

SOC140 - Phishing Mail Detected - Suspicious Task Scheduler

letsdefend link to case : <https://app.letsdefend.io/case-management/casedetail/shakeco1/82>

EventID :

82

Event Time :

Mar, 21, 2021, 12:26 PM

Rule :

SOC140 - Phishing Mail Detected - Suspicious Task Scheduler

Level :

Security Analyst

SMTP Address :

189.162.189.159

Source Address :

aaronluo@cmail.carleton.ca

Destination Address :

mark@letsdefend.io

E-mail Subject :

COVID19 Vaccine

Device Action :

Blocked

lets examine through logs.

The screenshot shows a security monitoring dashboard with a sidebar on the left containing links to Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a table of logs. A popup window titled 'RAW LOG' is open, showing the following details:

Sender Mail: aaronluo@mail.carleton.ca
Destination Mail: mark@letsdefend.io

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 21, 2021, 12:06 PM	Exchange	189.162.189.159	49371	172.16.20.3	25	

Sender Mail: aaronluo@mail.carleton.ca

The screenshot shows a security monitoring dashboard with a sidebar on the left containing links to Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a table of logs. A search filter 'aaronluo@mail.carle' is applied. The table shows three log entries:

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 21, 2021, 12:06 PM	Exchange	189.162.189.159	49371	172.16.20.3	25	
Mar, 07, 2021, 04:45 PM	Exchange	221.181.185.237	46245	172.16.20.3	25	
Oct, 29, 2020, 05:54 PM	Exchange	157.230.109.166	46938	172.16.20.3	25	

Destination Mail: mark@letsdefend.io

Destination Mail: nicolas@letsdefend.io

destination address: 172.16.20.3

let's check the attacker's ip

#1: 189.162.189.159

#2: 221.181.185.237

#3: 157.230.109.166

Check an IP Address, Domain Name, or Subnet
e.g. 93.173.64.21, microsoft.com, or 5.188.10.0/24


189.162.189.159

CHECK

189.162.189.159 was found in our database!

This IP was reported 206 times. Confidence of Abuse is 0%: ?

0%

ISP	Gestión de direccionamiento UniNet
Usage Type	Fixed Line ISP
ASN	AS8151
Hostname(s)	dsl-189-162-189-159-dyn.prod-infinity.com.mx
Domain Name	uninet.net.mx
Country	 Mexico
City	Leon de los Aldama, Guanajuato

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

REPORT 189.162.189.159

WHOIS 189.162.189.159

IP Abuse Reports for 189.162.189.159:

This IP address has been reported a total of 206 times from 110 distinct sources. 189.162.189.159 was first reported on March 19th 2021, 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	2023-07-04 10:09:57 (2 years ago)	\$f2bV_matches	Brute-Force SSH
✓ Anonymous	2023-07-01 17:09:48 (2 years ago)	\$f2bV_matches	Brute-Force SSH
✓ Anonymous	2023-03-06 23:00:59 (2 years ago)	\$f2bV_matches	Brute-Force SSH
✓ Anonymous	2023-03-03 17:52:46 (2 years ago)	\$f2bV_matches	Brute-Force SSH
✓ Anonymous	2023-01-15 21:10:34 (2 years ago)	\$f2bV_matches	Brute-Force SSH
✓ Anonymous	2022-12-07 15:38:00 (2 years ago)	\$f2bV_matches	Brute-Force SSH

AbuseIPDB » 221.181.185.237

Check an IP Address, Domain Name, or Subnet
e.g. 93.173.64.21, microsoft.com, or 5.188.10.0/24


221.181.185.237

CHECK

221.181.185.237 was found in our database!

This IP was reported **16,374** times. Confidence of Abuse is **0%** ?

0%

ISP China Mobile Communications Corporation
Usage Type Fixed Line ISP
ASN AS56046
Domain Name chinamobile.com
Country  China
City Nanjing, Jiangsu

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


REPORT 221.181.185.237

WHOIS 221.181.185.237

IP Abuse Reports for 221.181.185.237:

This IP address has been reported a total of **16,374** times from 332 distinct sources. 221.181.185.237 was first reported on February 25th 2021, and the most recent report was **3 years ago**.

