EventID 86 SOC141 Phishing URL

This incident is of type “Proxy”, indicating that suspicious activity was detected through proxy logs. In this case, a suspicious URL has been identified during proxy logs inspection.

The SIEM rule that created this incident is called “SOC141 Phishing URL Detected”.

Incident time: 2021, March (Monday) 22th at 21:23h

Source address: 172.16.17.49

Source hostname: EmilyComp

Username: ellie

Destination address: 91.189.114.8

Destination hostname: mogagrocol.ru

URL requested:

- 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

The device action is allowed, indicating that the proxy server didn’t block the request, and the source machine successfully requested the indicated resource.

Requested URL

VirusTotal flags the requested URL as phishing (last analysis 1 day ago), although “urlscan.io” detects it as a harmless WordPress site.

URLhaus has a register of "http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=” and flags it as a malware distribution URL. The register is three months old.

Hybrid Analysis has a lot of registers for “mogagrocol.ru” domain, the most recent one providing the following data:

- The requests to the target URL passes through many Russian Federation domains and some US domains
- From 17 IoCs listed, two of them are:
  - “GETs files from a web server”
    - Maps to MITRE ATT&CK Tactic T1071.001, indicating attackers avoid detection by blending with existing traffic
  - “Input URL references an email address”
    - Maps to MITRE ATT&CK Tactic T1566, indicating attackers may acquire domains that can be used during targeting

The domain has a Russian TDL, which indicates that’s hosted on Russia, and has an “email” URL param containing the victim’s email.

The URL mimics a legitimate WordPress plugin path (/wp-content/plugins/akismet/fv/), which explains why some Threat Intelligence Feeds identify the URL as a harmless WordPress site.

I notice the requested URL is not using TLS encryption, transmitting through HTTP (http://), why would an attacker do that? Wouldn't that make the URL even more suspicious in the first place?

There can be many reasons, but from what I've found:

- Setting up HTTPS requires obtaining and configuring SSL/TLS certificates, which can be a hurdle for attackers aiming for quick deployment. By using HTTP, they can rapidly set up phishing sites without the additional steps involved in securing the site
- Many users may overlook missing HTTPS warnings, and attackers exploit this by creating convincing replicas of legitimate sites
- HTTP traffic is susceptible to MitM attacks, attackers can manipulate responses for malicious purposes
- Some security tools prioritize scanning HTTPS over HTTP due to its encrypted nature. By using HTTP, attackers might bypass certain security measures

User-Agent

The User-Agent indicates the following:

- "Windows NT 6.1; Win64; x64" indicates the source computer system:
  - Uses Windows 7 with version "NT 6.1"
  - Uses a 64-bit version of Windows
  - Runs on a 64-bit CPU
- The client uses "Chrome/79.0.3945.88" browser
- Google Chrome adds "Safari/537.36" to ensure compatibility with websites that check for Safari browser
- Most browsers add "Mozilla/5.0" for compatibility with Firefox browser

- The client uses “AppleWebKit/537.36” browser engine
- “KHTML, like Gecko” is included for compatibility with Gecko browser engine, the software responsible for rendering content on Firefox browser

Log Management

I’ve checked the destination IP on the logs, which indicate:

- Two logs (proxy & firewall) display a request from “172.16.17.49:55662” to “91.189.114.8:80” at 21:23h

rDNS Lookup

> ❓ I’ve performed DNS Lookup with the help of MxToolbox SuperTool.

A Reverse DNS Lookup determines the domain name associated with an IP address by querying for a PTR Record. This can give additional information about the destination IP address.

The destination IP address “91.189.114.8” is associated with multiple domains (including “yngleaks.com”), this suggests that the IP is part of a shared hosting environment, which is common for hosting multiple websites on a single server.

A Forward DNS Lookup retrieves the IP address associated with a domain name by querying for an Address Record.

I’ve performed Forward DNS Lookup on "mogagrocol.ru” destination domain, which has an A Record pointing to “91.189.114.8”. This confirms it’s hosted on the same server as “yngleaks.com”.

This association confirms that “mogagrocol.ru” is hosted on a shared server, which may be relevant if the server is known to host malicious domains.

Actions

With help of EDR software, the user machine (EmilyComp) has been contained, and the Phishing Email has been deleted.

Further requests by other machines to the “mogagrocol.ru” domain have been checked under log management, and no more matches have been found. This indicates that there’s no evidence of other systems requesting the malicious domain.

Also, no more recipients have received emails containing the malicious domain.

The following artifacts are attached to the incident:

- “mogagrocol.ru” (URL): phishing domain
- “14b9a0281bcd5677207541479bb9dc9c” (MD5 Hash): destination address

The destination IP address has been identified as a shared hosting environment, and other domains that resolve to this IP are not proven harmful. This is why I’m not including the destination IP address.

Conclusion

The victim has received a Phishing Email with an URL coming from Russian servers, this URL contains an URL Param with the email of the recipient.

When the recipient requests the resource pointed to by the URL, is enabling the attacker to acknowledge that this email is responsive for future attacks.

A part from that, the URL uses unencrypted HTTP, meaning the email address from the victim is transmitted as plain text until reaching the destination server. The victim’s email is leaked for the attacker and unintended parties.

The request was not blocked, meaning the victim’s email has been compromised.