

Kia ora! This is my walkthrough/documentation of my process in investigating LetsDefend's SOC alert for SOC141 – Phishing URL Detected.

Lets start with going to our investigation channel inside the LetDefend practice sector and create a case for this alert.

The screenshot shows a detailed view of a SOC141 - Phishing URL Detected alert. At the top, it says "High" priority, the date "Mar, 22, 2021, 09:23 PM", and the title "SOC141 - Phishing URL Detected". On the right, there are buttons for "86" and "Proxy", with a circled "»/" button highlighted in red. Below the title, a message states "This alert has been re-investigated". The alert details are listed in a table:

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

Make note of the details on this screen. I like to keep a separate notepad open to get down the source address/hostname, destination address/hostname, and any other information that might call out to me. In this case, I take note of the user agent and request URL.

Now that we've created the case, I recommend duplicating the tab before starting the playbook. This ensures that you can always refer back to the playbook without losing your progress.

Personally, I like to do my investigation before going through the playbook. This is my process.

I put through the destination address through various online tools such as VirusTotal and Hybrid Analysis. Let's see what hits we get.

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendor	Status	Security vendor	Status
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AI Labs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
Chong Luu Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean

Putting the destination address through VirusTotal comes back clean, but we still need to keep looking.

I searched the request URL twice, once with the typical phishing "?email=ellie@letsdefend.io" and another without, I want to take a look if there are any differences there.

Community Score 11 / 98

11/98 security vendors flagged this URL as malicious

http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php
mogagrocol.ru

Status 403 Content type text/html; charset=utf-8 Last Analysis Date 2 minutes ago

text/html external-resources

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis Do you want to automate checks?

alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Phishing
CRDF	ⓘ Malicious	Fortinet	ⓘ Phishing
G-Data	ⓘ Phishing	Kaspersky	ⓘ Phishing
Lionic	ⓘ Phishing	Sophos	ⓘ Phishing
Trustwave	ⓘ Phishing	VIPRE	ⓘ Phishing
Webroot	ⓘ Malicious	ESET	ⓘ Suspicious
Abusix	✅ Clean	Acronis	✅ Clean

Community Score 10 / 98 -5

10/98 security vendors flagged this URL as malicious

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

Status 403 Content type text/html; charset=utf-8 Last Analysis Date a moment ago

text/html external-resources

DETECTION DETAILS COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis Do you want to automate checks?

alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Phishing
CRDF	ⓘ Malicious	Fortinet	ⓘ Phishing
G-Data	ⓘ Phishing	Kaspersky	ⓘ Phishing
Lionic	ⓘ Phishing	Sophos	ⓘ Phishing
VIPRE	ⓘ Phishing	Webroot	ⓘ Malicious
ESET	ⓘ Suspicious	Trustwave	ⓘ Suspicious
Abusix	✅ Clean	Acronis	✅ Clean

10-11 out of 98 vendors flagged this as malware. Checking the categories shows that this is suspected phishing and fraud according to the different vendors. We also see that the website is error code 403 (forbidden).

Another thing that is interesting is the different address in the HTTP response section. This is 195.24.68[.]4, putting this through shows that it communicates with a lot of risky executables, PDFs and other HTML files.

So VirusTotal is showing hits for it maybe being a phishing URL, lets take a look at Hybrid Analysis where it also runs it through a sandbox and can be a bit more detailed.

