

SOC140 - Phishing Mail Detected - Suspicious Task Scheduler

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	Mar, 21, 2021, 12:26 PM	SOC140 - Phishing Mail Detected - Suspicious Task Scheduler	82	Exchange	>> ✓
<div>EventID : 82</div> <div>Event Time : Mar, 21, 2021, 12:26 PM</div> <div>Rule : SOC140 - Phishing Mail Detected - Suspicious Task Scheduler</div> <div>Level : Security Analyst</div> <div>SMTP Address : 189,162,189,159</div> <div>Source Address : aaronluo@cmail.carleton.ca</div> <div>Destination Address : mark@letsdefend.io</div> <div>E-mail Subject : COVID19 Vaccine</div> <div>Device Action : Blocked</div>					

Click on >> and create case and click Continue.

Incident Details	
Incident Name:	EventID: 82 - [SOC140 - Phishing Mail Detected - Suspicious Task Scheduler]
Description:	EventID: 82
Incident Type:	Exchange
Created Date:	Jan, 07, 2024, 09:15 PM
<div>Start Playbook!</div>	

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

The rule talks about “**Phishing Mail Detected – Suspicious Task Scheduler**” ... so our first hit should be at the Mailbox.

Click on Email Security and search for the mail with “**COVID19 Vaccine**” as mentioned in the alert.

COVID19 Vaccine

OR

Detailed Search

Date	Sender	Recipients	Subject	Final Action
Mar, 21, 2021, 12:26 PM	aaronluo@email.carleton.ca	mark@letsdefend.io	COVID19 Vaccine	Unknown

←	From:	aaronluo@cmail.carleton.ca
	To:	mark@letsdefend.io
	Subject:	COVID19 Vaccine
	Date:	Mar, 21, 2021, 12:26 PM
	Action:	Action
Hey, did you read breaking news about Covid-19. Open it now!		
password: infected		
Attachments		
<div>72c812cf21909a48eb9cceb9e04b865d</div>		
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.

Lookup data results for IP Address

189.162.189.159

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data

LOCATION DATA

🇲🇽 Leon De Los Aldama, Mexico

OWNER DETAILS

IP ADDRESS	189.162.189.159
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	uninet

REPUTATION DETAILS

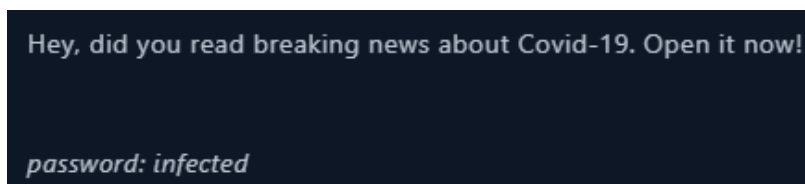
SENDER IP REPUTATION: Poor [Submit Sender IP Reputation Ticket](#)

WEB REPUTATION: Unknown [Submit Web Reputation Ticket](#)

EMAIL VOLUME DATA


	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Critical	

Upon checking the SMTP address is Talos Intelligence, the location of the server shows Mexico with Poor reputation and Critical Spam level. However, the domain Carleton.ca belongs to CA (Canada) which shows that **cmail.carleton.ca** is a spoofed mail domain.



The content of the email creates a certain type of urgency to open the attachment. The password of the attachment is *infected*. This further solidifies the fishy nature of the email.