Old Reports: The most recent abuse report for this IP address is from **3 years ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC) ?	Comment	Categories
✓  Eric	2021-10-22 09:46:38 (3 years ago)	Blocked by jail recidive	Brute-Force
✓  Parth Maniar	2021-04-08 03:35:10 (4 years ago)	SSH login attempts (SSH bruteforce attack). If you need more data for the IP address, give me a shou ... show more	Brute-Force SSH
✓  Parth Maniar	2021-04-06 14:14:33 (4 years ago)	SSH login attempts (SSH bruteforce attack). If you need more data for the IP address, give me a shou ... show more	Brute-Force SSH
 Miroslav Stampar	2021-03-26 04:00:00 ? (4 years ago)		Brute-Force SSH

AbuseIPDB » 157.230.109.166

Check an IP Address, Domain Name, or Subnet
e.g. 93.173.64.21, microsoft.com, or 5.188.10.0/24

157.230.109.166

CHECK

157.230.109.166 was found in our database!

This IP was reported **9,483** times. Confidence of Abuse is **0%**:

0%

ISP

DigitalOcean, LLC

Usage Type

Data Center/Web Hosting/Transit

ASN

AS14061


Hostname(s)

862613.cloudwaysapps.com

Domain Name

digitalocean.com

Country

 Germany

City

Frankfurt am Main, Hesse

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







REPORT 157.230.109.166

WHOIS 157.230.109.166

IP Abuse Reports for 157.230.109.166:

This IP address has been reported a total of **9,483** times from 749 distinct sources. 157.230.109.166 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.

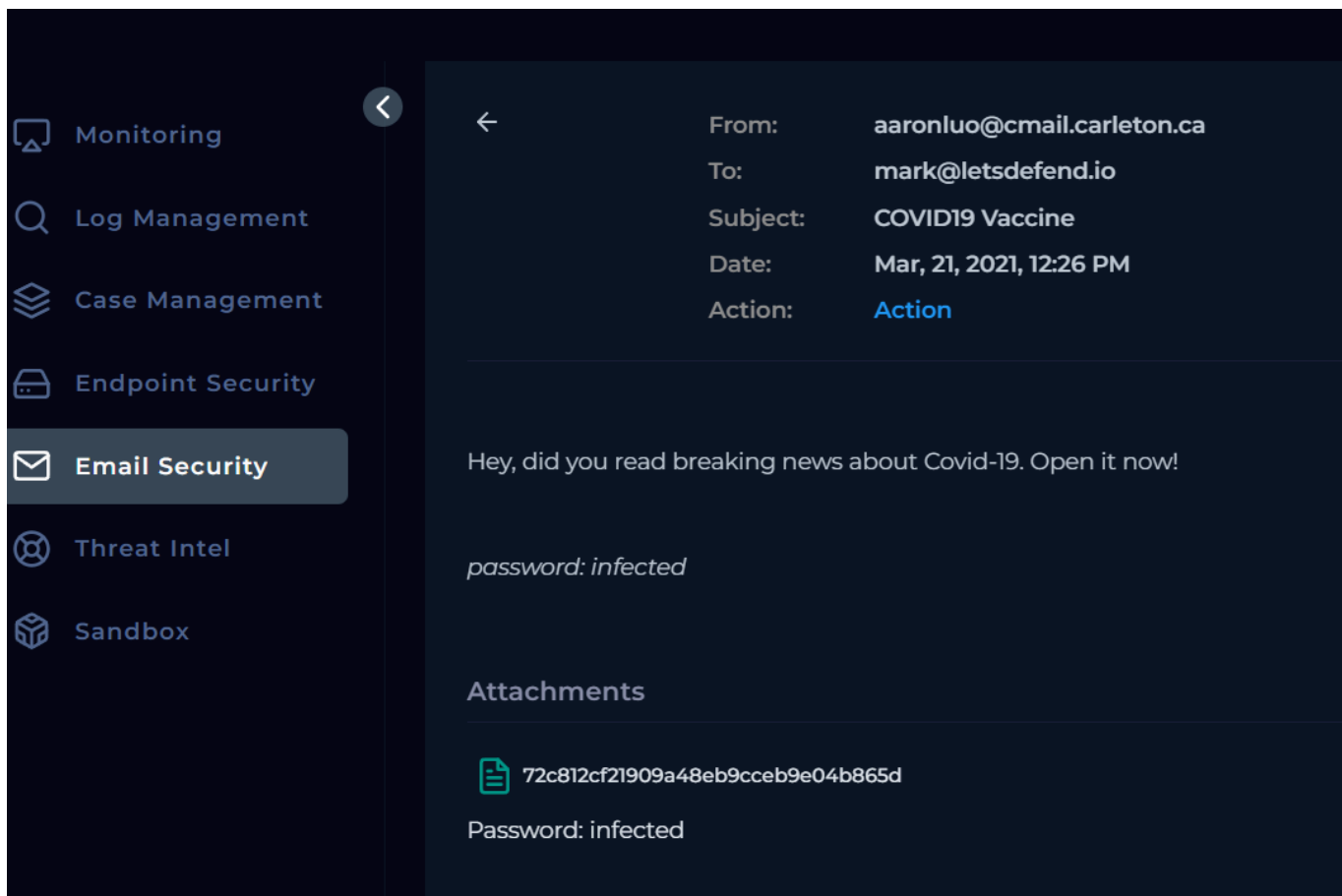
Reporter	IoA Timestamp (UTC)	Comment	Categories
 antihack.anarchista.xyz	2022-10-21 18:04:11 (2 years ago)	Jul 29 16:05:05 evulka sshd[860]: Failed password for root from 157.230.109.166 port 40296 ssh2<br / ... show more	<div>Brute-Force</div> <div>Web App Attack</div> <div>SSH</div>
 	2022-10-04 18:56:49 (2 years ago)		<div>Brute-Force</div> <div>SSH</div>
 	2022-09-14 18:47:40 (2 years ago)		<div>Brute-Force</div> <div>SSH</div>
 antihack.anarchista.xyz	2022-07-11 10:57:43	Jul 29 16:05:05 evulka sshd[860]: Failed password for r	<div>Brute-Force</div>

