

SOC114 - Malicious Attachment Detected - Phishing Alert

letsdefend link : <https://app.letsdefend.io/case-management/casedetail/shakeco1/45>

High	Jan, 31, 2021, 03:48 PM	SOC114 - Malicious Attachment Detected - Phishing Alert	45	Exchange
	<p>EventID :</p> <p>45</p> <p>Event Time :</p> <p>Jan, 31, 2021, 03:48 PM</p> <p>Rule :</p> <p>SOC114 - Malicious Attachment Detected - Phishing Alert</p> <p>Level :</p> <p>Security Analyst</p> <p>SMTP Address :</p> <p>49.234.43.39</p> <p>Source Address :</p> <p>accounting@cmail.carleton.ca</p> <p>Destination Address :</p> <p>richard@letsdefend.io</p> <p>E-mail Subject :</p> <p>Invoice</p> <p>Device Action :</p>			

High	Jan, 31, 2021, 03:48 PM	SOC114 - Malicious Attachment Detected - Phishing Alert	45	Exchange
	Allowed			

Show Filter

BasicPro

49.234.43.39

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jan, 31, 2021, 03:48 PM	Exchange	49.234.43.39	48928	172.16.20.3	25	🔍

RAW LOG

×


Sender Mail: accounting@cmail.carleton.ca
Destination Mail: richard@letsdefend.io

sender's ip (49.234.43.39):

49.234.43.39 was found in our database!

This IP was reported **2,399** times. Confidence of Abuse is **0%**: ?

0%

ISP	Tencent cloud computing (Beijing) Co., Ltd.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS45090
Domain Name	tencent.com
Country	 China
City	Shanghai, Shanghai

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.






REPORT 49.234.43.39

WHOIS 49.234.43.39

IP Abuse Reports for 49.234.43.39:

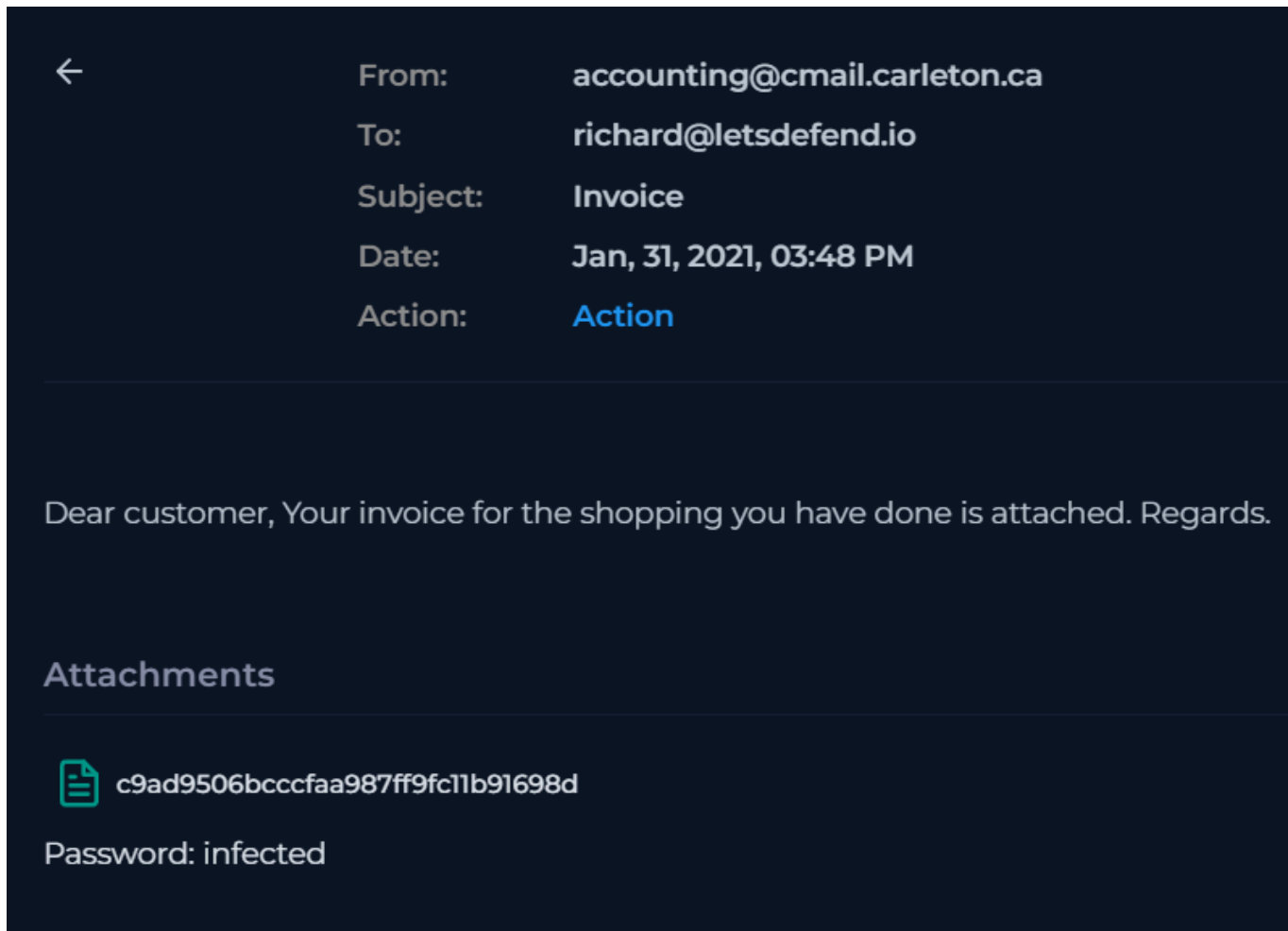
This IP address has been reported a total of **2,399** times from 381 distinct sources. 49.234.43.39 was first reported on November 21st 2020, and the most recent report was **2 years ago**.

