

SOC146 - Phishing Mail Detected - Excel 4.0 Macros

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Jun, 13, 2021, 02:13 PM	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros	93	Exchange	» ✓
★ 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 ⚙					

Click on >> and create case and click Continue.

Incident Details	
Incident Name:	EventID: 93 - [SOC146 - Phishing Mail Detected - Excel 4.0 Macros]
Description:	EventID: 93
Incident Type:	Exchange
Created Date:	Jan, 07, 2024, 03:44 PM
Start Playbook!	

Before we start the playbook, let’s initialize our analysis with what we have with us already.

The rule talks about “Phishing Mail Detected - Excel 4.0 Macros”... so our first hit should be at the Mailbox.

Click on Email Security and search for the mail with “RE: Meeting Notes” as mentioned in the alert.

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

←	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		

In order to analyse if the email is a Phishing Mail, we need to investigate the attachment. **It should be noted that we may be dealing with a potential malware and as such the usage of a Sandbox is highly advised.**

Let's check the reputation of the email we received the mail from.

tritoncomputers.com

0

/ 89

Community Score

1 detected file communicating with this domain

tritoncomputers.com

Registrar
GoDaddy.com, LLC

Cr
13

computersandsoftware information technology public information top-1M

DETECTION DETAILS RELATIONS COMMUNITY 1

The domain tritoncomputers.com has a relation to a file which is malicious and has been flagged as a Trojan.

Communicating Files (1)

Scanned	Detections	Type	Name
2022-07-25	6 / 70	Win32 EXE	fixthisjunk.exe

4c2b1ef16ab576456cc41901421a2c6b409eecd34f3c2a90a73d58207e2f02

6

/ 70

Community Score

6 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

4c2b1ef16ab576456cc41901421a2c6b409eecd34f3c2a90a73d58207e2f02

Size
2.77 MB

Last Analysis Date
1 year ago

EXE

peexe overlay

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Join the VT 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?

Cybereason	Malicious.7fd8e6	Cylance	Unsafe
Cynet	Malicious (score: 100)	MaxSecure	Trojan.Malware.300983.susgen
Trapsmine	Suspicious.low.ml.score	VBA32	TScope.Trojan.Delf

Upon downloading and opening the attachment, the contents are as follows:

<< Users > letsdefend > Downloads > 11f44531fb088d31307d87b01e8eabff > 11f44531fb08

Name	Type	Compressed
iroto.dll	Application extension	
iroto1.dll	Application extension	
research-1646684671.xls	XLS File	

A dll file within an attachment doesn't look good in itself. Moving further.

Now to check the reputation of the files, we find out their MD5 Hashes and search for them on Virustotal.

iroto.dll -> E03BDE4862D4D93AC2CEED85ABF50B18

iroto1.dll -> 8E6FBFCBAC2A1967941FA692C82C3CA

research-1646684671.xls -> B775CD8BE83696CA37B2FE00BCB40574

11

/ 66

Community Score

11 security vendors and no sandboxes flagged this file as malicious

055b9e9af987aec9ba7adb0eef947f39b516a213d663cc52a71c7f0af146a946

iroto.dll

Size434.56 KB

Last Analysis Date2 days ago

DLL

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY11

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

Popular threat labeltrojan

Threat categoriestrojan

Security vendors' analysis

Do you want to automate checks?

Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Bkav Pro	W32.AIDetectMalware	DeepInstinct	MALICIOUS
Fortinet	W32/Qshell.VHO!tr	MaxSecure	Trojan.Malware.3411146.susgen
McAfee	Artemis!E03BDE4862D4	Rising	Trojan.Generic@AI.90 (RDML:Ob4/VcDN...
Sangfor Engine Zero	Trojan.Win32.Agent.V7wi	SecureAge	Malicious
Skyhigh (SWG)	Artemis	Acronis (Static ML)	Undetected

11

/ 67

Community Score

11 security vendors and no sandboxes flagged this file as malicious

e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b

iroto1.dll

Size434.52 KB

Last Analysis Date2 days ago

DLL

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY12

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

Popular threat labeltrojan

Threat categoriestrojan

Security vendors' analysis

Do you want to automate checks?

Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Bkav Pro	W32.AIDetectMalware	DeepInstinct	MALICIOUS
Fortinet	W32/Qshell.VHO!tr	MaxSecure	Trojan.Malware.3411146.susgen
McAfee	Artemis!8E6FBFCBAC2	Rising	Trojan.Generic@AI.90 (RDML:Ob4/VcDN...
Sangfor Engine Zero	Trojan.Win32.Agent.Vbdc	SecureAge	Malicious
Skyhigh (SWG)	Artemis	Acronis (Static ML)	Undetected

39

/ 61

Community Score

39 security vendors and 0 sandboxes flagged this file as malicious

1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820

research-1646684671.xls

Size648.50 KB

Last Analysis Date15 days ago

XLS

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY18

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

Popular threat labeltrojan.x97m/dloader

Threat categoriestrojandownloader

Family labelsx97mdloadertioibesj

Security vendors' analysis

Do you want to automate checks?

ALYac	Trojan.GenericKD.46481356	Antiy-AVL	Trojan[Downloader]/Macro.Agent.weh
Arcabit	Trojan.Generic.D2C53FCC	Avast	VBS:Malware-gen
AVG	VBS:Malware-gen	Avira (no cloud)	XFI/Agent.B2
BitDefender	Trojan.GenericKD.46481356	Cynet	Malicious (score: 99)
DrWeb	X97M.DownLoader.782	Emsisoft	Trojan.GenericKD.46481356 (B)
eScan	Trojan.GenericKD.46481356	ESET-NOD32	A Variant Of VBA/TrojanDownloader.Agen...

Activity Summary

3 Detections

4 MALWARE 1 TROJAN
1 EVADER

Mitre Signatures

4 HIGH 6 LOW 23 INFO

IDS Rules

1 HIGH

Behavior Tags

calls-wmi detect-debug-environment unknown-behaviour

Dynamic Analysis Sandbox Detections

- The sandbox **Zenbox** flags this file as: MALWARE TROJAN EVADER
- The sandbox **ReaQta-Hive** flags this file as: MALWARE
- The sandbox **DOCGuard** flags this file as: MALWARE
- The sandbox **BitDam ATP** flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

- + Execution TAO002
- + Persistence TAO003
- + Privilege Escalation TAO004
- + Defense Evasion TAO005
- + Discovery TAO007
- + Command and Control TAO011

So, by virtue of all the finding, we can conclude that the attachment is indeed highly malicious.

Let's start the Playbook.

Parse Email

Before starting the analysis, information about the incoming email should be obtained.

- When was it sent?
- What is the email's SMTP address?
- What is the sender address?
- What is the recipient address?
- Is the mail content suspicious?
- Are there any attachment?

Next

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 attachment? Yes

“Yes” has been marked against “Is the mail content suspicious?” because if we notice the personalisation is generic with just a “Hello!” and the rest of the sentence doesn’t sound grammatically correct as well.

×

Are there attachments or URLs in the email?

Please click "Yes" if there are an attachments or URLs in the email, if there are no attachments or URLs in the email please click "No".

Contains Attachment or Url?

Selecting Yes here.

×

Analyze Url/Attachment

Analyze Url/Attachment in 3rd party sandboxes. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

As determined previously, the attachment is Malicious.

×

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.

Device Action :	Allowed
-----------------	---------

We did find the mail in the mailbox, so selecting Delivered here.

✕

Delete Email From Recipient!

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

Delete

←


From: trenton@tritowncomputers.com

To: lars@letsdefend.io

Subject: RE: Meeting Notes

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


Action: [Action](#)



Delete

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

Attachments



11f44531fb088d31307d87b01e8eabff

Password: infected

Delete the email from the mailbox and click the DELETE button on the playbook.

✕

Check If Someone Opened the Malicious 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

Now to check if Lars did or did not open the file, we need to look into his endpoint.

