Official Incident Report

Incident Name: EventID: 93 - [SOC146 - Phishing Mail Detected - Excel 4.0 Macros]

Description: EventID: 93

Incident Type: Exchange

Created Date: Jan, 23, 2025, 04:30 PM

Alert

The SIEM alert notified us that there is a “Phishing Email Detected”. On “**Jun, 13, 2021, 02:13 PM**” an email was allowed to be sent to a user, “**Lars**”, to the address “**lars@letsdefend.io**” from the source address “**trenton@tritowncomputers.com**”. The email’s SMTP address is “**24.213.228.54**”. The subject line of the email reads “**Meeting Notes**”

This alert has been re-investigated

⭐ This alert was generated from a real phishing attack.

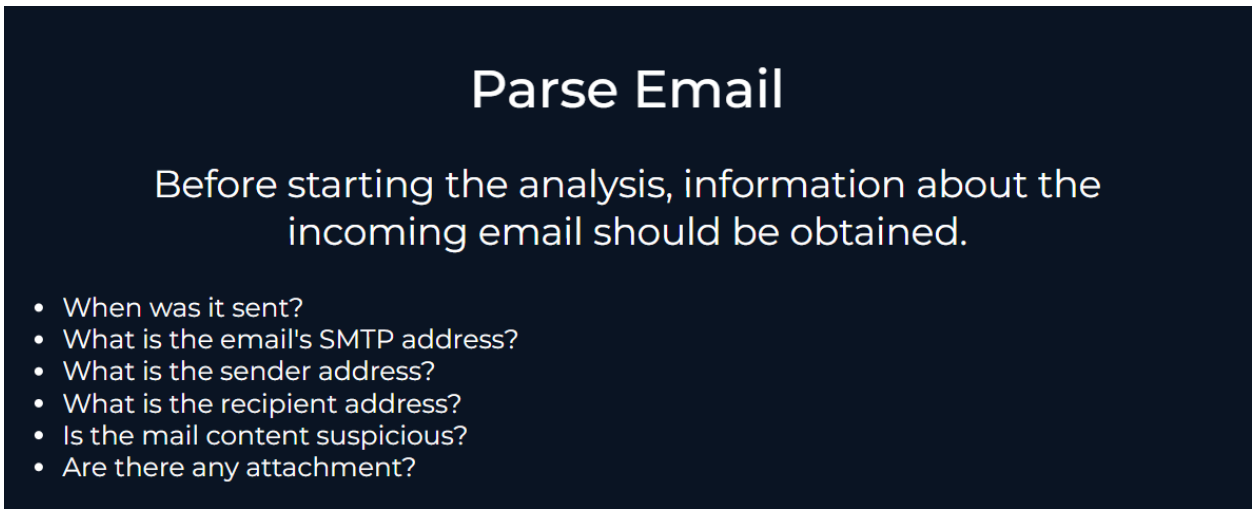
EventID :	93
Event Time :	Jun, 13, 2021, 02:13 PM
Rule :	SOC146 - Phishing Mail Detected - Excel 4.0 Macros
Level :	Security Analyst
SMTP Address :	24.213.228.54
Source Address :	trenton@tritowncomputers.com
Destination Address :	lars@letsdefend.io
E-mail Subject :	RE: Meeting Notes
Device Action :	Allowed

Show Hint

There seems to be a high probability that this is a **phishing** email.

Detection

The playbook calls for us to parse the email.



When was it sent?

Jun, 13, 2021, 02:13 PM

What is the email's SMTP address?

24.213.228.54

What is the sender address?

trenton@tritowncomputers.com

What is the recipient address?

lars@letsdefend.io

Is the mail content suspicious?

Yes

Are there any attachments?

Yes, zip file called “11f44531fb088d31307d87b01e8eabff”
https://files-ld.s3.us-east-2.amazonaws.com/b6fab9a8-3dab-4bf8-a2cb-b955b0c00ce8-11f44531fb088d31307d87b01e8eabff.zip