Old Reports: The most recent abuse report for this IP address is from **2 years ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC) ?	Comment	Categories
✓ Anonymous	2022-10-04 19:04:44 (2 years ago)	fail2ban detected brute force on sshd	Brute-Force SSH
✓ Anonymous	2022-08-23 14:09:15 (2 years ago)	fail2ban detected bruce force on ssh iptables	Brute-Force SSH
 Seguridad Narnia	2021-10-30 15:06:42 ? (3 years ago)	reported in darklist.de	Hacking
✓  moebius	2021-10-08 02:07:50 ? (3 years ago)	Invalid user hadoop from 49.234.43.39 port 50064	Brute-Force SSH
✓ Anonymous	2021-10-08 00:05:15 (3 years ago)	\$f2bV_matches	Brute-Force SSH
✓  pr0vieh	2021-10-07 22:34:21 (3 years ago)	Oct 8 04:16:47 Linux03 sshd[593560]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu ... show more	Brute-Force SSH
 Adam Dudzik	2021-10-07 22:07:32 (3 years ago)	Oct 8 04:03:01 pihole sshd[22077]: Failed password for root from 49.234.43.39 port 55828 ssh2 ... show more	Brute-Force SSH
✓  Vasili Sviridov	2021-10-07 21:26:37	2021-10-08T03:25:05.234976rus.vasi.li sshd[2656129]:	Brute-Force

it's been reported 2,399 times.

the email :



file hash : c9ad9506bcccf9a987ff9fc11b91698d

file link : <https://download.cyberlearn.academy/download/download?url=https://files-lid.s3.us-east-2.amazonaws.com/c9ad9506bcccf9a987ff9fc11b91698d.zip>

let's check the hash

#1 hybrid-analysis:

HYBRID ANALYSIS

SandboxQuick ScansFile CollectionsResourcesRequest Info

IP, Domain, Hash...

More

Search results for c9ad9506bccffaa987ff9fc11b91698d

Login to Download all DNS Requests [CSV]

Login to Download all Contacted Hosts [CSV]