Lars

LarsPRD
172.16.17.57

LabServer
192.168.10.15

Host Information

Hostname: LarsPRD

Domain: letsdefend.local

IP Address: 172.16.17.57

Bit Level: 64

OS: Windows 10

Primary User: Lars

Client/Server: Server

Last Login: Jun, 13, 2021, 02:47 PM

Action

Containment: ☒

Last Login: Jun, 13, 2021, 02:47 PM for Lars on the machine is approximately similar to Event date & time.

We see that the DLLs sprung into action suggesting the excel has been opened.

EVENT TIME	COMMAND LINE
10.06.2021 09:21	whoami
10.06.2021 09:22	ipconfig /all
10.06.2021 09:23	dir
13.06.2021 14:20	regsvr32.exe -s ../iroto.dll
13.06.2021 14:21	regsvr32.exe -s ../iroto1.dll

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS
✓ No Event Time	No Process ID	OUTLOOK.exe	—
✓ No Event Time	No Process ID	taskhostw.exe	—
^ No Event Time	No Process ID	regsvr32.exe	—
MD5 : b0c2fa35d14a9fad919e99d9d75e1b9e			
Size : 96.0 KB			
Path : C:/Windows/System32/regsvr32.exe			
Parent : C:/Windows/System32/excel.exe			
Command Line : regsvr32.exe -s iroto.dll			

So, we can safely select that the file was “Opened”.

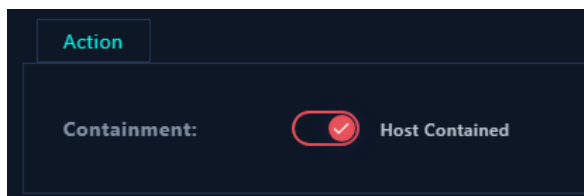
×

Containment

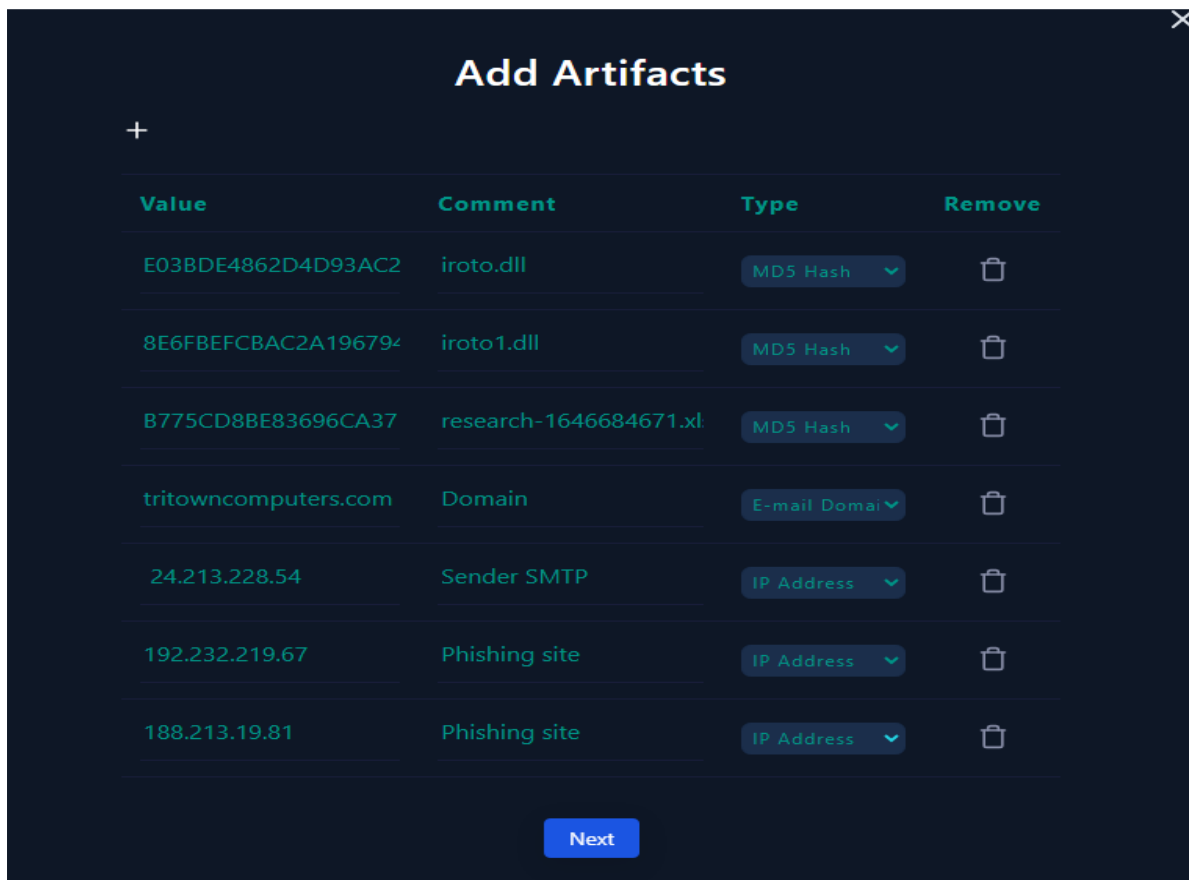
Please go to the "EDR" page and contain the user machine!