From: trenton@tritowncomputers.com

To: lars@letsdefend.io

Subject: RE: Meeting Notes

Date: Jun, 13, 2021, 02:11 PM

Action: Action

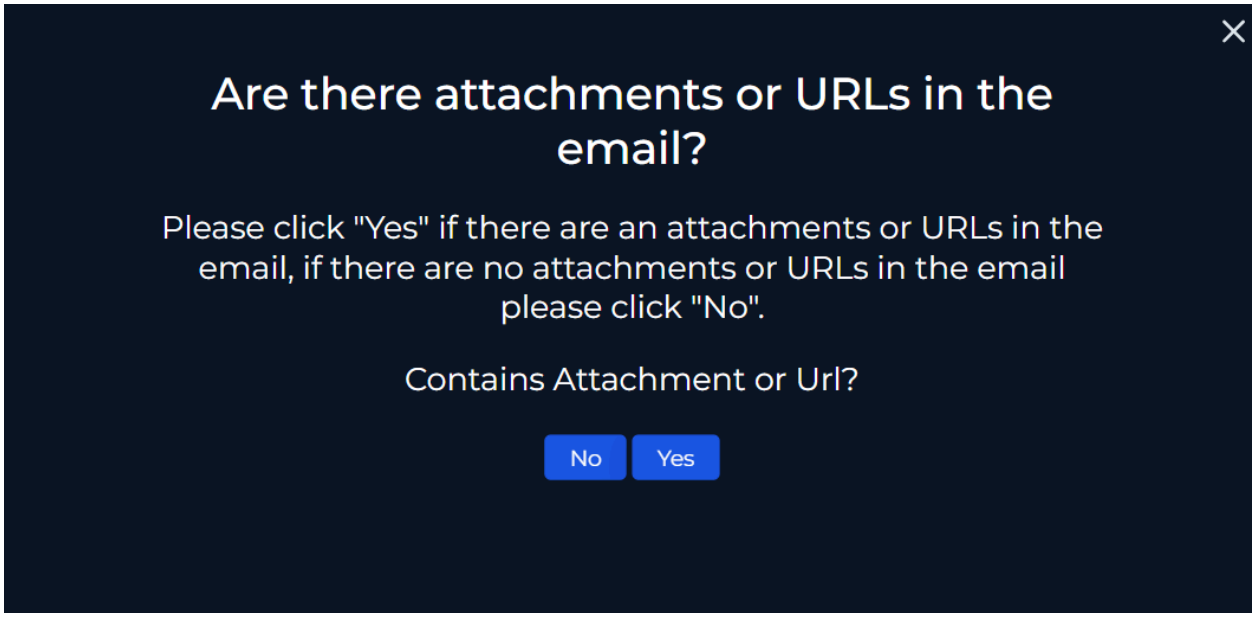
Hello! Please inspect your docs as one document that you can find through the attachment.

