Incident Investigation Report: SOC141 - Phishing URL Detected

REPORT DATE	October 6, 2023,
REPORTED BY	Humna Abid
INCIDENT ID	86

EXECUTIVE SUMMARY:

At 9:30 AM, the defense monitoring system receives an alert that an IP address `172.16.17.49` tries to access a malicious URL. The IP address is associated with the hostname EmilyComp. The connection was successfully established with the destination `91.189.114.8 mogagrocol.ru` and saw anomalous behavior on the system. I investigated this alert and successfully performed Containment on the End-point device to reduce further spreading on the network.

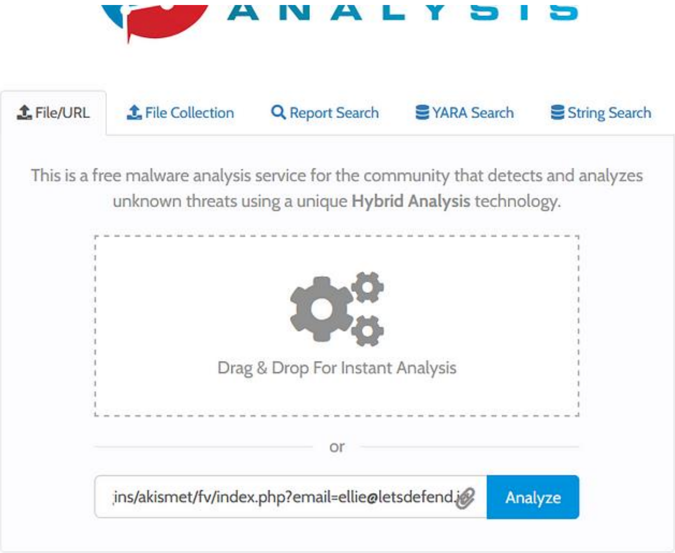
INCIDENT DETAILS:

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.

INVESTIGATION FINDINGS:

URL Analysis:

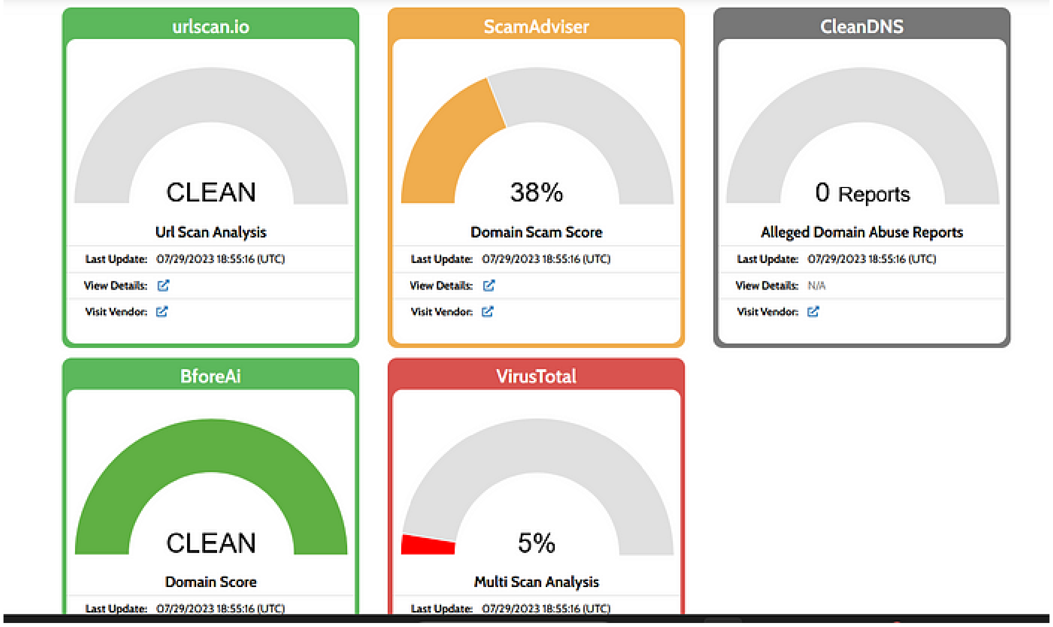
- Copy the URL and paste it into Hybrid Analysis.



