CIS Center for Internet Security®

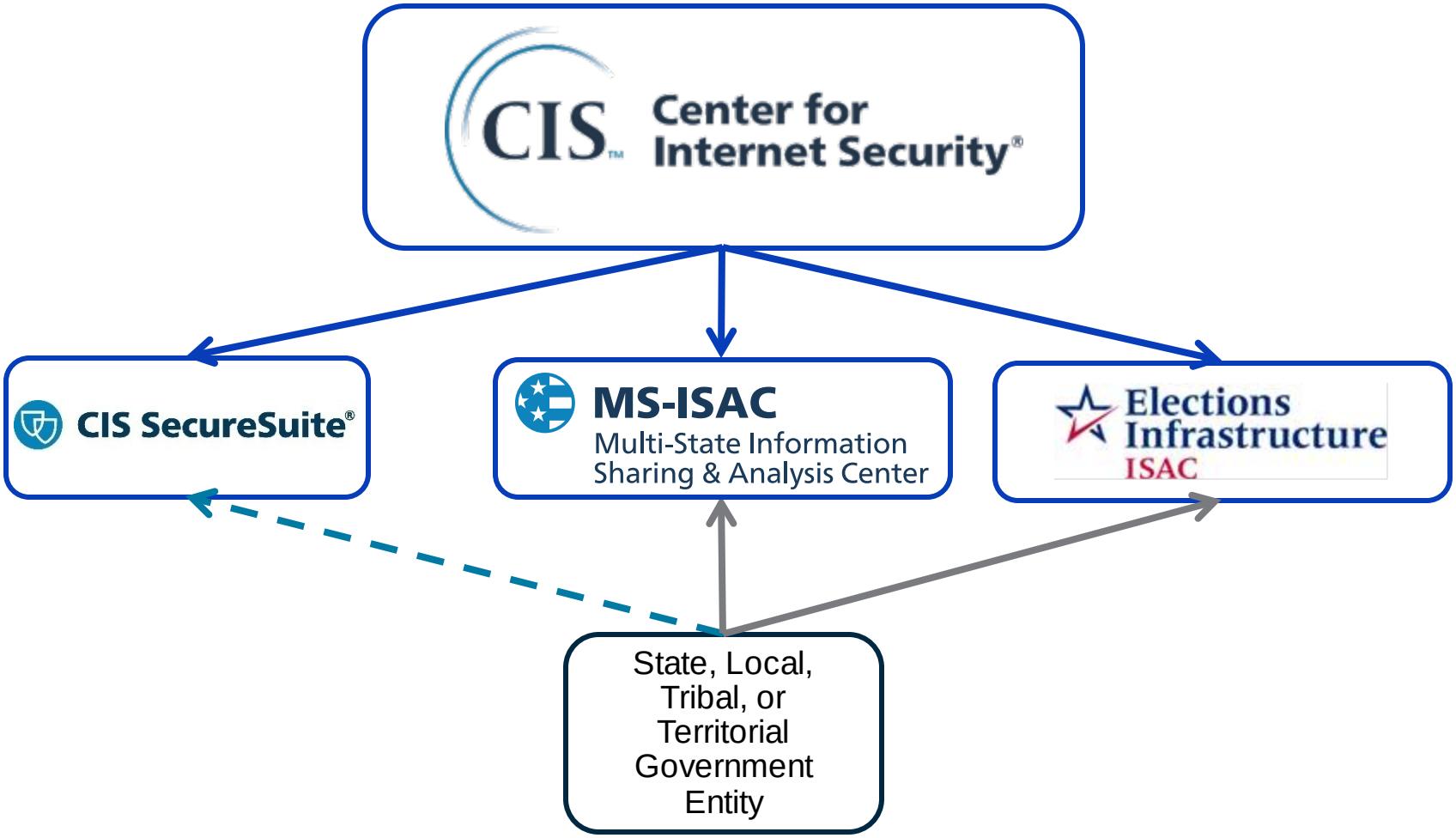
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC

SLTT Government Cyber Threat Landscape

Eugene Kipniss and Matt Grieco

December 19, 2018


CIS
Center for Internet Security®
CIS SecureSuite®
MS-ISAC
Multi-State Information Sharing & Analysis Center
Elections Infrastructure ISAC
State, Local, Tribal, or Territorial Government Entity

Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

TLP: WHITE

Intelligence Sources

- 24x7 monitoring
- Analysis of more than 1.5 trillion logs/month
- Integration with federal agencies via the NCCIC
- Trusted private companies
- Constant contact with all ISACs



Information Sharing and Analysis Centers

MS-ISAC® Multi-State Information Sharing & Analysis Center®
Elections Infrastructure ISAC
NCC
SC ISAC
AVIATION ISAC
FINANCIAL SERVICES ISAC
EMR-ISAC
PT-ISAC Public Transportation Information Sharing & Analysis Center
Real Estate ISAC Information Sharing and Analysis Center Serving the Commercial Facilities Sector
AUTO-ISAC Automotive Information Sharing and Analysis Center
REN-ISAC
R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER
NH-ISAC NATIONAL HEALTH - ISAC
HEALTHCARE READY STRENGTHEN. SAFEGUARD. RESPOND.
MARITIME ISAC MARITIME INFORMATION SHARING & ANALYSIS CENTER
WaterISAC
National Defense ISAC™
DIB
ICS-ISAC
IT ISAC
ONG-ISAC
DNG-ISAC
E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Why Governments?

Criminals look for data...
and governments have a lot of it!