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

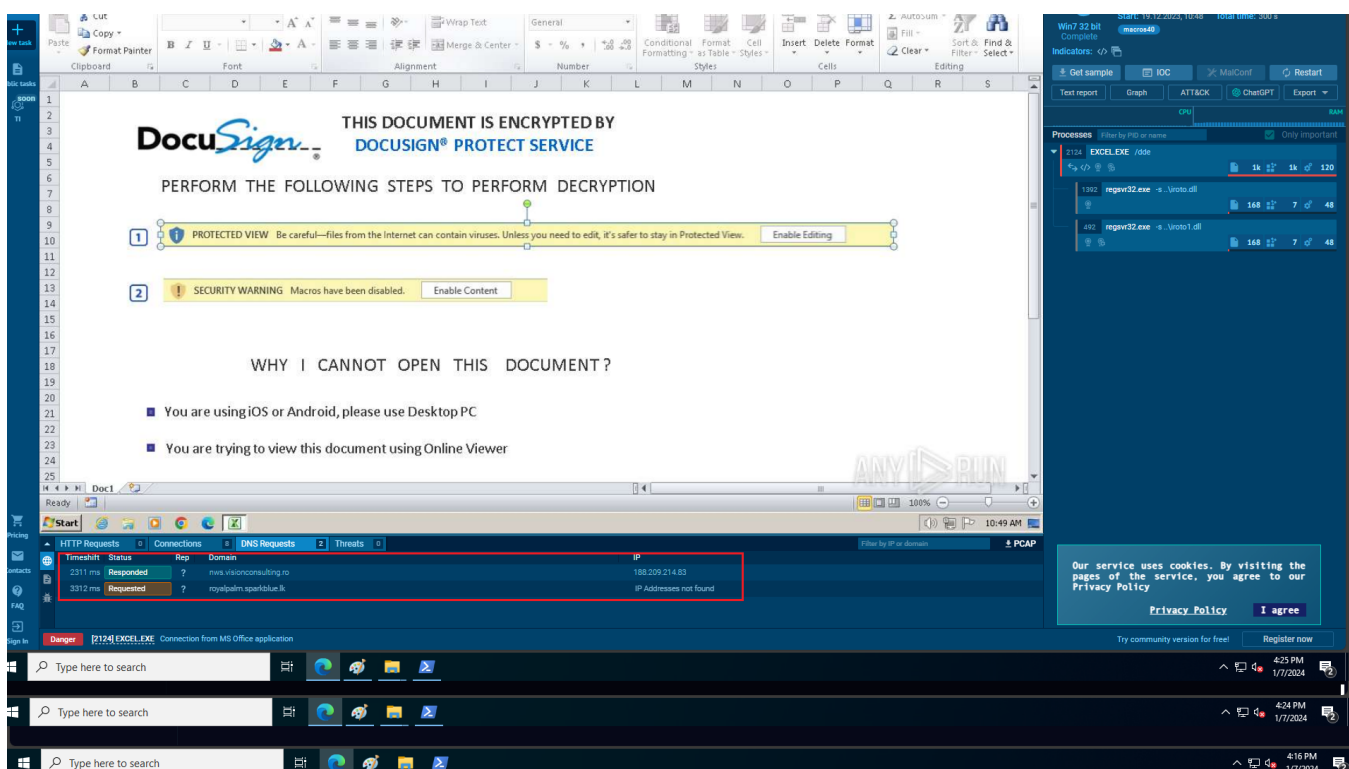
Next



Host “LardPRD” has now been contained.



Added artifacts based on our investigation. The Phishing site addresses were determined based on our investigation in app.any.run against the MD5 has of the malicious excel file.



And these were confirmed as logs present.

Event

[Jun, 13, 2021, 02:20 PM] source_address=172.16.17.57 source_port=43633 destination_address=188.213.19.81 destination_port=443 raw_log: {Request URL: 'https://nws.visionconsulting.ro/N1G1KCXA/dot.html', 'Req...

Field	Value
type	Proxy
source_address	172.16.17.57
source_port	43633
destination_address	188.213.19.81
destination_port	443
time	Jun, 13, 2021, 02:20 PM
Raw Log	
Request URL	https://nws.visionconsulting.ro/N1G1KCXA/dot.html

Event

[Jun, 13, 2021, 02:20 PM] source_address=172.16.17.57 source_port=45235 destination_address=192.232.219.67 destination_port=443 raw_log: {Request URL: 'https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html', '...

Field	Value
type	Proxy
source_address	172.16.17.57
source_port	45235
destination_address	192.232.219.67
destination_port	443
time	Jun, 13, 2021, 02:20 PM
Raw Log	
Request URL	https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html

Analyst Note

Please enter your analysis comments.

The email sent to Lars was determined as a phishing email based on the analysis. The attachments contained 3 files where clicking the excel files would trigger the execution of the DLL files.

The endpoint has been contained as it was determined that the file was opened. The mail domain and SMTP address should be added to the exchange blacklist.

~~The destination addresses which the malware was serving should be added to the~~

533 / 3000

Next

