[SOC-1] Suspicious link detected in mail

Created: 11/Jan/26 Updated: 14/Jan/26 Resolved: 14/Jan/26

Status:	Done
Project:	SOC Operations
Components:	Email and Collaboration Services
Affects versions:	None
Fix versions:	None

Type:	Task	**Priority:**	Medium
Reporter:	Shewag Bhattarai	**Assignee:**	Shewag Bhattarai
Resolution:	Done	**Votes:**	0
Labels:	Phising		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Team:	
Urgency:	Medium
Impact:	Moderate / Limited
Request language:	English
Request participants:	None
Organizations:	None

Description

EventID :86

Event Time :Mar, 22, 2021, 09:23 PM

Rule :SOC141 - Phishing URL Detected

Level :Security Analyst

Source Address :172.16.17.49

Source Hostname : EmilyComp

Destination Address :91.189.114.8

Destination Hostname :mogagrocol.ru

Username :ellie

Request URL :http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io

User Agent :Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36

Device Action :Allowed

Comments

Comment by Shewag Bhattarai [14/Jan/26]

On Mar 22, 2021 at 09:23 PM, SIEM detected access to a known phishing URL (http://mogagroco.ru/wp-content/plugins/akismet/fv/index.php?email=elletsdefend) originating from host EmilyComp. The request was allowed by the firewall.

Comment by Shewag Bhattarai [14/Jan/26]

Investigation confirmed that the user submitted their email address on the phishing page, indicating successful interaction. URL reputation analysis via VirusTotal identified the domain as malicious, flagged by more than 10 security vendors.

Following the initial access, multiple additional URLs were requested from the same host. Threat intelligence platforms classified this follow-on activity as botnet-related behavior. Sandbox analysis confirmed the presence of a credential harvesting landing page.

No evidence of lateral movement or further compromise was observed beyond the affected host.

Conclusion: This activity was confirmed as a successful phishing attack with user interaction.

Remediation Actions:

- User credentials reset
- User notified and security awareness guidance provided
- Malicious URLs blocked at proxy level
- Host monitored for additional suspicious activity

Verdict: True Positive