Attachments

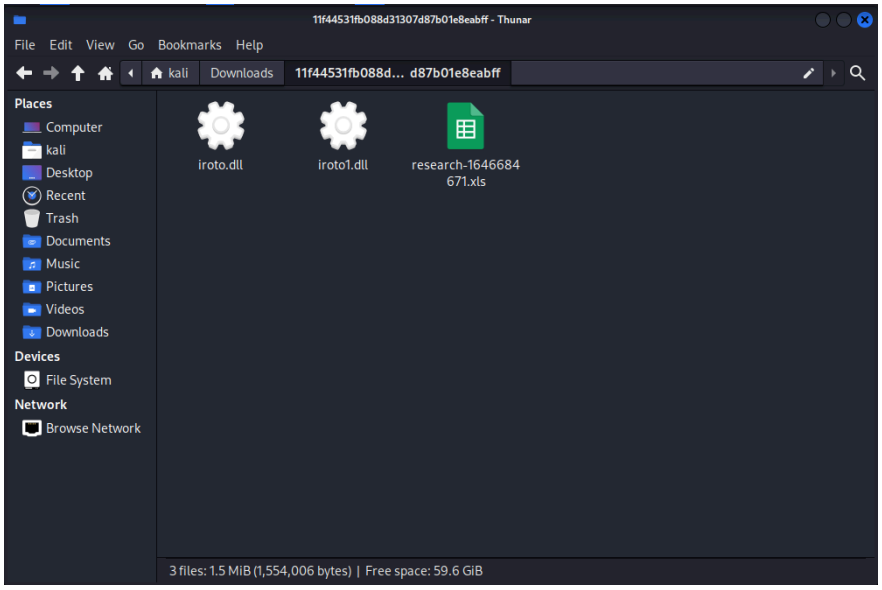
11f44531fb088d31307d87b01e8eabff

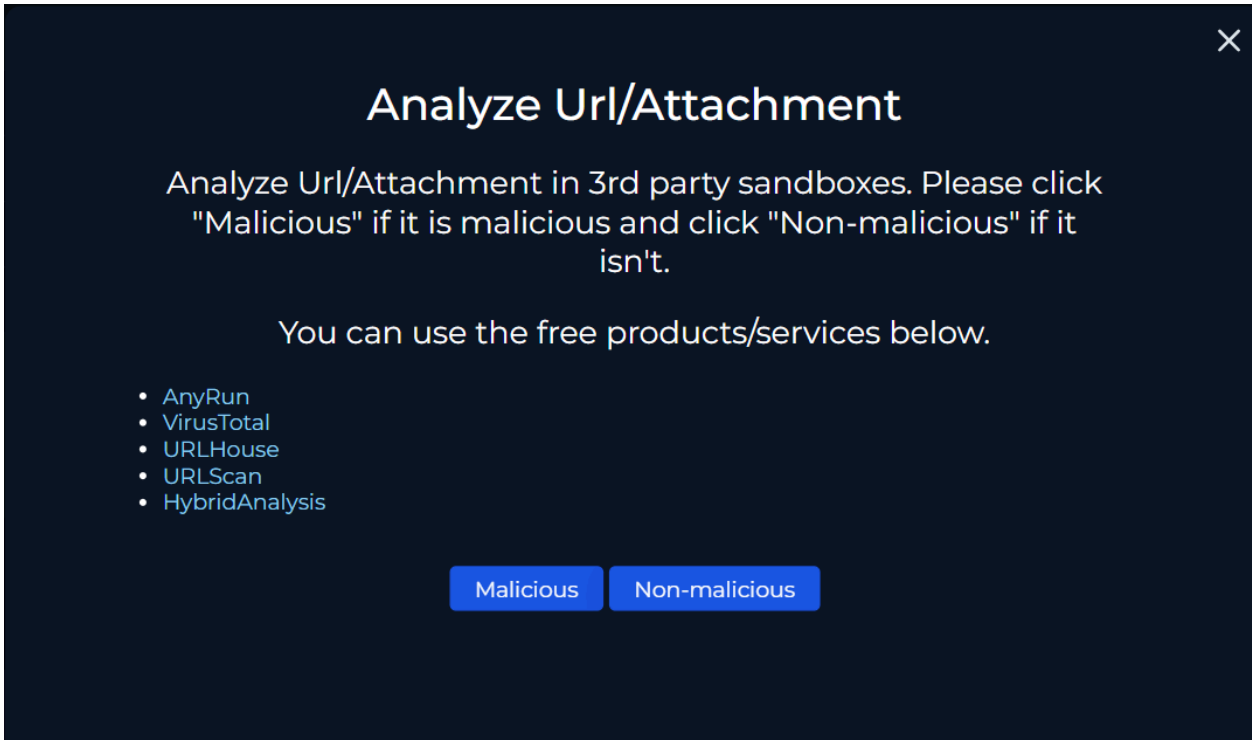
Password: infected

Analysis

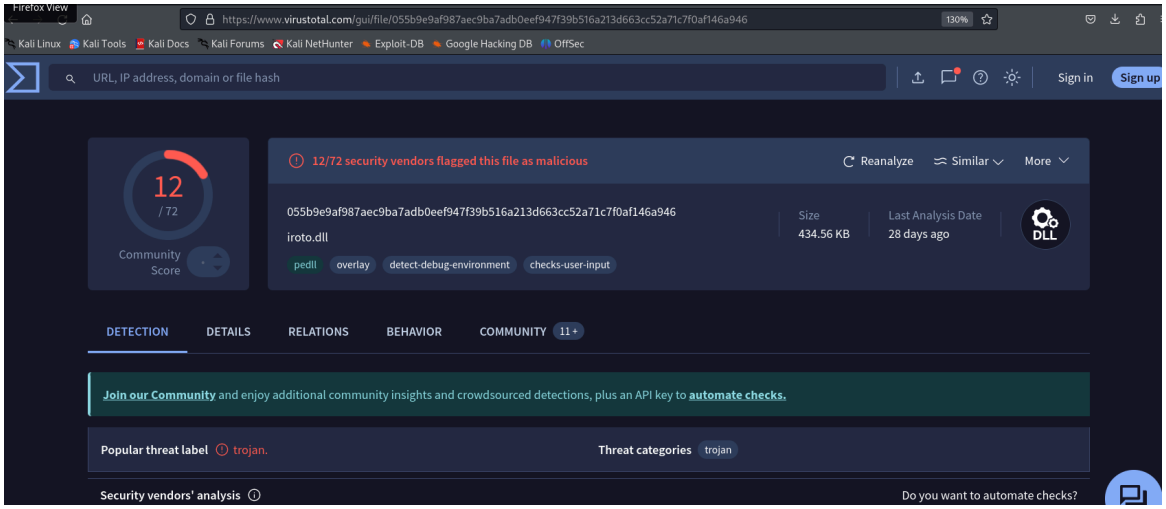


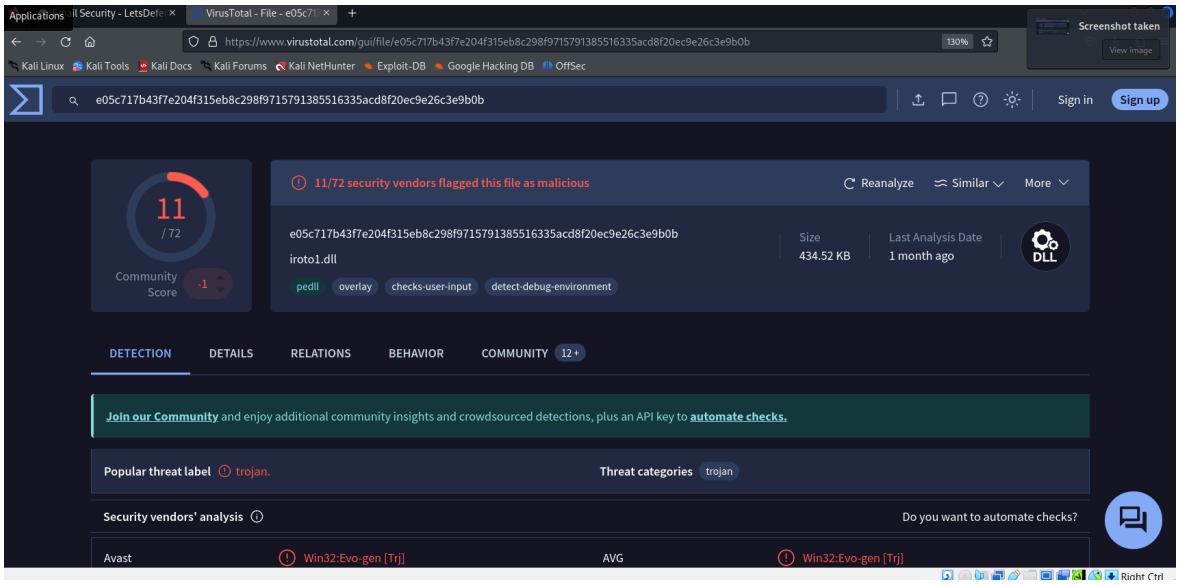
Now we must verify whether or not there are any attachments or URLs in the email. We could see clearly from the email that there is an attachment “11f44531fb088d31307d87b01e8eabff”. We downloaded it in a Kali Linux virtual machine. After downloading the ZIP and extracting it we can clearly see three files: “**iroto.dll**”, “**iroto1.dll**”, and “**research-1646684671.xls**”.