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

ins/akismet/fv/index.php?email=ellie@letsdefend.io

After uploading, we see that some anti-virus services mark the URL as malicious, while others mark it as clean (Figure 2).



urlscan.io — Last Update: 07/29/2023 18:55:16 (UTC); View Details:; Visit Vendor:

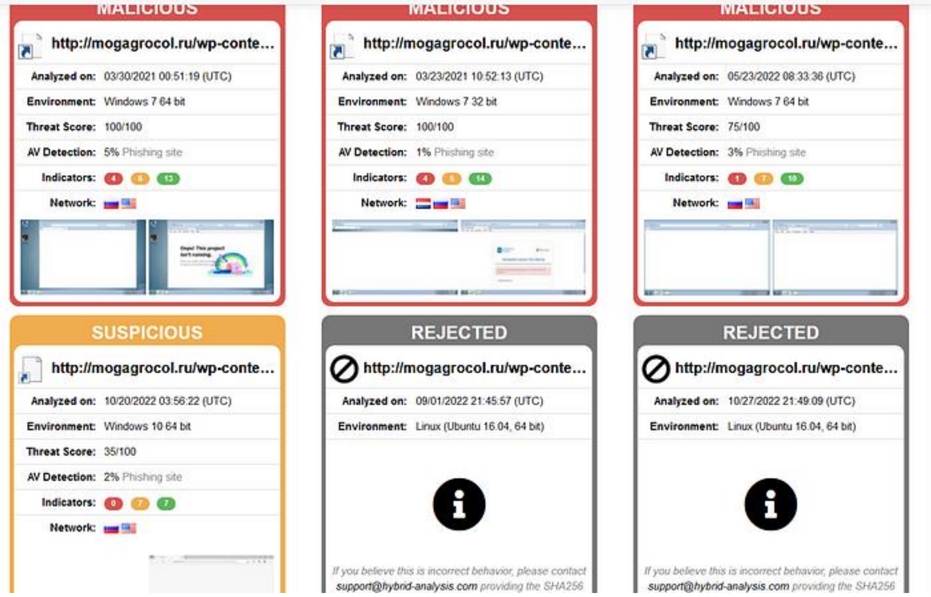
ScamAdviser — Last Update: 07/29/2023 18:55:16 (UTC); View Details:; Visit Vendor:

CleanDNS — Last Update: 07/29/2023 18:55:16 (UTC); View Details: N/A; Visit Vendor:

BforeAi — Last Update: 07/29/2023 18:55:16 (UTC)

VirusTotal — Last Update: 07/29/2023 18:55:16 (UTC)

You can go to Virus Total's report to see the details, but I will directly check the sandbox report in Hybrid Analysis (Figure 3).



MALICIOUS

http://mogagrocol.ru/wp-conte...

Analyzed on: 03/30/2021 00:51:19 (UTC)
Environment: Windows 7 64 bit
Threat Score: 100/100
AV Detection: 5% Phishing site
Indicators: 4 6 13
Network:

MALICIOUS

http://mogagrocol.ru/wp-conte...

Analyzed on: 03/23/2021 10:52:13 (UTC)
Environment: Windows 7 32 bit
Threat Score: 100/100
AV Detection: 1% Phishing site
Indicators: 4 5 14
Network:

MALICIOUS

http://mogagrocol.ru/wp-conte...

Analyzed on: 05/23/2022 08:33:36 (UTC)
Environment: Windows 7 64 bit
Threat Score: 75/100
AV Detection: 3% Phishing site
Indicators: 1 7 10
Network:

SUSPICIOUS

http://mogagrocol.ru/wp-conte...

Analyzed on: 10/20/2022 03:56:22 (UTC)
Environment: Windows 10 64 bit
Threat Score: 35/100
AV Detection: 2% Phishing site
Indicators: 0 7 7
Network:

REJECTED

http://mogagrocol.ru/wp-conte...