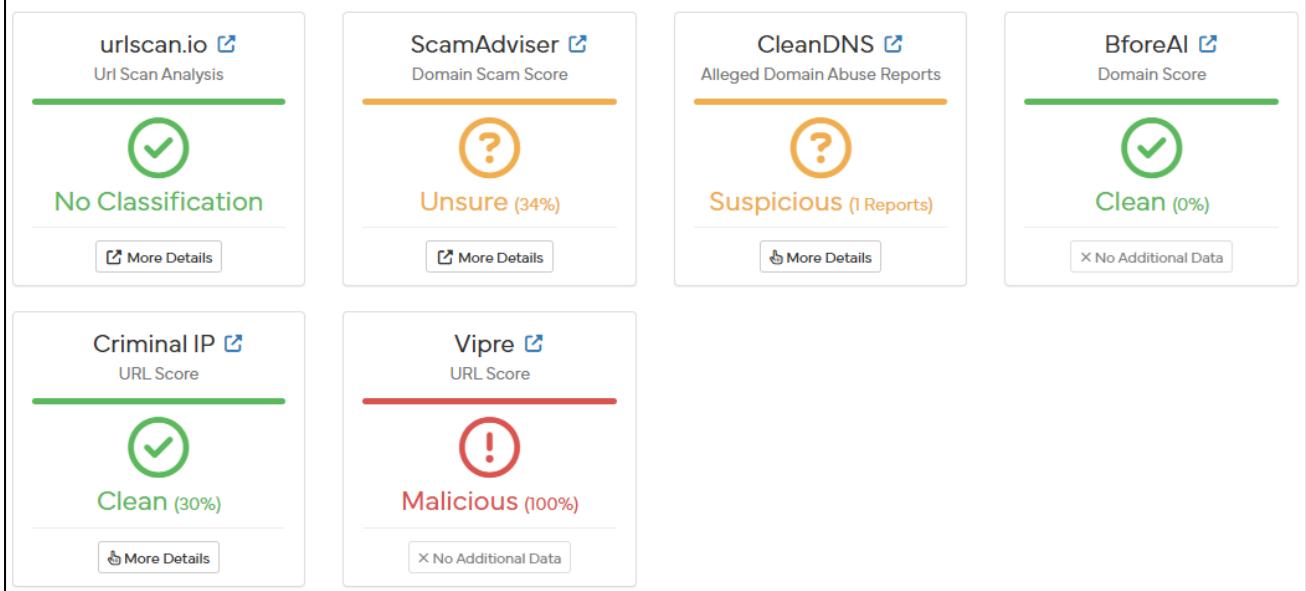
Analysis Overview

[Request Report Deletion](#)

Submission name:	hxxp://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie%40letsdefend.io	malicious
Size:	112B	Threat Score: 100/100
Type:	url	AV Detection: 22%
Mime:	text/plain	#letsdefend #phishing
Submitted At:	2021-03-23 10:52:11 (UTC)	X Post DLink E-Mail
Last Anti-Virus Scan:	2025-12-03 21:39:46 (UTC)	
Last Sandbox Report:	2023-12-03 08:53:39 (UTC)	Community Score 0 / 0

Anti-Virus Results

✓ Updated a while ago



Threat score is 100/100 and the overall is malicious rating. Lets take a look at what the Falcon Sandbox reported.

Falcon Sandbox Reports (10)

Characteristics Legend Show All As List

Not all reports are visible. 5 error reports are hidden.

Show All As List

 f64073d48d8906dce85471977606... May 23rd 2022 08:33:36 (UTC) Malicious Threat Score: 75/100 Labeled As: Phishing site Indicators: Characteristics:	 f64073d48d8906dce85471977606... March 30th 2021 00:51:19 (UTC) Malicious Threat Score: 100/100 Labeled As: Phishing site Indicators: Characteristics:	 f64073d48d8906dce85471977606... March 23rd 2021 10:52:13 (UTC) Malicious Threat Score: 100/100 Labeled As: Phishing site Indicators: Characteristics:
 f64073d48d8906dce85471977606... December 3rd 2023 08:53:39 (UTC) Suspicious Threat Score: 100/100 Labeled As: Phishing site Indicators: Characteristics:	 f64073d48d8906dce85471977606... October 20th 2022 03:56:22 (UTC) Suspicious Threat Score: 35/100 Labeled As: Phishing site Indicators: Characteristics:	

Not good, safe to say that this is 100% a phishing site. Ignore the 5 error reports, those were in a Linux environment that didn't support the "sample.url" files. Lets choose one of these and see what indicators are showing up.

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Suspicious Indicators	
External Systems	
Sample was identified as malicious by at least one Antivirus engine	
Installation/Persistence	
Found a string that may be used as part of an injection method	
Network Related	
Found potential IP address in binary/memory	
Uses a User Agent typical for browsers, although no browser was ever launched	
Spyware/Information Retrieval	
Found browser information locations related strings	
System Security	
Adjusts debug privileges	
Unusual Characteristics	
Drops script files inside temp directory	