we can see that all of his ip addresses are reported.

aaronluo@cmail.carlet <input type="text"/> OR <input type="button" value="Detailed Search"/>				
Date	Sender	Recipients	Subject	Final Action
Mar, 21, 2021, 12:26 PM	aaronluo@cmail.carleton.ca	mark@letsdefend.io	COVID19 Vaccine	Unknown
Mar, 07, 2021, 04:45 PM	aaronluo@cmail.carleton.ca	nicolas@letsdefend.io	Invoice	Unknown
Oct, 29, 2020, 06:40 PM	aaronluo@cmail.carleton.ca	mark@letsdefend.io	UPS Your Packages Status Has Changed	Allowed

we can see that he sent an email to 2 users in our company so we shall check them one by one.

lets begin with mark's first email:



file name : [72c812cf21909a48eb9cceb9e04b865d](https://download.cyberlearn.academy/download/download?url=https://files-ls3.us-east-2.amazonaws.com/72c812cf21909a48eb9cceb9e04b865d)

file address : <https://download.cyberlearn.academy/download/download?url=https://files-ls3.us-east-2.amazonaws.com/72c812cf21909a48eb9cceb9e04b865d>

Analyze URL Address

- [AnyRun](#) (buisness)
- [VirusTotal](#)
- [URLScan](#)
- [HybridAnalysis](#)
- [AbuseIPDB](#)

46 / 62

Community Score

-2

46/62 security vendors flagged this file as malicious

Reanalyze Similar More

0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92

Size 194.00 KB Last Analysis Date 11 days ago DOC

0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92.docx

doc calls-wmi runtime-modules hide-app macros long-sleeps auto-open detect-debug-environment create-ole checks-network-adapters direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 12+

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

Code insights

The VBA code defines multiple functions and a subroutine within modules named "Q1gh90bcm64K", "B8p6neu6jrdwr", and "Uf8rk_6463bcnzh1".

1. Module "Uf8rk_6463bcnzh1": This module contains a subroutine named "Document_open()" that is automatically executed upon opening the document. This subroutine calls the function "llenbqiklpik" within the "B8p6neu6jrdwr" module.