Analyzed on: 09/01/2022 21:45:57 (UTC)
Environment: Linux (Ubuntu 16.04, 64 bit)

If you believe this is incorrect behavior, please contact support@hybrid-analysis.com providing the SHA256

REJECTED

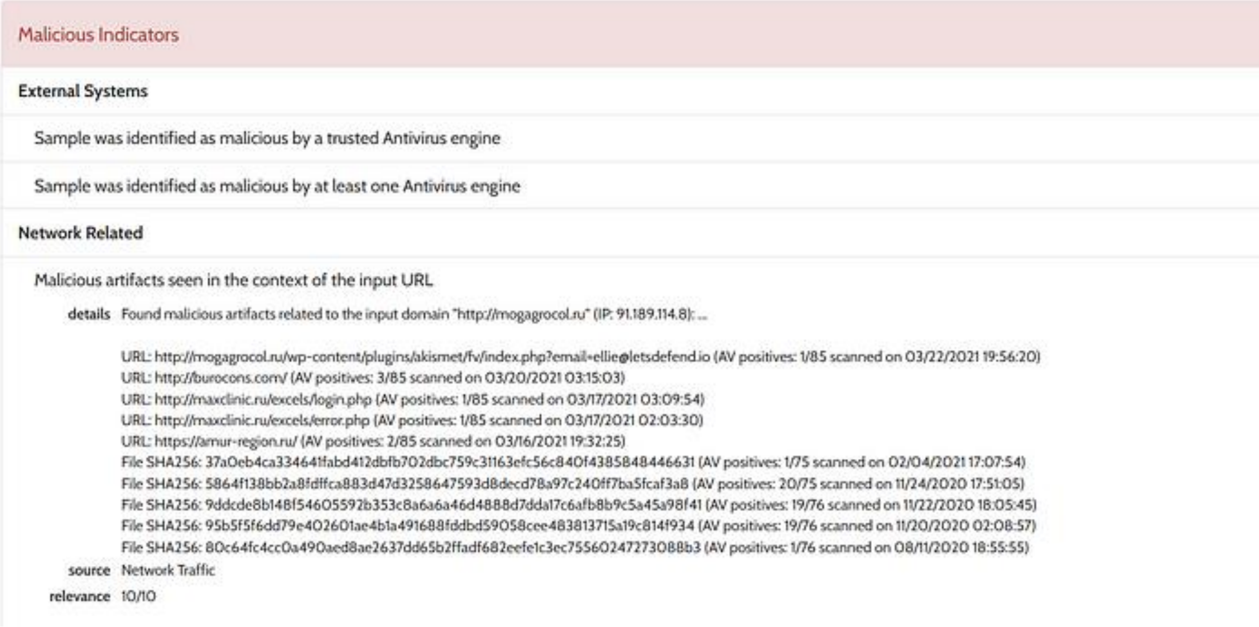
http://mogagrocol.ru/wp-conte...

Analyzed on: 10/27/2022 21:49:09 (UTC)
Environment: Linux (Ubuntu 16.04, 64 bit)

If you believe this is incorrect behavior, please contact support@hybrid-analysis.com providing the SHA256

The URL behaved differently in various environments. Let us click on the report with a screenshot of a form (top middle) because it looks more like a phishing attempt.

In the sandbox report, there are many suspicious indicators about the behavior of the URL.