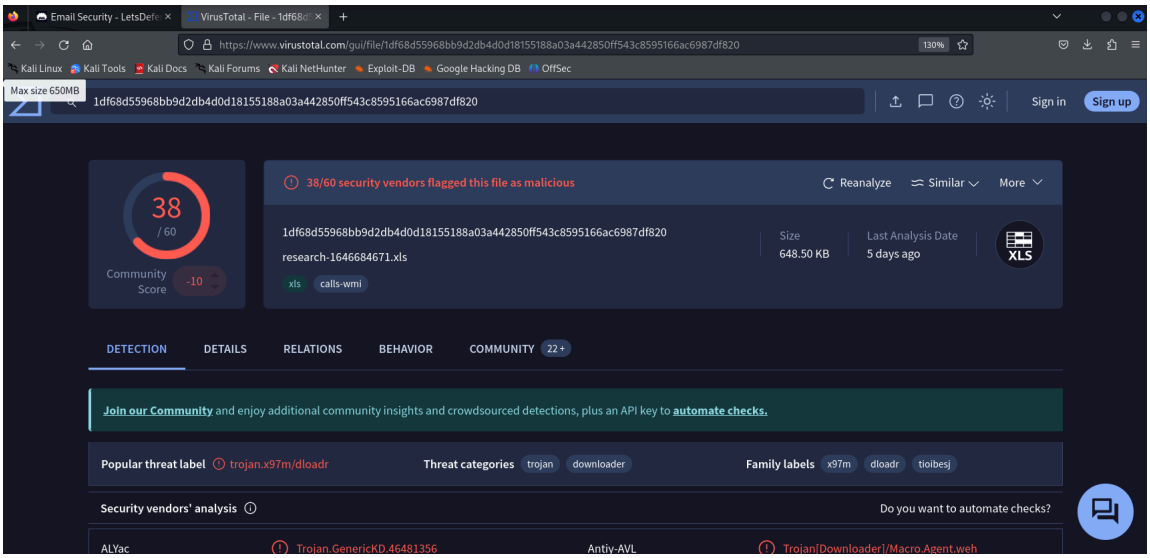




Now, we need to analyze the files we downloaded from the email attachment. We put the files into VirusTotal and we see that each file has been flagged as malicious by security vendors. The two .dll files are labeled as trojans, while the Microsoft Excel file is labeled as a Trojan.X97M/Dloadr, which is a trojan located in the macros that can download additional malware. So if the .xls file is opened and macros are enabled then the computer will be infected by malware.




Applications
VirusTotal - File - e05c71
https://www.virustotal.com/gui/file/e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b
Screenshot taken
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b
Sign in
Sign up
11
/ 72
Community Score
11/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b
iroto1.dll
pedll overlay checks-user-input detect-debug-environment
Size
434.52 KB
Last Analysis Date
1 month ago
DLL
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.
Threat categories trojan
Security vendors' analysis
Do you want to automate checks?
Avast Win32:Evo-gen [Trj]
AVG Win32:Evo-gen [Trj]


Email Security - LetsDefe
VirusTotal - File - 1df68d
https://www.virustotal.com/gui/file/1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Max size 650MB
1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820
Sign in
Sign up
38
/ 60
Community Score
38/60 security vendors flagged this file as malicious
Reanalyze
Similar
More
1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820
research-1646684671.xls
xls calls-wmi
Size
648.50 KB
Last Analysis Date
5 days ago
XLS
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 22+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.x97m/dloadr
Threat categories trojan downloader
Family labels x97m dloadr tioibesj
Security vendors' analysis
Do you want to automate checks?
ALYac Trojan.GenericKD.46481356
Antiy-AVL Trojan[Downloader]/Macro.Agent.weh

Check If Mail Delivered to User?

Answer the following question by determining whether the e-mail is delivered by looking at the "device action" part of the alert details.

Delivered | Not Delivered

This alert has been re-investigated

This alert was generated from a real phishing attack.

EventID :	93
Event Time :	Jun, 13, 2021, 02:13 PM
Rule :	SOC146 - Phishing Mail Detected - Excel 4.0 Macros
Level :	Security Analyst
SMTP Address :	24.213.228.54
Source Address :	trenton@tritowncomputers.com
Destination Address :	lars@letsdefend.io
E-mail Subject :	RE: Meeting Notes
Device Action :	Allowed

Show Hint

Date	Sender	Recipients	Subject	Final Action
Jun, 13, 2021, 02:11 PM	Trenton	Lars	RE: Meeting Notes	Unknown