Show more

Crowdsourced AI

Hispacec flags this file as benign

The macros extracted from the document exhibit behavior typical of benign functionality. The macros define several functions that involve error handling, variable assignments, and string manipulation operations. These functions seem to be part of a larger system for processing data or performing specific tasks within the document. There are no clear indicators of malicious intent such as obfuscation, suspicious function

Show more

Popular threat label downloader.emotet.w97m

Threat categories downloader trojan

Family labels emotet w97m emodldr

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Downloader/DOC.Emotet.S1297	AliCloud	Trojan(downloader).MSOffice/Emotet.P...
ALYac	Trojan.Downloader.DOC.Gen	Antiy-AVL	Trojan[Downloader]/MSOffice.Agent

2 / 97

Community Score

+

2/97 security vendors flagged this URL as malicious

Reanalyze Search More

https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.co... download.cyberlearn.academy

Status 200 Content type text/html; charset=utf-8 Last Analy... 21 days ago

text/html external-resources

DETECTION

DETAILS

COMMUNITY

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?

alphaMountain.ai	Malicious	Fortinet	Malware
------------------	-----------	----------	---------

hybrid-analysis:

Search results for 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92

Multi-Process Extracted Files Sample not shared Network Traffic TOR analysis Decrypted SSL traffic

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
August 1st 2024 06:42:15 (UTC)	https://files-ld.s3.us-east-2.amazonaws.com/5a3de19f198269947bb509152678b7d2.zip Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co... 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 25 Indicators #macro-cs-open	-	Windows 11 64 bit	
December 6th 2022 05:07:43 (UTC)	0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co... 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 11 Indicators #macro-cs-open	-	Windows 10 64 bit	
June 20th 2022 16:33:11 (UTC)	file Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co... 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92	malicious	AV Detection: 81% Trojan.Generic #macro-cs-open	-	quickscan	
June 29th 2021 21:01:22 (UTC)	0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co... 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 93/100 AV Detection: 81% Trojan.Generic Matched 15 Indicators #macro-cs-open	-	Windows 7 64 bit	
December 1st 2020 05:13:55 (UTC)	0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co... 0c55dae4a75373696f7af6d0a7db5092fbe4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 15 Indicators #macro-cs-open	-	Windows 7 32 bit	

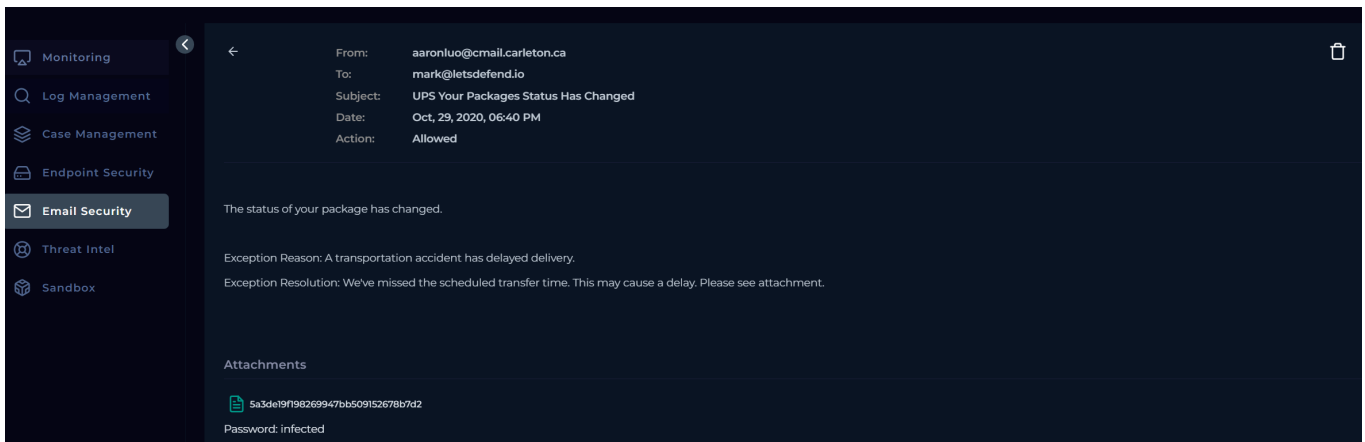
Copy hashes

Select all

1

both virustotal & hybrid-analysis flag it as a maleware.