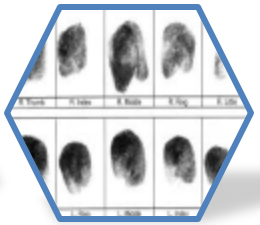








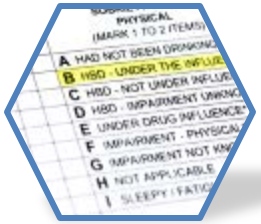












MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC

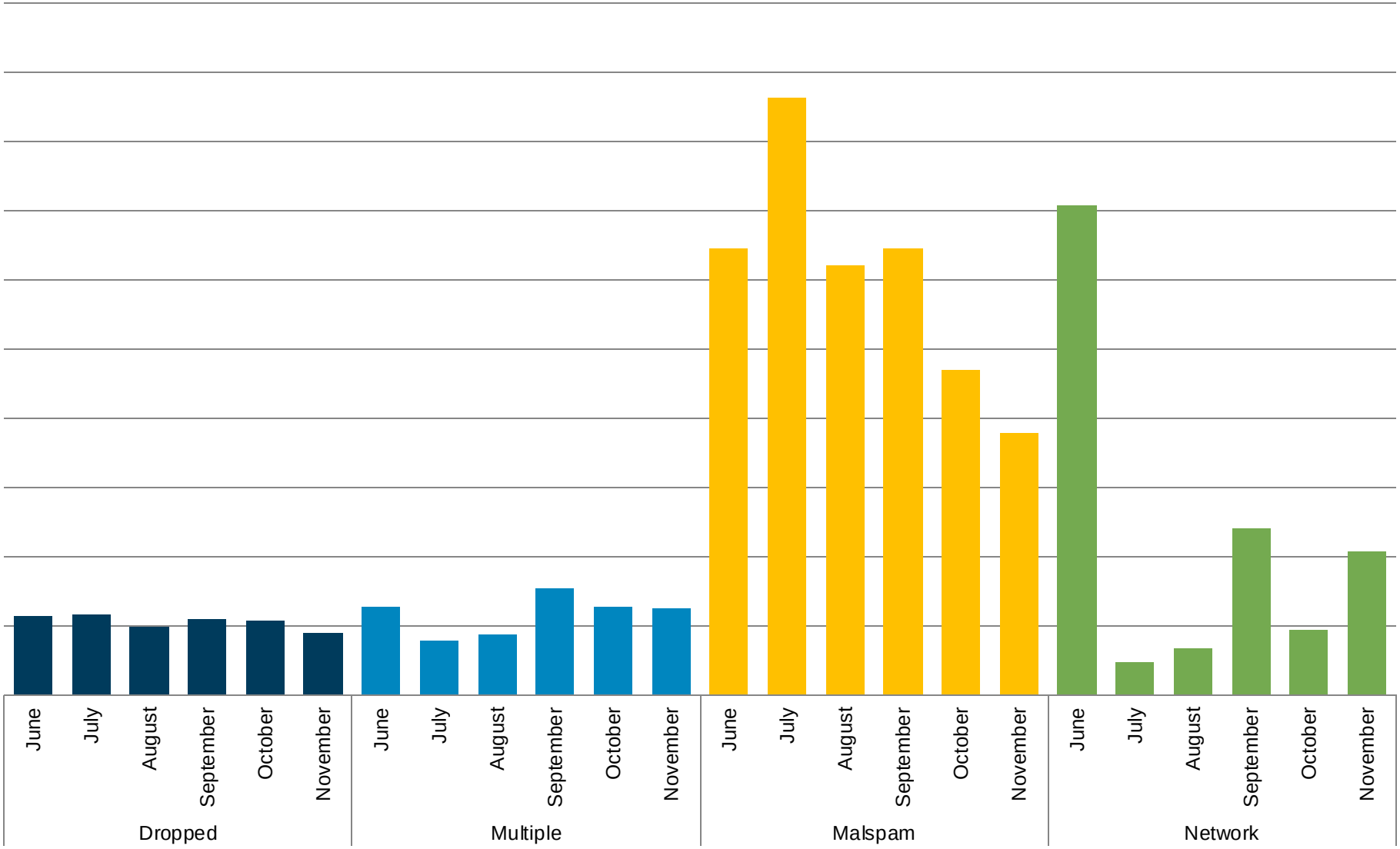
Malware and Technical Threats



Top 10 Malware

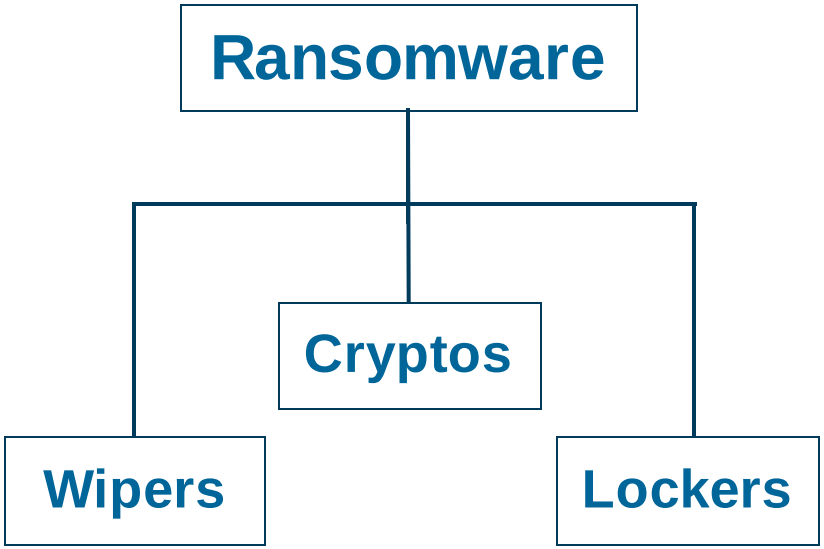
	October 2018	November 2018	
1.	Emotet (Infostealer)	WannaCry (Ransomware)	
2.	Kovter (Click Fraud)	Emotet (Infostealer)	
3.	ZeuS (Banking Trojan)	ZeuS (Banking Trojan)	
4.	WannaCry (Ransomware)	Kovter (Click Fraud)	
5.	NanoCore (RAT)	CoinMiner (Cryptocurrency Miner)	
6.	Gh0st (RAT)	Mirai (Botnet)	
7.	CoinMiner (Cryptocurrency Miner)	NanoCore (RAT)	
8.	Mirai (Botnet)	Gh0st (RAT)	
9.	Ursnif (Banking Trojan)	SmokeLoader (Banking Trojan)	
10.	SmokeLoader (Banking Trojan)	Ursnif (Banking Trojan)	

