

SOC114 - Malicious Attachment Detected - Phishing Alert

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Jan, 31, 2021, 03:48 PM	SOC114 - Malicious Attachment Detected - Phishing Alert	45	Exchange	>> ✓
EventID : 45					
Event Time : Jan, 31, 2021, 03:48 PM					
Rule : SOC114 - Malicious Attachment Detected - Phishing Alert					
Level : Security Analyst					
SMTP Address : 49.234.43.39					
Source Address : accounting@mail.carleton.ca					
Destination Address : richard@letsdefend.io					
E-mail Subject : Invoice					
Device Action : Allowed					

Click on >> and create case and click Continue.


Incident Details	
Incident Name:	EventID: 45 - [SOC114 - Malicious Attachment Detected - Phishing Alert]
Description:	EventID: 45
Incident Type:	Exchange
Created Date:	Jan, 11, 2024, 11:01 AM
Start Playbook!	

Let's check the information at hand before we start the playbook.

The rule talks about, “**Malicious Attachment Detected – Phishing Alert**” with type as “**Exchange**” ... so our first hit would be at the mailbox.

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

Invoice <input type="text"/> OR Detailed Search <input type="button" value="v"/>				
Date	Sender	Recipients	Subject	Final Action
Mar, 07, 2021, 04:45 PM	aaronluo@mail.carleton.ca	nicolas@letsdefend.io	Invoice	Unknown
Jan, 31, 2021, 03:48 PM	accounting@mail.carleton.ca	richard@letsdefend.io	Invoice	Unknown
Oct, 29, 2020, 07:43 PM	icianb@hotmail.com	sofia@letsdefend.io	Invoice	Unknown

←	From: accounting@mail.carleton.ca	🗑
	To: richard@letsdefend.io	
	Subject: Invoice	
	Date: Jan, 31, 2021, 03:48 PM	
	Action: Action	
Dear customer, Your invoice for the shopping you have done is attached. Regards.		
Attachments		
 c9ad9506bccfaa987f9fc11b91698d		
Password: infected		

Observing the language of the email gives a sense of generalization, not addressed to someone specific even though the subject is an invoice for a person. The email salutation and body is drafted in the same line ending with **“Regards.”** This lets out a sense of suspicion.

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 SMTP on Talos.

Lookup data results for IP Address

49.234.43.39

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

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

LOCATION DATA

Shanghai, China

OWNER DETAILS

IP ADDRESS	49.234.43.39
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	tencent cloud computing beijing co., ltd.

REPUTATION DETAILS

SENDER IP REPUTATION: Neutral

WEB REPUTATION: Unknown

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	None	

Upon checking the SMTP address is Talos Intelligence, the location of the server shows Shanghai, China belonging to tencent cloud computing. However, the domain Carleton.ca belongs to CA (Canada) which shows that **cmail.carleton.ca** is a spoofed mail domain.

cmail.carleton.ca

0 / 89

Community Score

At least 8 detected files communicating with this domain

cmail.carleton.ca
carleton.ca


education education & reference educational institutions top-1M

Communicating Files (23)

Scanned	Detections	Type	Name
2022-11-18	56 / 70	Win32 EXE	vt-upload-p9QuT
2023-04-01	56 / 69	Win32 EXE	b15142b0dbf1e48d8525004bb3793a63
2022-03-10	56 / 67	Win32 EXE	vt-upload-SEfHc
2022-12-11	59 / 71	Win32 EXE	8f5f4ac3e7a61e552aaed67b959217a
2023-03-23	47 / 63	Win32 EXE	MVhNJQ
2023-11-08	62 / 72	Win32 EXE	VirusShare_08142d441835f1787bf5503cddb7178
2023-09-19	60 / 71	Win32 EXE	iarodig8
2023-06-12	0 / 60	PDF	Ali - Resume PM.pdf
2012-12-27	34 / 44	Win32 EXE	8aaa444c3e67de39a5104779ebbf9ec
2023-08-21	0 / 60	PDF	CV.pdf

This domain has previously been used to transmit executable files which are highly malicious in nature based on the depicted detection rates above.

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

Name	Date modified	Type	Size
 44e65a641fb970031c5efed324676b5018...	1/31/2021 1:55 PM	XLSX File	2,167 KB

To analyse the file, we compare its MD5 Hash signature in Virustotal.