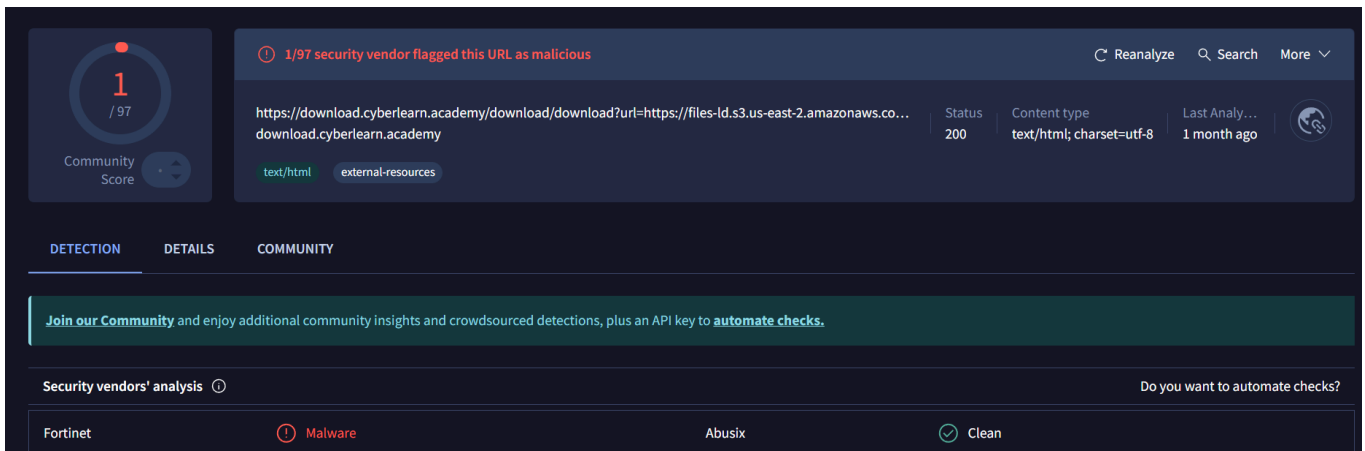
now the 2nd mail that mark recived :



file name : [5a3de19f198269947bb509152678b7d2](https://files-ls3.us-east-2.amazonaws.com/5a3de19f198269947bb509152678b7d2)

file address: <https://download.cyberlearn.academy/download/download?url=https://files-ls3.us-east-2.amazonaws.com/5a3de19f198269947bb509152678b7d2.zip>

VirusTotal:



0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92

46

/ 62

Community Score

-2

46/62 security vendors flagged this file as malicious

ReanalyzeSimilarMore

0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92

Size194.00 KB

Last Analysis Date11 days ago

DOC

doc

calls-wmi

runtime-modules

hide-app

macros

long-sleeps

auto-open

detect-debug-environment

create-ole

checks-network-adapters

direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY12+

Join our Community

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

Code insights

The VBA code defines multiple functions and a subroutine within modules named "Q1gh90bcm64k", "B8p6neu6jrdwr", and "Uf8rk_64630bcnz1".

1. Module "Uf8rk_64630bcnz1": This module contains a subroutine named "Document_open()" that is automatically executed upon opening the document. This subroutine calls the function "lilenbqikpik" within the "B8p6neu6jrdwr" module.

Show more

Crowdsourced AI

Hispasser flags this file as benign

The macros extracted from the document exhibit behavior typical of benign functionality. The macros define several functions that involve error handling, variable assignments, and string manipulation operations. These functions seem to be part of a larger system for processing data or performing specific tasks within the document. There are no clear indicators of malicious intent such as obfuscation, suspicious function

Show more

Popular threat label

download.emotet.w97m

Threat categories

downloader

trojan

Family labels

emotet

w97m

emodldr

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

Downloader/DOC.Emotet.S1297

AliCloud

Trojan[downloader].MSOffice/Emotet.P...

ALYac

Trojan.Downloader.DOC.Gen

Antiy-AVL

Trojan[Downloader]/MSOffice.Agent

hybrid-analysis:

Search results for 5a3de19f198269947bb509152678b7d2

Login to Download all DNS Requests [CSV]

Login to Download all Contacted Hosts [CSV]

Multi-Process

Extracted Files

Sample not shared

Network Traffic

TOR analysis

Decrypted SSL traffic

Copy hashes

Select all

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
August 1st 2024 06:42:15 (UTC)	https://file-id.s3.us-east-2.amazonaws.com/5a3de19f198269947bb509152678b7d2.zip Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ... 0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 25 Indicators #macros-on-open	-	Windows 11 64 bit	<input type="checkbox"/>
December 6th 2022 05:07:43 (UTC)	0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ... 0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 11 Indicators #macros-on-open	-	Windows 10 64 bit	<input type="checkbox"/>
June 20th 2022 16:33:11 (UTC)	file Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ... 0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92	malicious	AV Detection: 81% Trojan.Generic #macros-on-open	-	quickscan	<input type="checkbox"/>
June 29th 2021 21:01:22 (UTC)	0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ... 0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 93/100 AV Detection: 81% Trojan.Generic Matched 15 Indicators #macros-on-open	-	Windows 7 64 bit	<input type="checkbox"/>
December 1st 2020 05:13:55 (UTC)	0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92.docx Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ... 0c55dae4a753736967af6d0a7db5092f8e4f15c3c92d8dc9433949837b5db92	malicious	Threat Score: 100/100 AV Detection: 81% Trojan.Generic Matched 15 Indicators #macros-on-open	-	Windows 7 32 bit	<input type="checkbox"/>