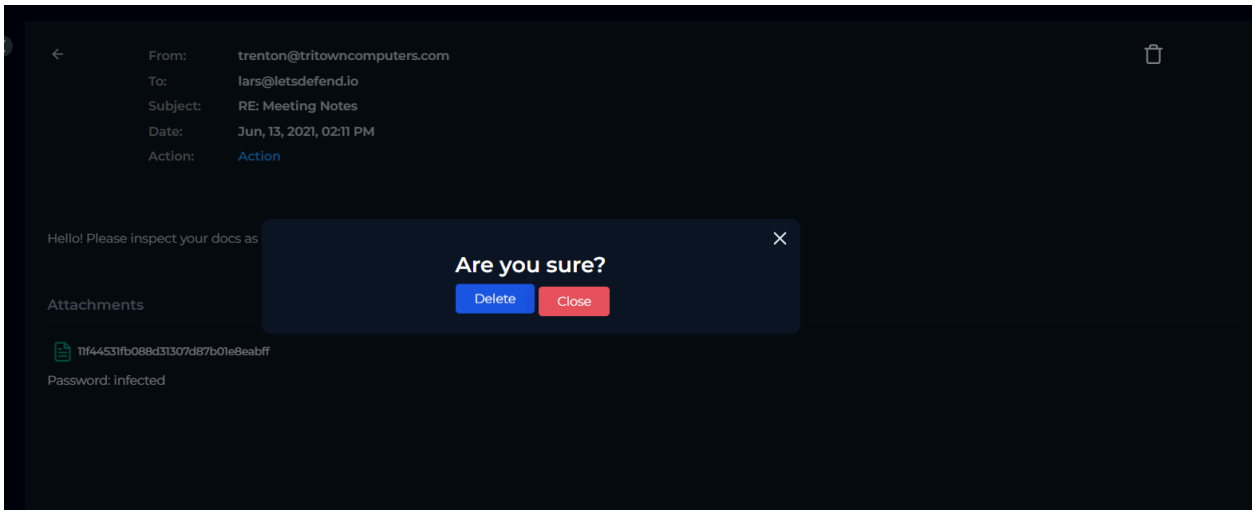
To check to see if the email was delivered to the user, we can simply go to the alert and look at “Device Action”. Here we see that it was allowed.

Delete Email From Recipient!

You should delete the malicious email from user's mailbox.
Please click "DELETE" button to delete malicious email.

Delete

We have verification that the email was delivered so we delete the malicious email from Lars's mailbox.



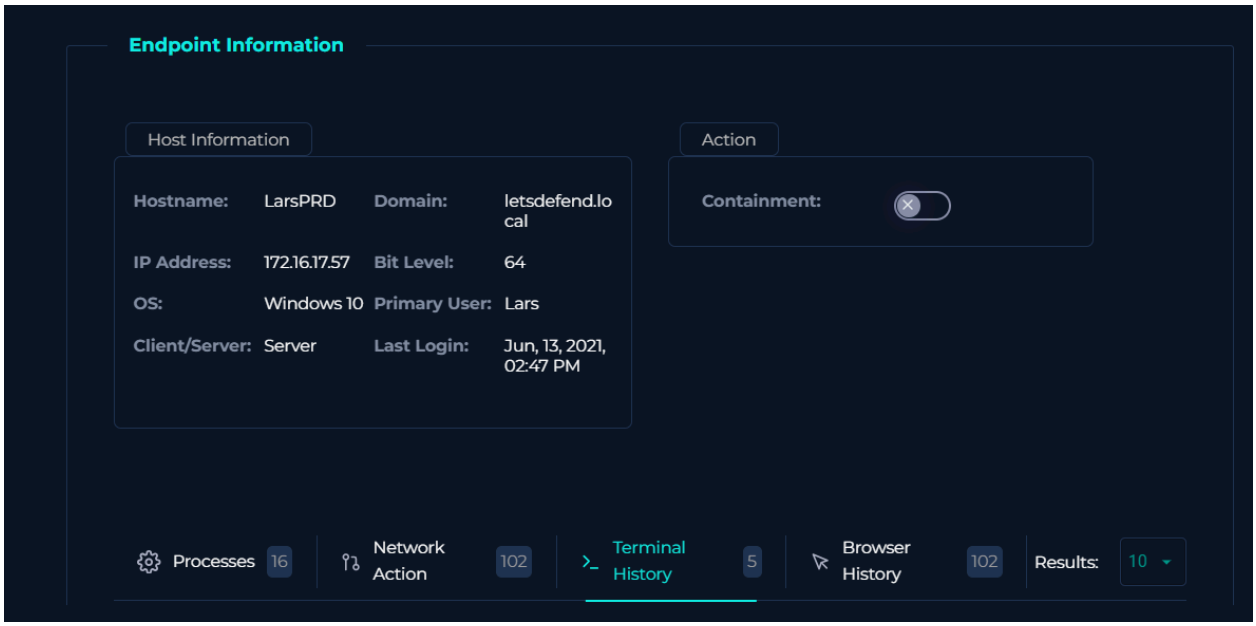
Check If Someone Opened the Malicios File/URL?