Malicious Indicators

External Systems

Sample was identified as malicious by a trusted Antivirus engine

Sample was identified as malicious by at least one Antivirus engine

Network Related

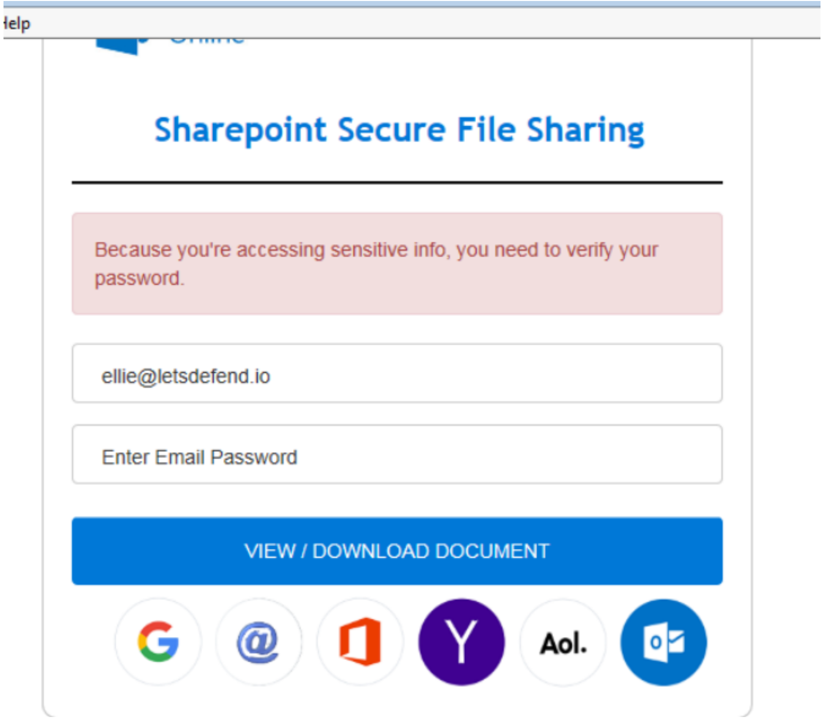
Malicious artifacts seen in the context of the input URL

```
details   Found malicious artifacts related to the input domain "http://mogagrocol.ru" (IP: 91.189.114.8): ...

          URL: http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io (AV positives: 1/85 scanned on 03/22/2021 19:56:20)
          URL: http://burocons.com/ (AV positives: 3/85 scanned on 03/20/2021 03:15:03)
          URL: http://maxclinic.ru/excels/login.php (AV positives: 1/85 scanned on 03/17/2021 03:09:54)
          URL: http://maxclinic.ru/excels/error.php (AV positives: 1/85 scanned on 03/17/2021 02:03:30)
          URL: https://amur-region.ru/ (AV positives: 2/85 scanned on 03/16/2021 19:32:25)
          File SHA256: 37a0eb4ca334641fabd412dbfb702dbc759c31163efc56c840f4385848446631 (AV positives: 1/75 scanned on 02/04/2021 17:07:54)
          File SHA256: 5864f138bb2a8fdffca883d47d3258647593d8decd78a97c240ff7ba5fcaf3a8 (AV positives: 20/75 scanned on 11/24/2020 17:51:05)
          File SHA256: 9ddcde8b148f54605592b353c8a6a6a46d4888d7dda17c6afb8b9c5a45a98f41 (AV positives: 19/76 scanned on 11/22/2020 18:05:45)
          File SHA256: 95b5f5f6dd79e402601ae4b1a491688fddbd59058cee483813715a19c814f934 (AV positives: 19/76 scanned on 11/20/2020 02:08:57)
          File SHA256: 80c64fc4cc0a490aed8ae2637dd65b2ffadf682eefe1c3ec755602472730 88b3 (AV positives: 1/76 scanned on 08/11/2020 18:55:55)
   source Network Traffic
relevance 10/10
```

If you search the related URL addresses provided in Figure 4 in Virus total, you can see that every one of them is associated with phishing.

Now let us look at screenshots to see what's happening on the website.



Sharepoint Secure File Sharing

Because you're accessing sensitive info, you need to verify your password.

ellie@letsdefend.io

Enter Email Password

VIEW / DOWNLOAD DOCUMENT

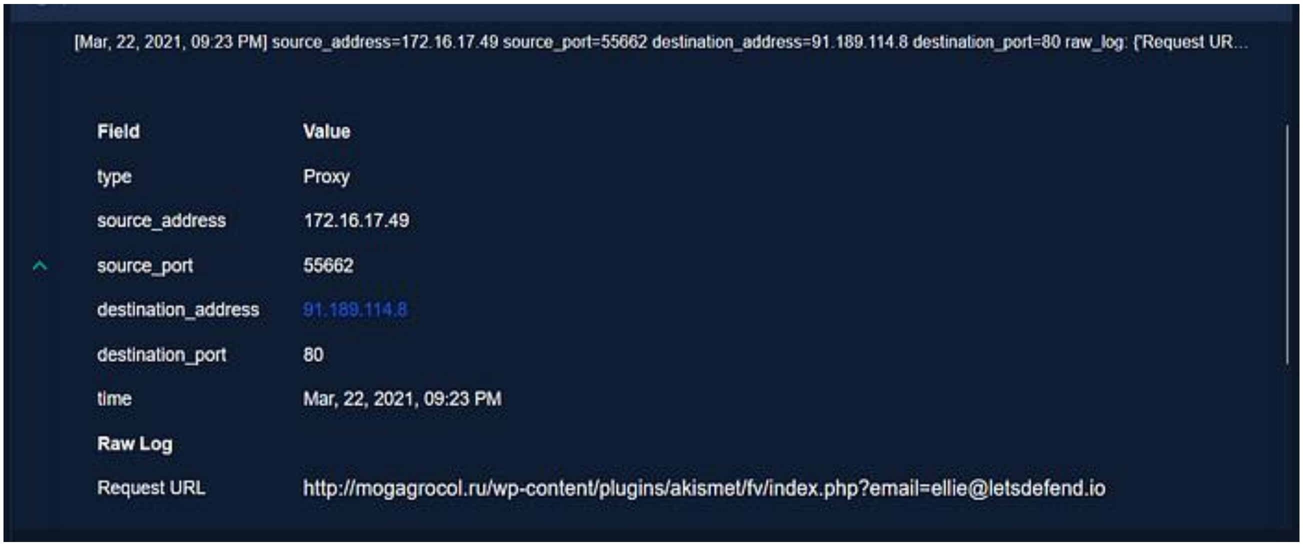
The login form requires email name and email password information to download/view some sensitive information.