Copy hashes

Select all

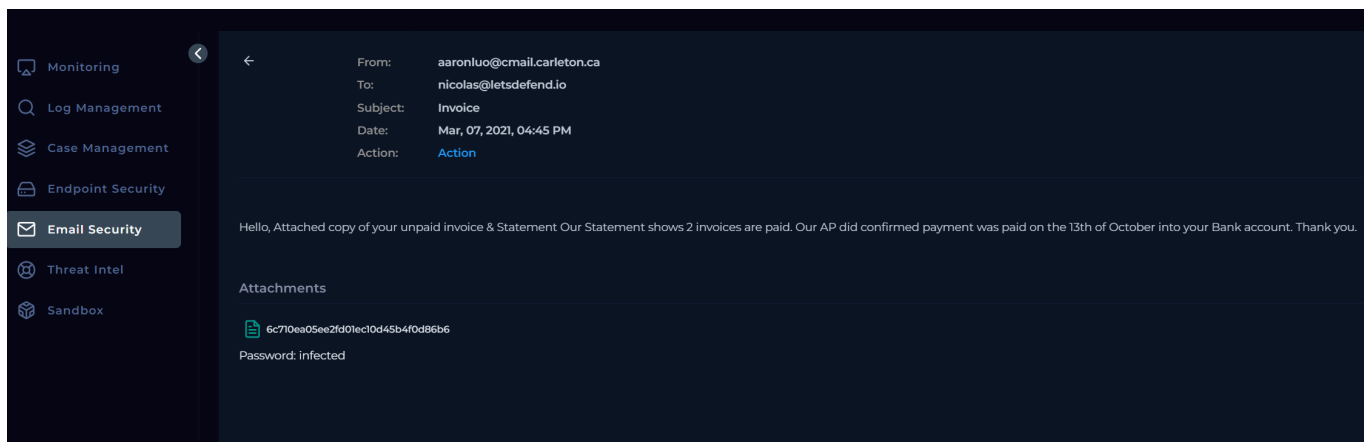
<

1

>

both virustotal & hybrid-analysis flag it as a maleware.

now lets move on to nicolas:



file name : [6c710ea05ee2fd01ec10d45b4f0d86b6](https://download.cyberlearn.academy/download/download?url=https://files-id.s3.us-east-2.amazonaws.com/6c710ea05ee2fd01ec10d45b4f0d86b6.zip)

file address : <https://download.cyberlearn.academy/download/download?url=https://files-id.s3.us-east-2.amazonaws.com/6c710ea05ee2fd01ec10d45b4f0d86b6.zip>

Search results for **6c710ea05ee2fd01ec10d45b4f0d86b6**

Login to Download all DNS Requests [CSV] | Login to Download all Contacted Hosts [CSV]

Multi-Process | Extracted Files | Sample not shared | Network Traffic | TDR analysis | Decrypted SSL traffic | Copy hashes | Select all

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
November 16th 2022 03:40:16 (UTC)	ALLEGATO_FT_del_20-06-2019.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C... 8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb	malicious	Threat Score: 100/100 AV Detection: 75% VBA.Heur2.EmotetDldr Matched 9 Indicators #macros-on-open	-	Windows 10 64 bit	<input type="checkbox"/>
July 21st 2022 05:34:45 (UTC)	ALLEGATO_FT_del_20-06-2019.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C... 8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb	malicious	Threat Score: 100/100 AV Detection: 75% VBA.Heur2.EmotetDldr Matched 23 Indicators #malware-on-open	-	Windows 7 64 bit	<input type="checkbox"/>
June 8th 2021 06:40:14 (UTC)	file Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C... 8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb	malicious	AV Detection: 75% VBA.Heur2.EmotetDldr #macros-on-open	-	quickscan	<input type="checkbox"/>
June 20th 2019 09:03:15 (UTC)	ALLEGATO FT del 20-06-2019.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C... 8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb	ambiguous	Threat Score: 35/100 AV Detection: 75% VBA.Heur2.EmotetDldr Matched 12 Indicators #macros-on-open	-	Windows 7 32 bit	<input type="checkbox"/>