44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx →
C9AD9506BCCCFAA987FF9FC11B91698D

32
/ 59

Community Score

32 security vendors and 2 sandboxes flagged this file as malicious

Reanalyze Similar

44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795

44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx

Size: 2.12 MB | Last Analysis Date: 4 days ago

doc exploit executes-dropped-file cve-2017-11882

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 17 +

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 automa

AhnLab-V3	OLE/Cve-2017-11882.Gen	Arcabit	Trojan.Generic.D417B242
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Trojan.GenericKD.68661826	DrWeb	Exploit.Siggen3.9145
Emsisoft	Trojan.GenericKD.68661826 (B)	eScan	Trojan.GenericKD.68661826
ESET-NOD32	Multiple Detections	Fortinet	MSOffice/CVE_2017_11882.Clexploit
GData	Trojan.GenericKD.68661826	Kaspersky	UDS:DangerousObject.Multi.Generic

Activity Summary

3 Detections

2 MALWARE 1 EXPLOIT 1 SPREADER

Mitre Signatures

NOT FOUND

IDS Rules

1 HIGH 2 LOW

Sigma Rules

NOT FOUND

Behavior Tags

detect-debug-environment executes-dropped-file long-sleeps

Dynamic Analysis Sandbox Detections

The sandbox Dr.Web vxCube flags this file as: MALWARE EXPLOIT SPREADER

The sandbox SecneurX flags this file as: MALWARE

Crowdsourced IDS rules

Matches rule EVENT_GZIP_OVERRUN at Snort registered user ruleset
↳ unknown

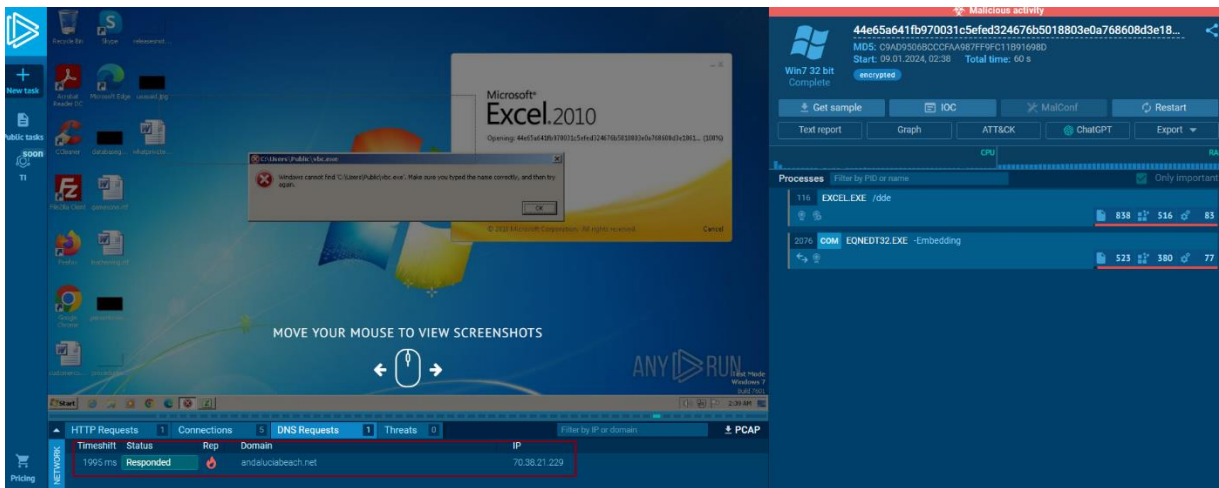
Matches rule SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee) at Abuse.ch Suricata JA3 Fingerprint Ruleset

Matches rule ET POLICY PE EXE or DLL Windows file download HTTP at Proofpoint Emerging Threats Open
↳ Potential Corporate Privacy Violation