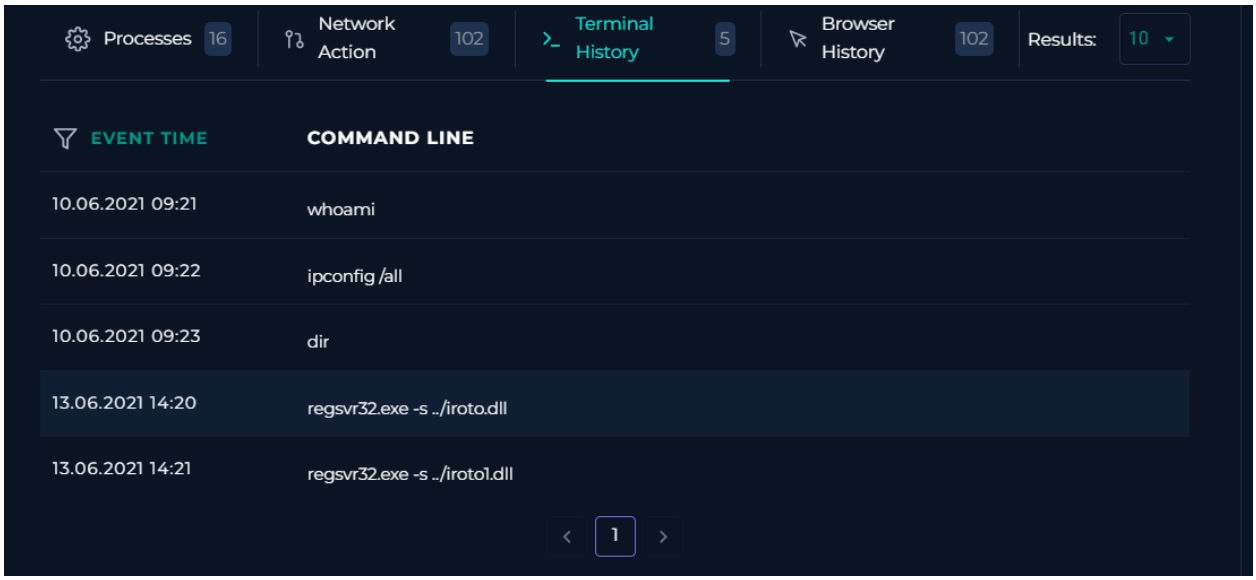
Please go to the "Log Management" page and check if the c2 address accessed. You can check if the malicious file is run by searching the c2 addresses of the malicious file.

Please click "Opened" if someone access the malicious address. Otherwise please click "Not Opened" button.

Not Opened | Opened

To check if someone opened the malicious file or malicious URL we first go to the user endpoint. We check Lars's Terminal History, and we see that commands that ran the malicious .dll files have been executed. So we know that Lars must have opened the malicious file.





In Log Management we look up Lars's IP Address and see that he connected to two malicious URLs.

Basic

Show Filter

172.16.17.57

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 13, 2021, 11:20 AM	Proxy	172.16.17.57	43633	188.213.19.81	443	
Jun, 13, 2021, 11:20 AM	Proxy	172.16.17.57	45235	192.232.219.67	443	

Basic Pro

Show Filter

172.16.17.57

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 13, 2021, 11:20 AM				188.213.19.81	443	
Jun, 13, 2021, 11:20 AM				192.232.219.67	443	

RAW LOG

Request URL: https://nws.visionconsulting.ro/N1G1KCXA/dot.html
Request Method: GET
Device Action: Allowed
Process: excel.exe
Parent Process: explorer.exe
Parent Process MD5: 8b88ebbb05a0e56b7dcc708498c02b3e