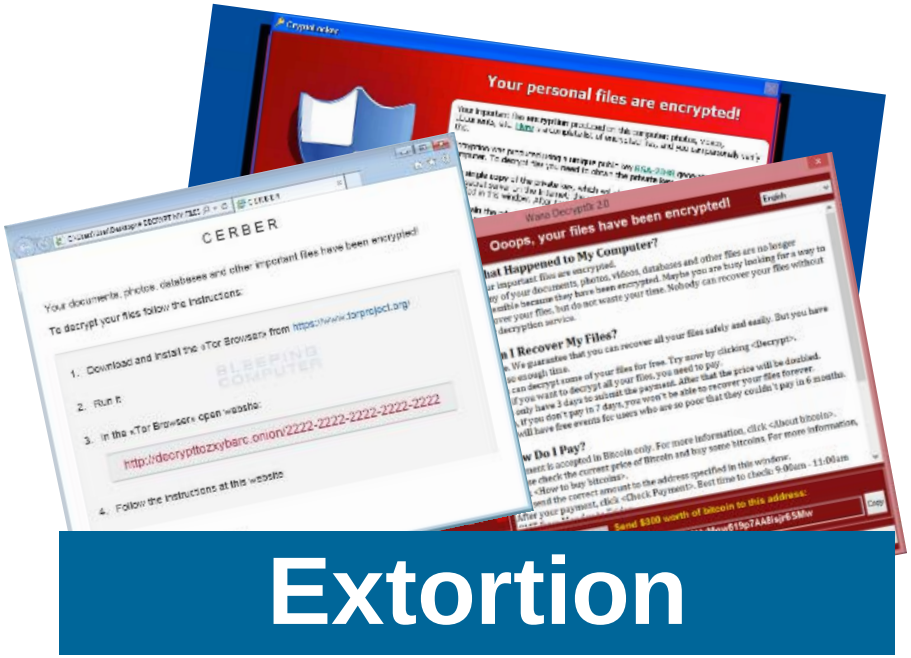
Top 10 Malware - Initiation Vectors



Ransomware

Malware that blocks access to a system, device, or file until a ransom is paid; commonly demand that the victim pays $200 - $1,000 in bitcoins, gift cards, etc.





1. Cryptos – ransomware that encrypts files
2. Wipers – ransomware that erases files; no recovery
3. Lockers – ransomware that blocks access to files or the system

EternalBlue

- Ransomware, trojans, and cryptocurrency miners utilize EternalBlue exploit for its spreading capabilities