Copy hashes

Select all

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
May 30th 2025 15:04:09 (UTC)	44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx CDFV2 Encrypted	malicious	AV Detection: 37% CVE-2017-11882 #botdefend #phishing #ransom #exploit #evadom	-	quickscan	
March 20th 2024 20:09:21 (UTC)	44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx CDFV2 Encrypted	malicious	Threat Score: 100/100 AV Detection: 37% CVE-2017-11882 Matched 115 indicators #botdefend #phishing #ransom #exploit #evadom	IN	Windows 11 64 bit	
March 14th 2024 23:37:34 (UTC)	https://files-id.s3.us-east-2.amazonaws.com/c9ad9506bccffaa987ff9fc11b91698d.zip CDFV2 Encrypted	malicious	Threat Score: 100/100 AV Detection: 37% CVE-2017-11882 Matched 108 indicators #botdefend #phishing #ransom #exploit #evadom	-	Windows 7 32 bit (HWP Support)	
November 28th 2023 12:59:24 (UTC)	44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx CDFV2 Encrypted	malicious	Threat Score: 100/100 AV Detection: 37% CVE-2017-11882 Matched 137 indicators #botdefend #phishing #ransom #exploit #evadom	IN	Windows 7 64 bit	
October 19th 2022 14:44:53 (UTC)	44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx CDFV2 Encrypted	malicious	Threat Score: 100/100 AV Detection: 37% CVE-2017-11882 Matched 28 indicators #botdefend #phishing #ransom #exploit #evadom	-	Windows 10 64 bit	
February 17th 2021 18:35:33 (UTC)	44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795.xlsx CDFV2 Encrypted	malicious	Threat Score: 100/100 AV Detection: 37% CVE-2017-11882 Matched 15 indicators #botdefend #phishing #ransom #exploit #evadom	-	Windows 7 32 bit	

Copy hashes

Select all

<

1

>

#2 virustotal:

44e65a641fb970031c5efed324676b5018803e0a768608d3e186152102615795

37 / 62

Community Score

-8

37/62 security vendors flagged this file as malicious

Reanalyze

Similar

More

Size

2.12 MB

Last Analysis Date

3 days ago

PPT

ppt

exploit

executes-dropped-file

cve-2017-11882

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

20

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

downloader

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	OLE/Cve-2017-11882.Gen	AliCloud	Exploit:Win/CVE-2017-11882.C
ALYac	Exploit.CVE-2017-11882	Arcabit	Trojan.Generic.D417B242
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Trojan.GenericKD.68661826	CTX	Ppt.exploit-kit.generic
DrWeb	Exploit.Siggen3.9145	Emsisoft	Trojan.GenericKD.68661826 (B)
eScan	Trojan.GenericKD.68661826	ESET-NOD32	Multiple Detections
Fortinet	Msoffice/CVE_2017_11882.Cexploit	GData	Trojan.GenericKD.68661826
Google	Detected	Huorong	Exploit/CVE-2017-11882.g
Ikarus	Trojan-Downloader.DOC.Agent	Kaspersky	UDS.DangerousObject.Multi.Generic

this tells us it's a trojan.

Contacted Domains (7)

Domain	Detections	Created	Registrar
andaluciabeach.net	6 / 94	2011-08-29	PDR Ltd. d/b/a PublicDomainRegistry.com
centourismeadddynamicoptional001.loseyourip.com	9 / 94	2017-02-02	Dynu Systems Incorporated
controllerfinalineballinglove33.webredirect.org	3 / 94	2016-07-23	Dynu Systems Incorporated
ministeredelasantnj.sytes.net	0 / 94	1999-04-22	Vitalwerks Internet Solutions, LLC / No-IP.com
nexus.officeapps.live.com	0 / 94	1994-12-28	CSC Corporate Domains, Inc.
pastebin.com	1 / 94	2002-09-03	NameCheap, Inc.
www.andaluciabeach.net	1 / 94	2011-08-29	PDR Ltd. d/b/a PublicDomainRegistry.com

Contacted IP addresses (11)

IP	Detections	Autonomous System	Country
104.23.98.190	0 / 94	-	-
104.23.99.190	0 / 94	-	-
194.5.98.8	16 / 94	149020	NO
46.173.211.171	0 / 94	47196	RU
5.135.143.133	0 / 94	16276	FR
5.39.67.131	0 / 94	16276	FR
52.111.229.11	0 / 94	8075	US
52.111.229.50	0 / 94	8075	US
52.111.236.25	0 / 94	8075	IE
52.111.236.26	0 / 94	8075	IE

we have to check if any addresses has been contacted

andaluciabeach.net

centourismeadddynamicoptional001.loseyourip.com

controllerfinalineballinglove33.webredirect.org

ministeredelasantnj.sytes.net

nexus.officeapps.live.com

pastebin.com

104.23.98.190

104.23.99.190

194.5.98.8

46.173.211.171

5.135.143.133

5.39.67.131

52.111.229.11

52.111.229.50

52.111.236.25

52.111.236.26

pastebin has been contacted but it's a very generic site and the dates don't match