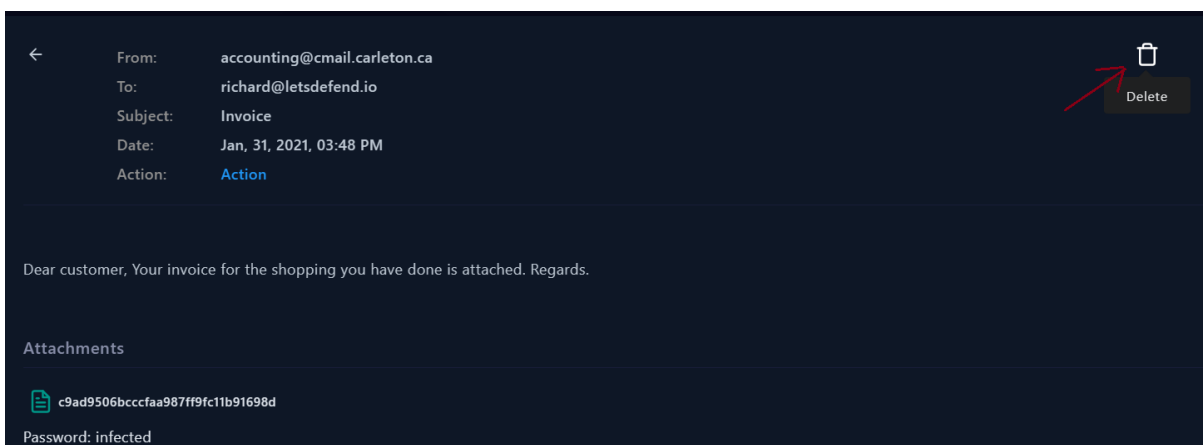
When scanned in app.any.run, the file was found to have DNS linkage with the site: andaluciabeach.net

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2021-01-31 08:08:04	http://andaluciabeach.net/image/network.exe	Offline	exe njRAT opendir rat RemcosRAT	abuse_ch

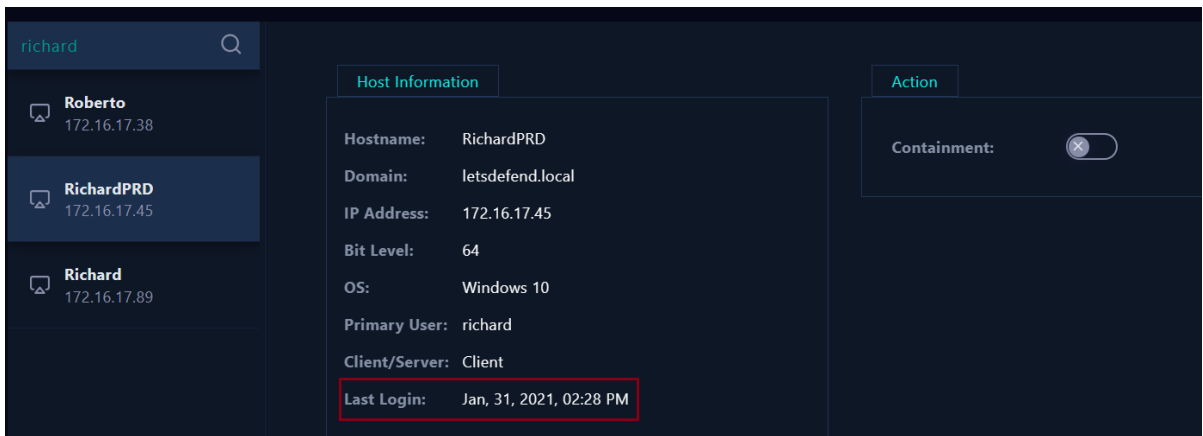
Reputation on URLhaus advises that the site installs a RemcosRAT (Remote Controlled & Surveillance RAT)



It has been determined that the file is highly malicious in nature and that the email should be deleted from the mailbox. The device action is “Allowed” which means the mail was delivered to Richard’s mailbox.



Let’s check if there are instances if the file was executed. Let’s open the Endpoint.



✓	No Event Time	No Process ID	EXCEL.EXE	—	C:/Program Files/Micr...
✓	2021-01-31 12:29	No Process ID	outlook.exe	—	c:/program files [x86]/...
✓	2021-01-31 16:15	No Process ID	EQNEDT32.EXE	—	C:/Program Files/Com...
✓	2021-01-31 16:20	No Process ID	JuicyPotato.EXE	—	C:/User/Public/JuicyP...

We can see that excel & outlook was run post which Richard logged off from the machine as denoted by the Last Login timestamp. The malware has a deferred launch capability and started working at 16:15 based on the endpoint process logs and confirmed with network logs (below)

