affected workstations to see if any artifacts were installed post outbound visit to those domains.
- If artefacts are found, detonate in ANY.RUN to observe execution behaviour, network activity, and potential C2 destinations.
- Analyse endpoint logs for activity of PowerShell and CMD, notable execution commands: Invoke-WebRequest (IWR), Invoke-Expression (IEX) and network discovery tools such as nltest, net view). (T1059.001)

Monitor for Possible Persistence or Lateral Movement | Investigate the integrity of core services and potential ports to pivot:

- If execution is confirmed, inspect registry keys, scheduled tasks, and DLL modifications for persistence mechanisms (T1547, T1053)
- Assess internal authentication logs (Event IDs 4624, 4625) for unusual login attempts indicating lateral movement (T1021, T1047)
- Investigate network/endpoint logs for abnormal SSH SMB or RDP activity coming from those compromised workstations. (T1021.002, T1021.001, T1021.004)

Remediation Measures

Containment:
Isolate Affected Endpoints **|** Block Malicious Domains & IPs **|** Reset Compromised Accounts:

- Immediately disconnect WS-029, WS-032, and WS-073 from the network to prevent lateral movement.
- Add the identified domains (.ml, .gq, .tk, .ga) and any associated IPs to firewall and email security (e.g. Mimecast) block lists.
- Suspend compromised accounts and reset passwords and enforcing MFA.

Eradication:
Remove Malicious Payloads **|** Identify and Remove Persistent Mechanisms **|** Directly Block C2 Traffic:

- Remove Malicious tools or payloads used in the attack.
- Safely remove malicious artefacts and amend any persistent conditions (e.g registry changes, scheduled tasks).
- If C2 beaconing were detected, block outbound traffic to those known C2 IPs/domains at the firewall.

Recovery:
Compromised System Backups **|** Ensure Availability:

- Restore affected systems using verified clean backups or rebuild systems from scratch if clean backups are unavailable.
- Restore networks and verify that all restored systems and applications are functioning correctly with continuous monitoring

Proactive Post Incident Activity:
Leveraging Microsoft Identity Intelligence Tools:

- Microsoft Defender ITDR – Increase identity intelligence through ITDR designed to map, investigate, and respond to identity-based attacks such as phishing, privilege escalation, and lateral movement. This correlation of intelligence is going to allow a greater depth in analysing behaviour which allows functions like Entity Behaviour Analytics (UEBA) to alert and prevent attacks before they progress.

- Microsoft Attack Simulation Training – Proactively have users engage in phishing simulations that improve awareness through action rather than feedback. Telling users to be more aware of phishing emails is not going to grantee reduced probability of risk long term. Its vital that users are actively engaged and taught through these simulations to get quantifiable results that can influence policy and strategy.

References

https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/

https://attack.mitre.org/

https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-simulations

https://www.microsoft.com/en-us/security/blog/2023/05/31/xdr-meets-iam-comprehensive-identity-threat-detection-and-response-with-microsoft/?culture=en-us&country=us&culture=en-us&country=us