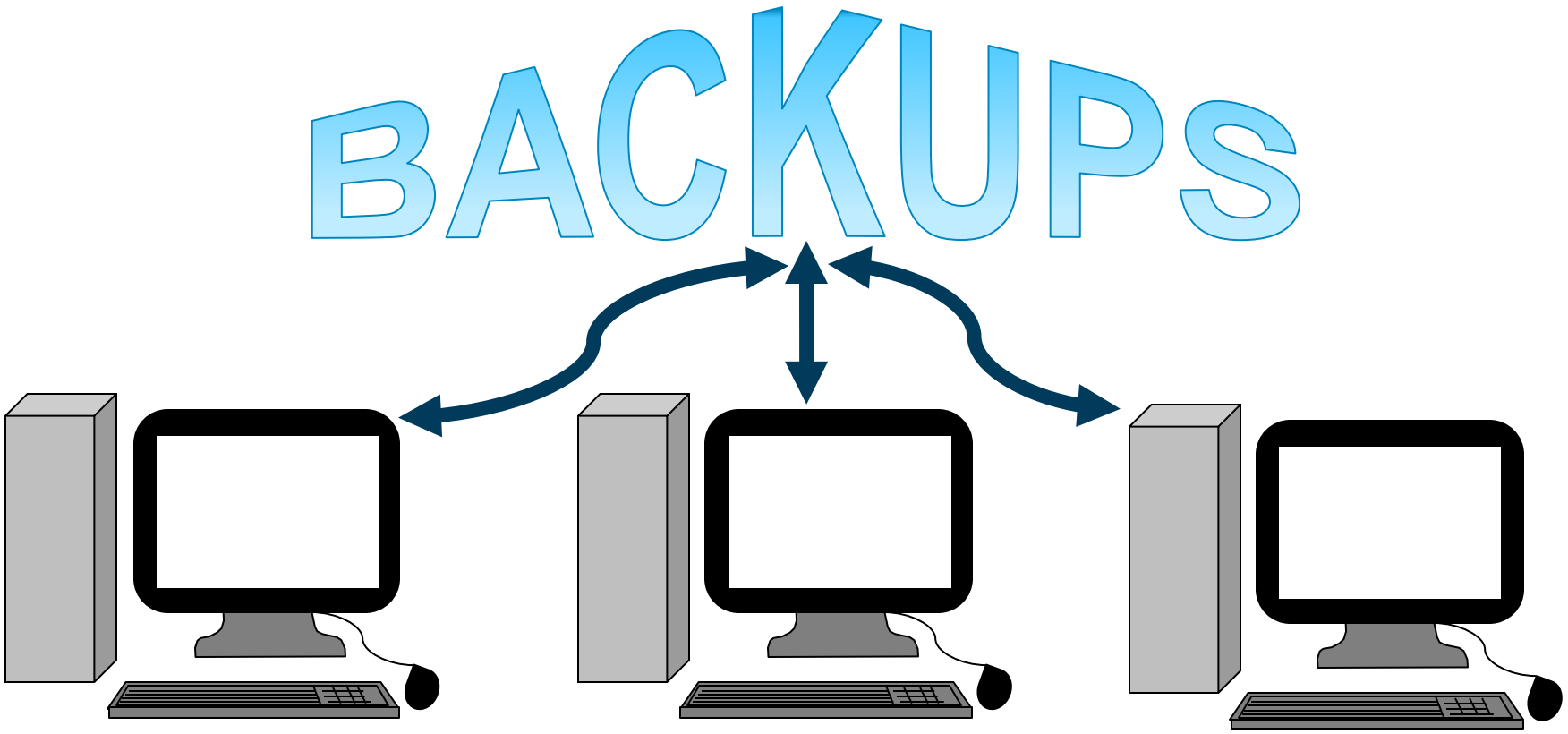


ETERNALBLUE

- MS17-010 (March 2017) Microsoft patch

Don’t Be Next! - Backups

- Frequent
- Complete
- Off-line
- Off-site
- Tested



Don’t Be Next

- Have a backup and test it!
- Have an incident response plan and test it!
- Make sure executives, PIOs, and General Counsel know and understand what ransomware is
- Implement software restriction policies & whitelisting
- Audit for unauthorized access attempts, brute forcing, and the use of common pen-testing tools
- Disable SMBv1 on all systems
- Patch the CVE-2017-0147 vulnerability (MS17-010)
- Assess the need to have RDP (port 3389) open
- Verify cloud installations do not re-enable RDP

Cryptocurrency Miners

Malware:

- Coinhive
- CoinMiner
- WannaMine
- Dark Test
- BrowseAloud

Infection Vectors:

- Malspam
- Eternal Blue
- Exploit Kits
- Worms
- Tech Support Scam
- Plugins

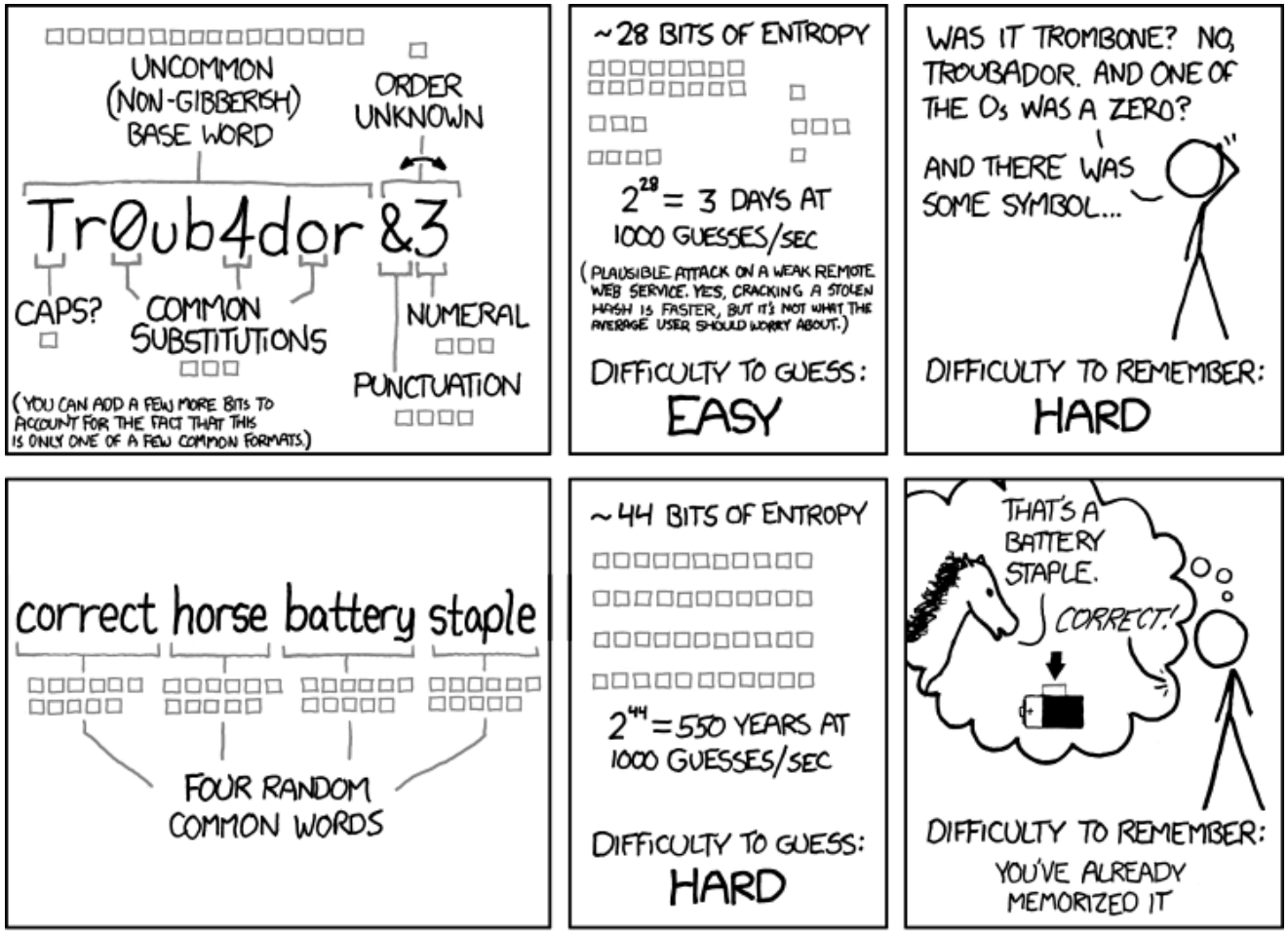
ORACLE WEBLOGIC SERVER

ORACLE PEOPLESOFT

Struts

- Masquerading as Windows/system files, Fake AV
- Fileless malware
- Windows, Mac, smartphones, SmartTVs, SCADA
- Water utilities, Hospitals