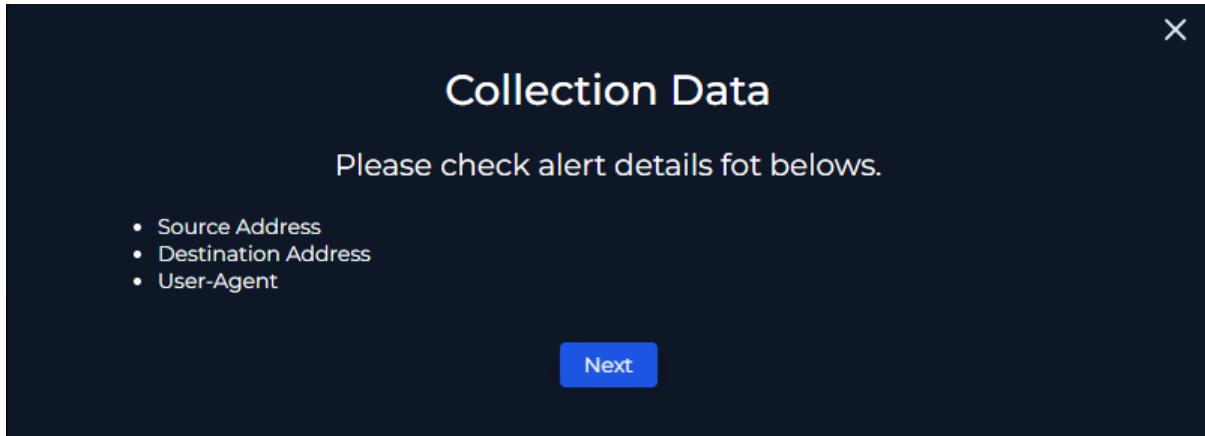
Here we can see the risk assessment and MITRE ATT&CK techniques used as well as indicators that show why its suspicious/malicious. Scrolling down to the contacted hosts shows the IP addresses from the original alert plus the one that was connected to the VirusTotal result from earlier.

Alright so we've done a bit of an indepth research using the online tools available and we can conclude that this is a malicious piece of software. There's another section that I would like you to take a look at – the URL itself:

[[http://mogagrocol.ru/wp-content/plugins/akismet/fv/index\[.\]php?email=ellie@letsdefend.io](http://mogagrocol.ru/wp-content/plugins/akismet/fv/index[.]php?email=ellie@letsdefend.io)]

Please look at the highlighted part, the plugin “Akismet” used for anti-spam does not have a directory /fv. This directly indicates the use of a compromised site as well as hiding in plain sight. Uses for this could be a backdoor with index.php.

Well, this seems like a substantial amount of information from the top layer, lets go onto the playbook and following along with it.

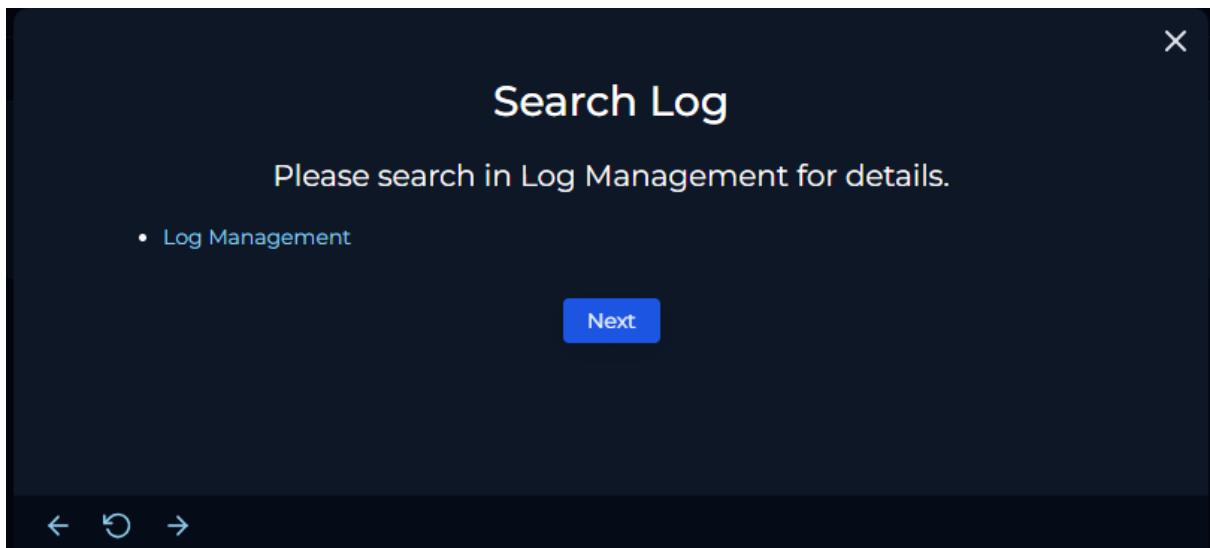


We already have all this information, something to note is the User-Agent here

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

We see that Emily is using outdated versions of Windows 7 (Windows NT 6.1 is the same thing) and the browser information being Chrome 79 (we are currently at Chrome version 143). This poses great risks, and should be taken note of for the remediation process.