This is a phishing attempt because no site will ask you for your email password. Here, the attacker aims to gain access to your email account.

Let us go to the Log Management tab to see communications between the host and the malicious URL address.

LOG MANAGEMENT

If you search for the logs with a source address of 172.16.17.49 and a destination address of 91.189.114.8,

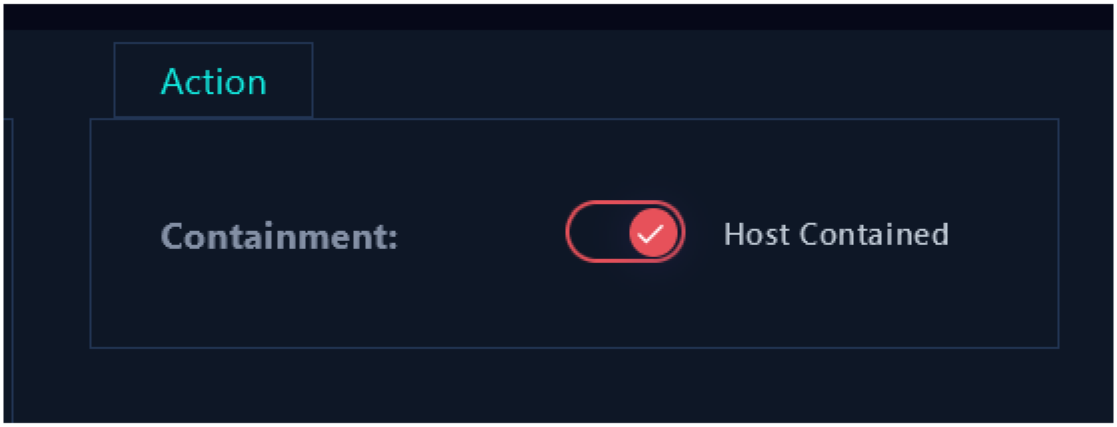


```
[Mar, 22, 2021, 09:23 PM] source_address=172.16.17.49 source_port=55662 destination_address=91.189.114.8 destination_port=80 raw_log: {'Request UR...

Field                Value
type                 Proxy
source_address       172.16.17.49
source_port          55662
destination_address  91.189.114.8
destination_port     80
time                 Mar, 22, 2021, 09:23 PM
Raw Log
Request URL          http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io
```

We see that successful communication has occurred and we know that the device did not prevent it.

At this point, we must contain the machine in case the phishing has been successful.



Containment: Host Contained

USER TRAINING AND AWARENESS:

- Affected users were immediately notified of the phishing attempt and instructed not to click on suspicious links.
- A reminder of the organization's policies was sent to all employees.

ACTIONS TAKEN:

1. The affected user accounts were monitored for any signs of unauthorized access.
2. The malicious URL was blocked to prevent access from within the organization.
3. Employees were informed about the incident and advised to remain vigilant against phishing attempts.

RECOMMENDATIONS:

Conduct a thorough forensic investigation.

1. Analyze the IP reputation of 172.16.17.49 and 91.189.114.8 mogagrocol.ru.
2. Strengthen employee awareness training.
3. Ensure endpoint security and patch management.
4. Enhance email filtering solutions.
5. Review and update the incident response plan.

CONCLUSION:

In reaction to the occurrence involving IP address 172.16.17.49 trying to access a malicious URL, prompt containment was carried out. The extent of the breach requires more research. This incident highlights the necessity of strong cybersecurity measures, such as employee education and prompt threat detection.