Copy hashes | Select all

1

8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb

43 / 64
Community Score -48

43/64 security vendors flagged this file as malicious

Reanalyze Similar More

8b84bbf5fee07dd41cfaecbc527da1fed3bcf4adab2541a00f55422093f216fb
ALLEGATO_FT_del_20-06-2019.xls
Size 96.00 KB Last Analysis Date 7 hours ago XLS

xls run-file auto-open macros calls-wmi attachment macro-run-file obfuscated

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

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

Code insights
The VBA code presents several highly suspicious functionalities when examined for potentially malicious behavior.
* Code Obfuscation: The code heavily employs obfuscation techniques such as meaningless variable names (e.g., 'tebor', 'pls', 'muji', 'DmE') and string manipulation, making it difficult to understand the code's true purpose.
[Show more](#)

Crowdsourced AI

Hispasec flags this file as malicious
The macros extracted from the document exhibit several signs of malicious intent.
[Show more](#)

Popular threat label trojan.x97m/emotetdldr Threat categories trojan downloader Family Labels x97m emotetdldr heur2

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AliCloud	Trojan(downloader);MSOffice/Donoff.Gen
ALYac	Trojan.Downloader.XLS.gen	Antiy-AVL	Trojan(Downloader);MSOffice.Agent

now lets check the destination address: 172.16.20.3

and we see that it's the Exchange Server.

The screenshot shows a security dashboard with a sidebar on the left containing a search bar and a list of endpoints: DockerBox (172.16.20.36), Chandler (172.16.20.33), PentestMachine (172.16.20.5), Aldo (172.16.17.51), and Exchange Server (172.16.20.3). The main panel displays 'Endpoint Information' for the selected IP. It includes a 'Host Information' tab with details like Hostname (Exchange Server), Domain (LetsDefend), IP Address (172.16.20.3), Bit Level (64), OS (Windows Server 2012), Primary User (Administrator), Client/Server (Server), and Last Login (Oct. 10, 2020, 10:08 PM). There is also an 'Action' tab with a 'Containment' toggle. Below this, a navigation bar shows 'Processes' (6), 'Network Action' (1), 'Terminal History' (4), and 'Browser History' (1). The 'Terminal History' section is active, showing a table with columns: EVENT TIME, PROCESS ID, PROCESS NAME, PARENT PROCESS, and COMMAND LINE. The table contains two rows, both with 'No Event Time' and 'No Process ID'.

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	Chrome.exe	—	c:/program files (x86)/googl...
No Event Time	No Process ID	hh.exe	—	C:/Windows/hh.exe

אני רואה בטרמינל שהפקודות נעשו עוד לפני קבלת המייל.

This screenshot shows the 'Terminal History' section of the dashboard. The navigation bar at the top shows 'Processes' (6), 'Network Action' (1), 'Terminal History' (4), and 'Browser History' (1). The 'Terminal History' section is active, displaying a table with columns: EVENT TIME and COMMAND LINE. The table lists four commands executed on 2020-10-10 at 10:29:04, 10:29:03, 10:29:02, and 10:29:01. The third row, showing 'net user', is highlighted. At the bottom, there is a pagination control showing '< 1 >'.

EVENT TIME	COMMAND LINE
2020-10-10 10:29:04	net localgroup backupGroup backupUser /add
2020-10-10 10:29:03	net user backupUser
2020-10-10 10:29:02	net user
2020-10-10 10:29:01	cls

נראה שהעמדה לא הודבקה.

Analyst Note:

Phishing mail blocked – subject “COVID19 Vaccine” sent from aaronluo@cmail.carleton.ca to two users (**mark**, **nicolas**) with .zip files flagged as malware (VT & Hybrid Analysis). Attacker IPs: 189.162.189.159 , 221.181.185.237 , 157.230.109.166 . No infection found.

Close Alert Note:

True Positive – Phishing email with subject “COVID19 Vaccine” sent to two users. Contained malicious .zip files flagged by VT & Hybrid Analysis. Source IPs confirmed malicious in OSINT. Email blocked. No execution or compromise detected.