Don't Be Next! - Password Standards



https://xkcd.com/936/

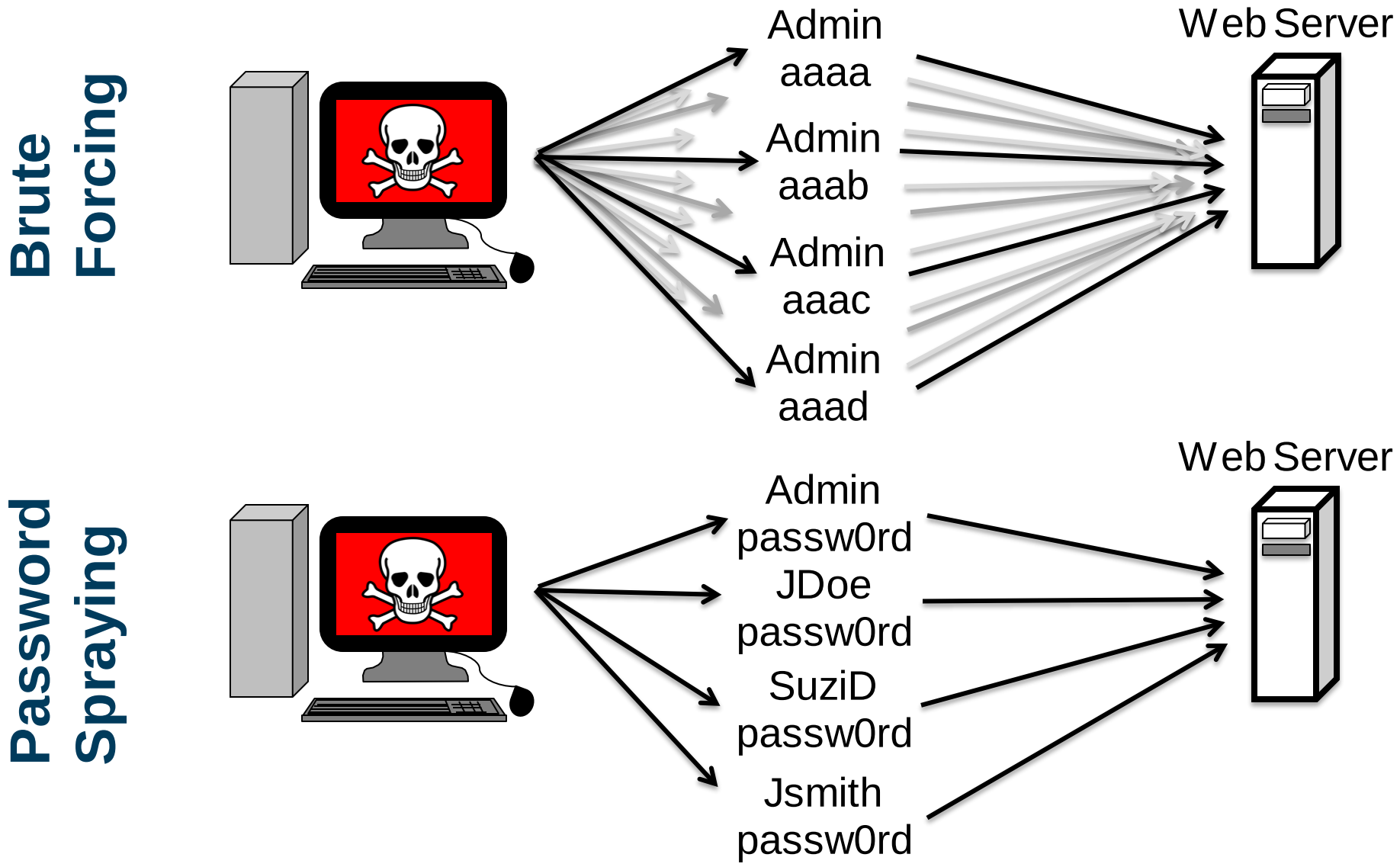
Technique 1:

- 14+ characters
- Uppercase, lowercase, numbers, symbols
- Changed every 60 days
- Unique

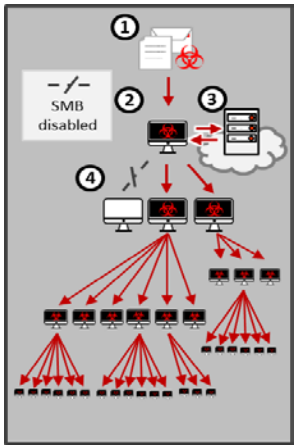
Technique 2:

- 8-64 characters
- All characters
- Hashed, salted
- Screen against dictionaries
- Changed when compromised
- Unique