< Hide Fields

INTERESTING FIELDS

α type

α source_address

source_port

α destination_address

destination_port

α raw_log

Event

type

Proxy

source_address

172.16.17.45

source_port

53948

destination_address

5.135.143.133

destination_port

443

time

Jan, 31, 2021, 04:15 PM

Raw Log

Request URL

http://andaluciabeach.net/image/network.exe

Request Method

GET

Device Action

Allowed

Process

EQNEDT32.EXE

It then downloaded the hacktool JuicyPotato.EXE at 16:20

54

172

54 security vendors and 1 sandbox flagged this file as malicious

Reanalyze

0f56c703e9b7ddeb90646927bac05a5c6d95308c8e13b88e5d4f4b572423e036

Size

339.50 KB

Last Anal

13 days aq

UpdateHelper.exe

peexe

assembly

runtime-modules

detect-debug-environment

idle

spreader

64bits

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 14 +

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

Popular threat label

hacktool/juicypotato/jpotato

Threat categories

hacktool trojan

Family labels

juicypotato jpotato mikey

Security vendors' analysis

Do you w

AhnLab-V3	HackTool/Win.JuicyPotato.R509932	Alibaba	HackTool/Win64.JPotato.a305353e
ALYac	Misc.HackTool.JuicyPotato	Antiy-AVL	Trojan[APT]/Win64.Pioneerkitten
Arcabit	Trojan.Application.Mikey.D21164	Avira (no cloud)	TR/JuicyPotato.twazv
BitDefender	Gen:Variant.Application.Mikey.135524	Bkav Pro	W32.Common.8AC7FF23
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.b6c792
Cylance	Unsafe	Cynet	Malicious (score: 99)

The machine has been compromised and should be immediately contained.

Action

Containment:

Host Contained

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? Jan, 31, 2021, 03:48 PM

What is the email's SMTP address? 49.234.43.39

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

What is the recipient address? richard@letsdefend.io

Is the mail content suspicious? Yes

Are there any attachments? 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?

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

Selecting “Malicious” here based on our observation.

×

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.

Mail was “Delivered” as device action was Allowed.

×

Delete Email From Recipient!

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

Deleted already. Select “Delete”

×

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.

It was clear from the logs that the file was opened. Selecting “**Opened**” here.

×

Containment

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

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

Next

Machine has already been contained. Select Next.

Adding the obtained artifacts

+

Add Artifacts

Value	Comment	Type	Remove
c9ad9506bcccf9a987ff9	Malicious attachment	MD5 Hash	
andaluciabeach.net	Phishing site	URL Address	
5.135.143.133	Phishing IP address	IP Address	
49.234.43.39	SMTP	IP Address	
accounting@cmail.carle	Sender address	E-mail Sender	
cmail.carleton.ca	Sender domain	E-mail Domain	

Next

×

Analyst Note

Please enter your analysis comments.

The email received by Richard had an attachment containing a malicious file. The file was opened which downloaded a possible RAT/Hacktool (JuicyPotato.exe) on the endpoint. The machine has been contained. The SMTP address & the spoofed domain of the sender should be added to the exchange blocklist and the Phishing URL & its DNS should be added to the Firewall. Additionally, Richard should also be trained on cybersecurity Dos and Don'ts to avoid such instances in the future.

478 / 3000

Next

The email received by Richard had an attachment containing a malicious file. The file was opened which downloaded a possible RAT/Hacktool (JuicyPotato.exe) on the endpoint. The machine has been contained. The SMTP address & the spoofed domain of the sender should be added to the exchange blocklist and the Phishing URL & its DNS should be added to the Firewall. Additionally, Richard should also be trained on cybersecurity Dos and Don'ts to avoid such instances in the future.

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

Close Alert

Event ID :

45

☐ True Positive
 ☒ False Positive

Note:

The email received by Richard had an attachment containing a malicious file. The file was opened which downloaded a possible RAT/Hacktool

Close Alert

This would be a True Positive as the email indeed contained a “**Malicious Attachment**”.

Let’s check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 12, 2024, 04:24 AM	SOC114 - Malicious Attachment Detected - Phishing Alert	45	Exchange	✓	↺
EventID :		45				
Event Time :		Jan, 31, 2021, 03:48 PM				
Rule :		SOC114 - Malicious Attachment Detected - Phishing Alert				
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 Url/Attachment (+5 Point) Are there attachments or URLs in the email? (+5 Point)				
Analyst Note :		The email received by Richard had an attachment containing a malicious file. The file was opened which downloaded a possible RAT/Hacktool (JuicyPotato.exe) on the endpoint. The machine has been contained. The SMTP address & the spoofed domain of the sender should be added to the exchange blocklist and the Phishing URL & its DNS should be added to the Firewall. Additionally, Richard should also be trained on cybersecurity Dos and Don'ts to avoid such instances in the future.				
Community Walkthrough :		Show				
Rate this case :		☆				
Writeups :		✍				

Hope this helped.