6 / 96

Community Score

6/96 security vendors flagged this URL as malicious

Reanalyze Search More

https://nws.visionconsulting.ro/N1G1KCXA/dot.html
nws.visionconsulting.ro

text/html

Status	Content type	Last Analysis Date
404	text/html	13 days ago

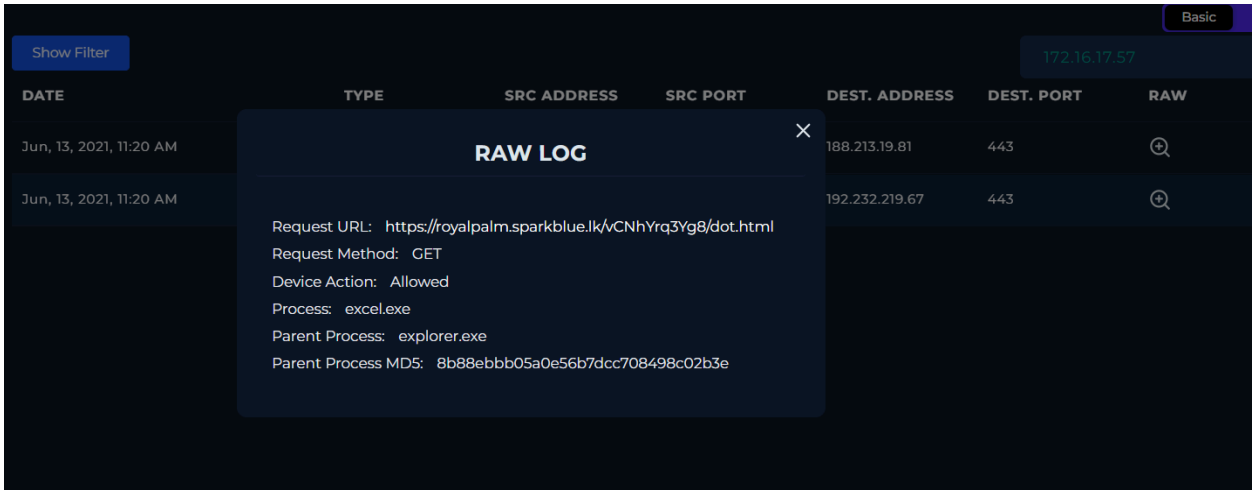
DETECTION DETAILS COMMUNITY 1

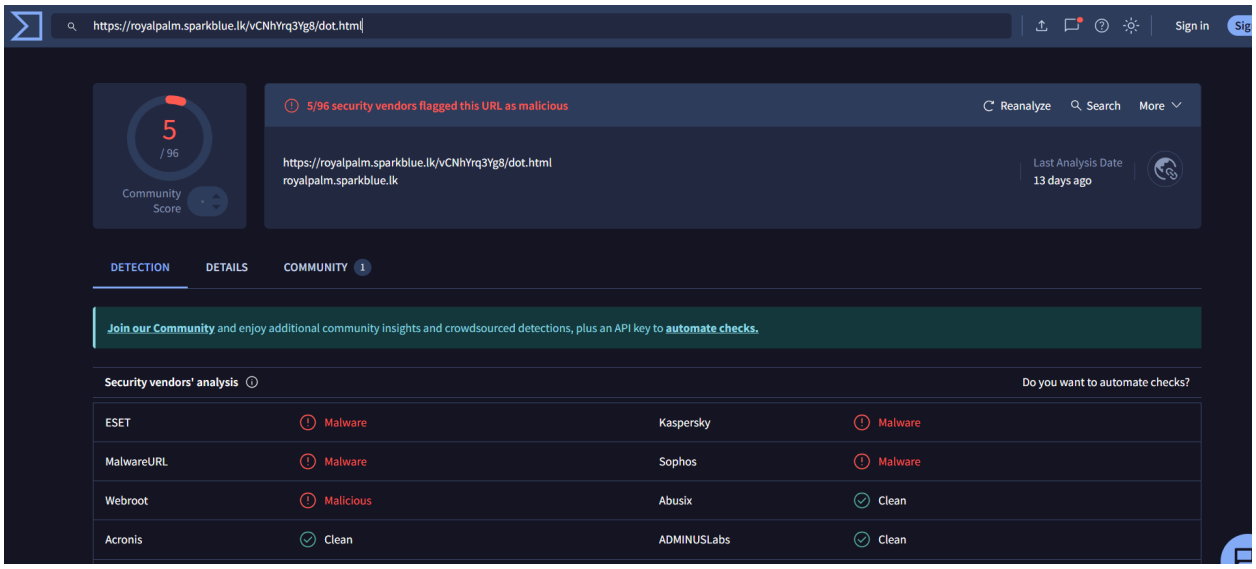
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	ESET	Malware
Kaspersky	Malware	MalwareURL	Malware
Sophos	Malware	Webroot	Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean





We then go back to his Endpoint and see that the two malicious IPs are in his Network History. The C2 IP's are "**192.232.219.67**" and "**188.213.19.81**".