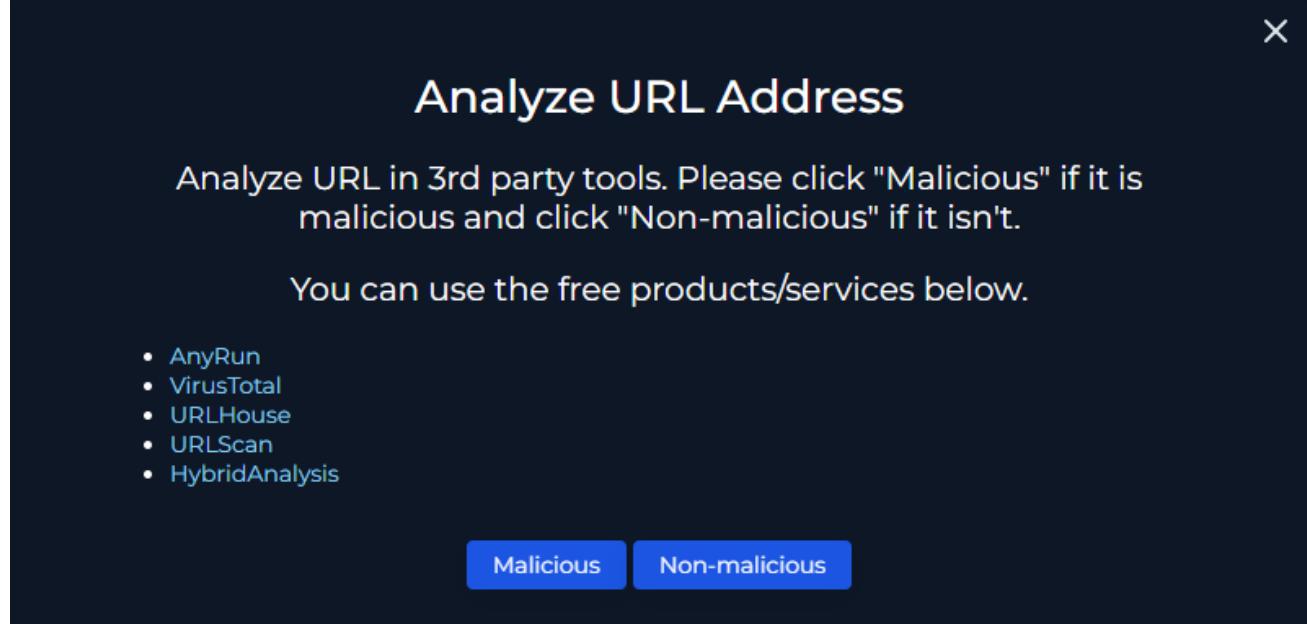
Let's click next to continue through the playbook.



In that duplicated tab, go to Log Management and look at the destination address along with the source address.

When looking at the destination address, we see that Ellie did access this URL at March 22nd 2021 09:23pm. Thankfully no other users also accessed this URL. As a precaution I also input the other IP addresses that we saw earlier, but no logs are returned.

We can go next through the playbook and with our knowledge answer whether this is malicious or non-malicious.



Now we must determine if anyone has accessed the IP/URL/Domain.

X

Has Anyone Accessed IP/URL/Domain?

Check with Log Management whether there is a device that can access these addresses from devices in the network. Also Find answers to the following questions

- When was it accessed?
- What is the source address?
- What is the destination address?
- Which user tried to access?
- What is User Agent?
- Is the request blocked?

Is there any access to URL?

Accessed Not Accessed

With our information and the log management section we can confidently answer all these questions. The last one can be a bit confusing if you are new to this, but we can see that the firewall allowed this URL.

Go to the end point security and contain the threat before continuing.

Now we can enter all the artifacts that we acquired during this investigation.

Value	Comment	Type	Remove
91.189.114.8	Attacker IP	IP Address	
http://mogagrocol.ru	Requested URL	URL Address	
195.24.68.4	Serving IP Address	IP Address	
172.16.17.49	Victim IP	IP Address	
mogagrocol.ru	Parent URL	URL Address	

Fill out your analysis comments and complete the playbook. We can now close the alert and make a note to explain your result.

Congratulations! That's the SOC141 – Phishing URL Detected alert completed. As a part of good practice, we should think about some further remediation.

1. Block the IP addresses and URL

Make this into a firewall rule to ensure that no one else gets this URL and possibly contaminates their system.

2. Update Emily/Ellie's computer OS

This event time was in March of 2021, and Windows 7 ended support back in January of 2020, meaning this was very high risk of vulnerabilities. The system must be either updated or upgraded immediately – upgraded if the phish attack is serious.

We must also ensure that the Chrome version is also updated to the most recent version at that time, which would've been Chrome 89 (March 2nd 2021)

3. Train the Employees

A mandatory training exercise for the employees of the company to teach them the risks of clicking on untrusted URLs to raise awareness.