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

Name	Date modified	Type	Size
 Material	1/7/2024 6:33 PM	Microsoft Edge P...	351 KB

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

Material.pdf -> 72C812CF21909A48EB9CCEB9E04B865D

39fb927c32221134a423760c5d1f58bca4cbbcc87c891c79e390a22b63608eb4

22 / 58

22 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

39fb927c32221134a423760c5d1f58bca4cbbcc87c891c79e390a22b63608eb4

Size 350.14 KB

Last Analysis Date 1 day ago

PDF

Material.pdf

pdf runtime-modules detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access checks-user-input acroform

Community Score

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY15

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

Popular threat label trojan.fraud

Threat categories trojan downloader

Family labels fraud

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Trojan[Downloader]/PDF.Agent	Arcabit	Trojan.PDF.Fraud.AD
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Trojan.PDF.Fraud.AD	DrWeb	PDF.DownLoader.359
Emsisoft	Trojan.PDF.Fraud.AD (B)	eScan	Trojan.PDF.Fraud.AD

Activity Summary

Detections

1 GREYWARE

Mitre Signatures

3 LOW 26 INFO

IDS Rules

1 MEDIUM

Sigma Rules

NOT FOUND

Behavior Tags

checks-network-adapters checks-user-input detect-debug-environment direct-cpu-clock-access long-sleeps runtime-modules

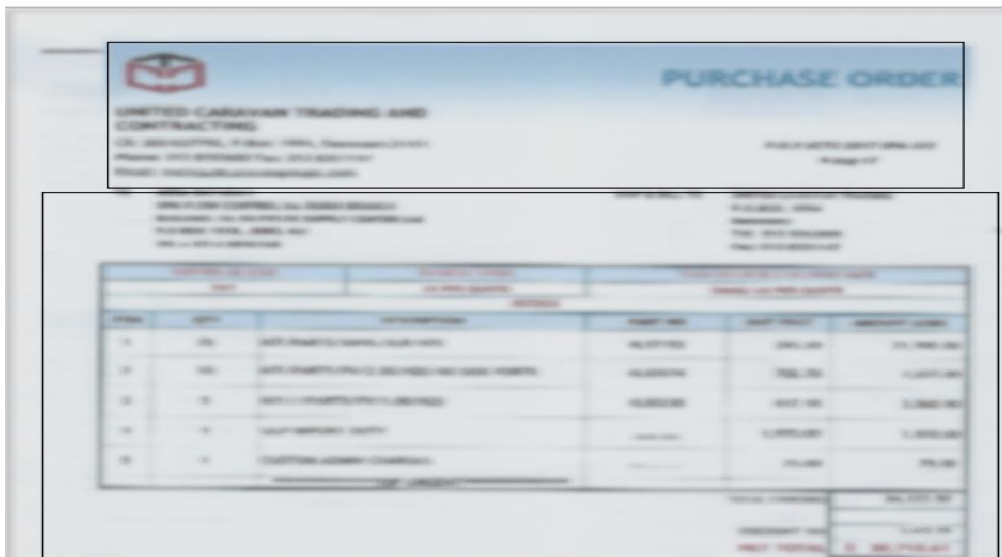
Dynamic Analysis Sandbox Detections

The sandbox DOCGuard flags this file as: GREYWARE

MITRE ATT&CK Tactics and Techniques

- + Initial Access TA0001
- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- + Collection TA0009
- + Command and Control TA0011

Upon opening the file, we see a blurred image of a what looks to be a Purchase Order



The file has an embedded link which we can copy without clicking and check its reputation.

https://a.pomf.cat/hgftb.R11

10 / 91

Community Score

10 security vendors flagged this URL as malicious

https://a.pomf.cat/hgftb.R11

a.pomf.cat

application/octet-stream, text/html

Status 200

Last Analysis Date 5 days ago

Did you intend to search across the file corpus instead? Click here

Reanalyze

Search

Graph

API

DETECTION

DETAILS

COMMUNITY

Join the VT 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?