Show Filter

BasicPro

pastebin.com

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Oct, 12, 2023, 01:36 PM	DNS	172.16.17.142	0	172.16.17.142	0	🔍
Oct, 12, 2023, 01:36 PM	Proxy	172.16.17.142	25036	104.20.67.143	443	🔍
Jun, 26, 2024, 07:16 AM	DNS	172.16.17.63	32522	104.20.3.235	53	🔍
Jun, 26, 2024, 07:16 AM	Firewall	172.16.17.63	0	104.20.3.235	443	🔍

we found it *andaluciabeach.net* has been contacted

Show Filter

andaluciabeach.net

BasicPro

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jan, 31, 2021, 04:15 PM	Proxy	172.16.17.45	53948	5.135.143.133	443	

RAW LOG

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

Request Method: GET

Device Action: Allowed

Process: EQNEDT32.EXE

Parent Process: excel.exe

Parent Process MD5: 8b88ebbb05a0e56b7dcc708498c02b3e

src address : 172.16.17.45

172.16.17.45

RichardPRD
172.16.17.45

172.16.17.45

RichardPRD
172.16.17.45

Katie
172.16.17.35

Processes6

Network Action20

Terminal History0

Browser History20

Results:10

EVENT TIME

PROCESS ID

PROCESS NAME

PARENT PROCESS

COMMAND LINE

User:richard

Start Time:2021-01-31 16:15

2021-01-31 16:20

No Process ID

JuicyPotato.EXE

—

C:/User/Public/JuicyPotato.e...

MD5:808502752ca0492aca995e9b620d507b

Path:C:/User/Public/JuicyPotato.exe

Size:340 KB

User:NT Authority/System

Start Time:2021-01-31 16:20

<

1

>

0f56c703e9b7ddeb90646927bac05a5c6d95308c8e13b88e5d4f4b572423e036

58

/71

Community Score

-168

58/71 security vendors flagged this file as malicious

Reanalyze Similar More

0f56c703e9b7ddeb90646927bac05a5c6d95308c8e13b88e5d4f4b572423e036

original.exe

Size339.50 KB

Last Analysis Date9 days ago

EXE

peexe64bitsidle

detect-debug-environment

spreader

runtime-modules

assembly

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY20+

Join our 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

pua

Family labels

juicypotato

jpotato

mikey

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	HackTool/Win.JuicyPotato.R509932	Alibaba	HackTool:Win64/JPotato.cbd2dbdd
Alibaba	HackTool:Win/Juicypotato	ALYac	Misc.HackTool.JuicyPotato
Antiy-AVL	Trojan/APTJ/Win64.PioneerKitten	Arcabit	Trojan.Application.Mikey.D21164
Arctic Wolf	Unsafe	Avira (no cloud)	TR/JuicyPotato.twazv
BitDefender	Gen:Variant.Application.Mikey.135524	Bkav Pro	W64.AIDetectMalware
ClamAV	Win.Tool.juicypotato-10041758-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.juicypotato	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Tool.JuicyPotato.4
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Application.Mikey.135524 (B)

Popular threat label: hacktool.juicypotato/jpotato

we have to contain richard's pc

Action

Containment:

✓

Host Contained



Add Artifacts

+

Value	Comment	Type	Remove
email.carleton.ca	Comment	E-mail Dom. ▾	
accounting@cmail.c	Comment	E-mail Send ▾	
49.234.43.39	sender's ip	IP Address ▾	
c9ad9506bcccf9a98	attached file's hash	MD5 Hash ▾	
https://download.cyl	attached url	URL Address ▾	
http://andaluciabea	malicious download	URL Address ▾	
808502752ca0492ac	JuicyPotato	MD5 Hash ▾	

Next



Analyst Note

Please enter your analysis comments.

phishing email delivered , the user downloaded a malware.
the malware then contacted : andaluciabeach
and downloaded Juicy Potato.
I have contained the user's computer.
recommend full endpoint scan and credential reset

222 / 3000

Next