The email sent to Lars was determined as a phishing email based on the analysis. The attachments contained 3 files where clicking the excel files would trigger the execution of the DLL files.

The endpoint has been contained as it was determined that the file was opened.

The mail domain and SMTP address should be added to the exchange blacklist.

The destination addresses which the malware was serving should be added to the firewall.

Additionally, Lars should be made aware of cybersecurity threats by way of training/consultation.

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

×

Close Alert

Event ID :

93

True Positive False Positive

Note:

Additionally, Lars should be made aware of cybersecurity threats by way of training/consultation.

Close Alert

This would be a True Positive as it was indeed a “Phishing Email”.

Let’s check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 07, 2024, 07:54 PM	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros	93	Exchange	✓	↺
★ 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				
Answer :		True Positive (+5 Point)				
Playbook Answers :		Check If Someone Opened the Malicious File/URL? (+5 Point) Check If Mail Delivered to User? (+5 Point) Analyze Uri/Attachment (+5 Point) Are there attachments or URLs in the email? (+5 Point)				
Analyst Note :		The email sent to Lars was determined as a phishing email based on the analysis. The attachments contained 3 files where clicking the excel files would trigger the execution of the DLL files. The endpoint has been contained as it was determined that the file was opened. The mail domain and SMTP address should be added to the exchange blocklist. The destination addresses which the malware was serving should be added to the firewall. Additionally, Lars should be made aware of cybersecurity threats by way of training/consultation.				
Community Walkthrough :		Show				

Hopefully this helped.