Avira	Malware	BitDefender	Malware
ESET	Malware	Fortinet	Malware
G-DATA	Malware	Lionic	Malicious
malwares.com URL checker	Malicious	Sophos	Malware
VIPRE	Malware	Webroot	Malicious

HTTP Response ⓘ

Final URL

https://a.pomf.cat/hgftb.R11

Serving IP Address

69.39.225.3

Status Code

200

URLhaus mostly classifies this Domain containing RATs

URLhaus by ABUSE.ch

Browse

API

Feeds

S

Submit a URL

In order to submit a URL to URLhaus, you need to login with [your abuse.ch account](#)

Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2023-03-14 19:32:16	https://a.pomf.cat/pganjz.exe	Offline	bitrat exe rat	abuse_ch
2023-02-24 11:30:14	https://a.pomf.cat/ytxecu.hts	Offline		Anonymous
2023-02-22 11:41:12	https://a.pomf.cat/zxkqif.hta	Offline	ascii hta Loki	abuse_ch
2023-02-16 15:45:13	https://a.pomf.cat/kfbahy.hta	Offline	aggah	Anonymous
2022-12-01 15:06:11	https://a.pomf.cat/cbocwj.png	Offline	bitrat	abuse_ch
2022-12-01 15:05:13	https://a.pomf.cat/mhlewy.exe	Offline	bitrat exe	abuse_ch
2022-11-24 09:41:11	https://a.pomf.cat/jdcqfw.jpeg	Offline	bitrat encrypted	abuse_ch

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? Mar, 21, 2021, 12:26 PM

What is the email's SMTP address? 189.162.189.159

What is the sender address? aaronluo@cmail.carleton.ca

What is the recipient address? mark@letsdefend.io

Is the mail content suspicious? Yes

Are there any attachment? Yes

×

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?

NoYes

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

MaliciousNon-malicious

Analysed and found 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.

Delivered

Not Delivered

Device Action :Blocked

Mail was "Not Delivered" to the user's mailbox it was blocked at the server level.

+

Add Artifacts

Value	Comment	Type	Remove
189.162.189.159	SMTP address	IP Address	
cmail.carleton.ca	Spoofed domain	E-mail Domain	
https://a.pomf.cat/	Malicious URL	URL Address	
69.39.225.3	Malicious IP	IP Address	
72C812CF21909A48EB5	Malicious attachment	MD5 Hash	

Next

Artifacts added based on investigation.

×

Analyst Note

Please enter your analysis comments.

An email containing an attachment was received at Mar, 21, 2021, 12:26 PM. The mail was blocked at exchange level and never made it to user's mailbox. The attachment was analysed and found containing a Trojan (RAT) which was directing data to a malicious website.

The mail domain was spoofed. Both the SMTP address & the mail domain should be blocked at Exchange level and the malicious URL and the malicious IP address

440 / 3000

Next

An email containing an attachment was received at Mar, 21, 2021, 12:26 PM. The mail was blocked at exchange level and never made it to user's mailbox. The attachment was analysed and found containing a Trojan (RAT) which was directing data to a malicious website.

The mail domain was spoofed. Both the SMTP address & the mail domain should be blocked at Exchange level and the malicious URL and the serving IP address added to the firewall.

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

Close Alert

Event ID :

82

☐ True Positive ☐ False Positive

Note:

An email containing an attachment was received at Mar, 21, 2021, 12:26 PM. The mail was blocked at exchange level and never made it to user's

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
Medium	Jan, 07, 2024, 10:13 PM	SOC140 - Phishing Mail Detected - Suspicious Task Scheduler	82	Exchange	✓	↺
EventID :		82				
Event Time :		Mar, 21, 2021, 12:26 PM				
Rule :		SOC140 - Phishing Mail Detected - Suspicious Task Scheduler				
Answer :		True Positive (+5 Point)				
Playbook Answers :		Check If Mail Delivered to User? (+5 Point) Analyze Url/Attachment (+5 Point) Are there attachments or URLs in the email? (+5 Point)				
Analyst Note :		An email containing an attachment was received at Mar, 21, 2021, 12:26 PM. The mail was blocked at exchange level and never made it to user's mailbox. The attachment was analysed and found containing a Trojan (RAT) which was directing data to a malicious website. The mail domain was spoofed. Both the SMTP address & the mail domain should be blocked at Exchange level and the malicious URL and the serving IP address added to the firewall.				

Hopefully this helped.