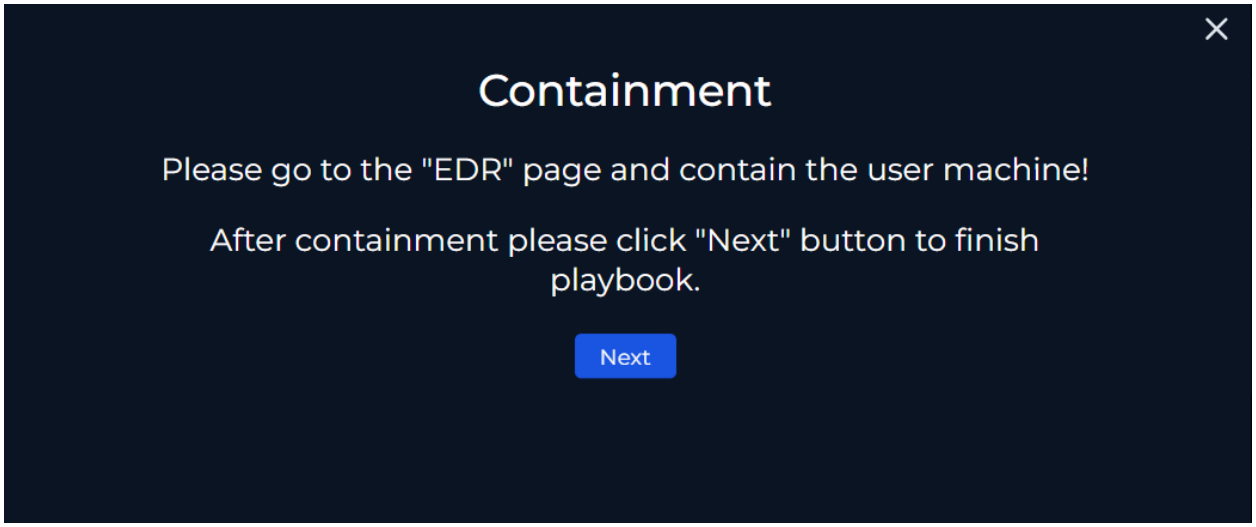
lars

LabServer
192.168.10.15

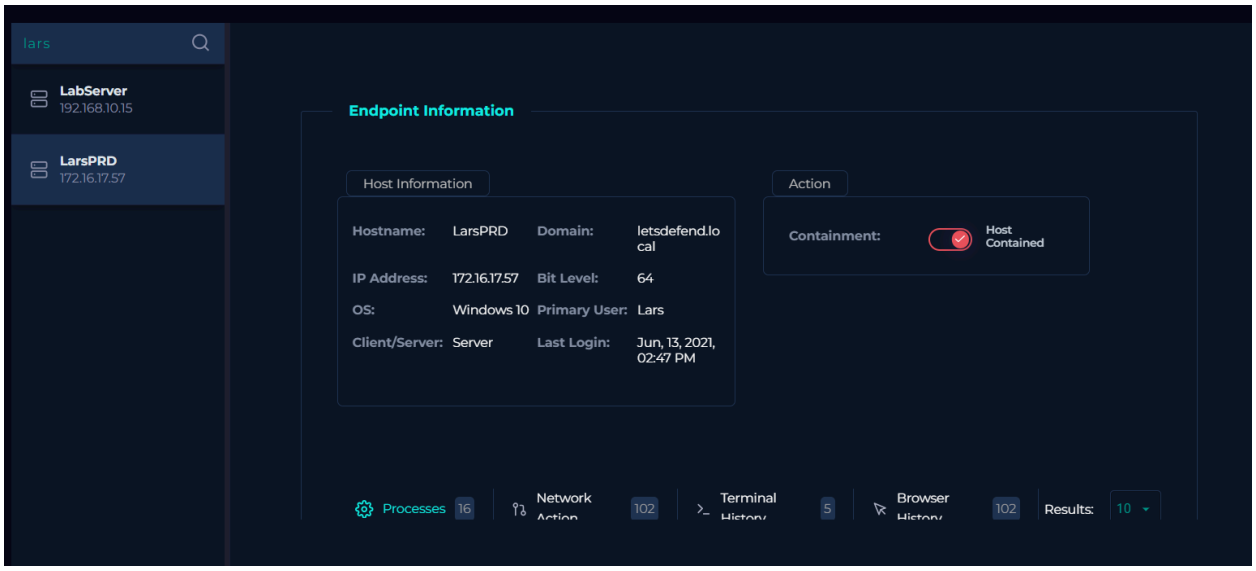
LarsPRD
172.16.17.57

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS ↓
07.05.2021 23:46	213.248.110.126
08.05.2021 13:57	213.248.110.126
09.05.2021 18:19	199.232.56.95
25.05.2021 02:21	199.232.56.95
13.06.2021 14:21	192.232.219.67
13.06.2021 14:20	188.213.19.81
10.05.2021 08:15	185.85.0.29
06.05.2021 08:53	185.60.218.36
07.05.2021 21:48	185.60.218.36

Containment



Now, in order to prevent any more damage to the security posture of the organization we must contain his host machine.



Lessons Learned

- Users must be cautious about clicking on links or downloading attachments sent by email
- Phishing emails are designed to look legitimate, but users must be aware of the phishing email indicators

Remediation Actions

- Provide awareness training to users, teaching them how to determine if an email is a phishing email and what they should do if they realize it is a phishing email
- Implement email filtering and security measures, such as DKIM and SPF, to help detect and block spoofed emails.
- Reset any compromised user credentials and implement a strong password policy
- Restrict macro execution in Excel
- Use Windows Defender Application Control to block unsigned macros and unknown DLLs

Appendix

MITRE ATT&CK

Tactic: Initial Access

- Technique: Phishing (T1566.001 - Spear Phishing Attachment)
  The attack begins with a phishing email containing a malicious attachment. The email bypassed initial defenses and reached the user's inbox.

Tactic: Execution

- Technique: User Execution (T1204.002 - Malicious File)
  The user executed the malicious Excel file, which contained Excel 4.0 Macros. These macros are often leveraged for payload execution without requiring user interaction beyond enabling content.
- Technique: Command and Scripting Interpreter (T1059.003 - Windows Command Shell)
  Commands such as `regsvr32.exe -s ../iroto.dll` and `regsvr32.exe -s ../iroto1.dll` were executed. This indicates the use of `regsvr32.exe` to execute DLL files, which can bypass application whitelisting.

Tactic: Defense Evasion

- Technique: Masquerading (T1036)
  The use of `regsvr32.exe` is a legitimate tool commonly used by Windows, making it harder for security solutions to detect malicious activity.

- Technique: Obfuscated Files or Information (T1027)
  The use of DLL files and encoded strings within the phishing email suggests obfuscation to avoid detection by antivirus engines.

Tactic: Persistence

- Technique: Scheduled Task/Job (T1053.005) *(Potentially Implied)*
  Although not explicitly mentioned, DLL files and malicious macros can be used to establish persistence.

Tactic: Discovery

- Technique: System Information Discovery (T1082)
  The malicious attachment likely collected system information to determine the environment before executing further actions.

Tactic: Command and Control (C2)

- Technique: Application Layer Protocol (T1071.001 - Web Protocols)
  Communication with malicious domains and IP addresses using HTTP/HTTPS is a hallmark of command and control.
- Technique: Remote File Copy (T1105)
  The malicious Excel file attempted to download additional payloads or communicate with C2 servers via URLs.

Tactic: Exfiltration

- Technique: Exfiltration Over C2 Channel (T1041)
  The malicious domains and IP addresses could also serve to exfiltrate sensitive data from the compromised machine.

Tactic: Impact

- Technique: Data Destruction (T1485) *(Potentially Implied)*
  If the malicious payload included data-destroying capabilities, it could lead to significant damage.

Tactic: Impact

- Technique: Data Destruction (T1485) *(Potentially Implied)*
  If the malicious payload included data-destroying capabilities, it could lead to significant damage.

Artifacts

IOC	Value
URL	https://files-ld.s3.us-east-2.amazonaws.com/b6fab9a8-3dab-4bf8-a2cb-b955b0c00ce8-11f44531fb088d31307d87b01e8eabff.zip
SMTP Address	24.213.228.54
C2 Addresses	192.232.219.67 188.213.19.81
research-1646684671.xls	1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820