Office 365 Brute Forcing



Emotet



1 Infection

Invoice or shipment themed spam email with malicious attachments or links

Users open document with malicious macros

Malicious macros download Emotet malware

2 Establish Persistence

Emotet creates registry auto start keys and injects itself into running processes

3 Instructions Phase

Emotet reports a new infection to its C2 server and receives instructions

4 Network Propagation

Outlook Scraper

WebBrowserPassView

NetPass.exe

Mail PassView

SMB

Credential Enumerator

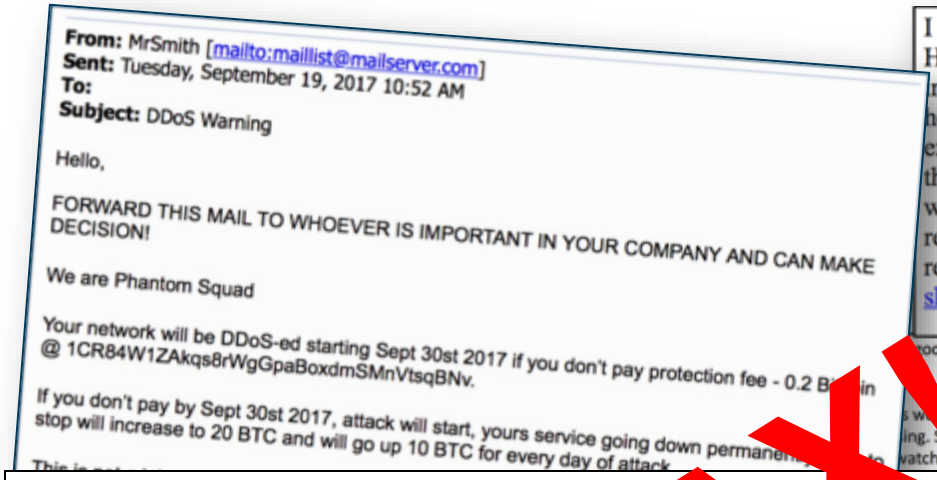
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC

Social Engineering



Hoax Extortion Schemes



From: MrSmith [mailto:maillist@mailserver.com]
Sent: Tuesday, September 19, 2017 10:52 AM
To:
Subject: DDoS Warning

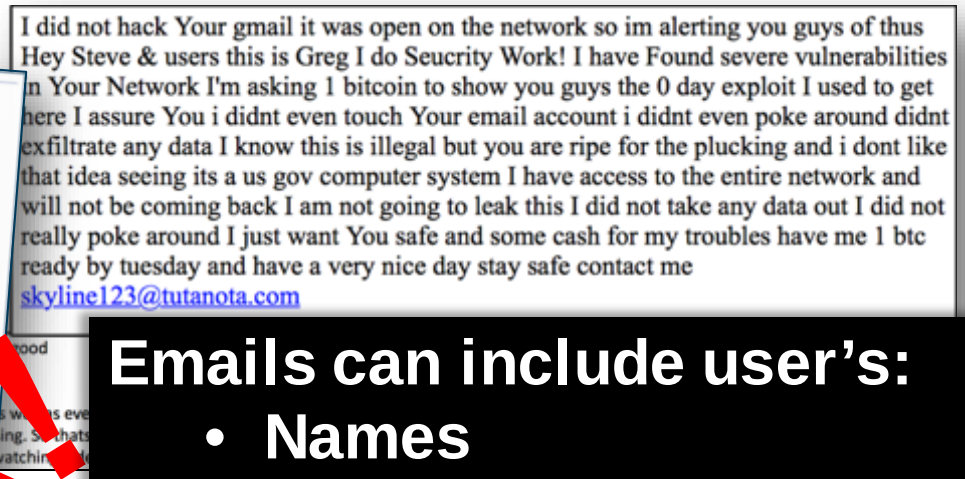
Hello,

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 B in @ 1CR84W1ZAkqs8rWgGpaBoxdmSMnVtsqBNv.

If you don't pay by Sept 30st 2017, attack will start, yours service going down permanen stop will increase to 20 BTC and will go up 10 BTC for every day of attack



I did not hack Your gmail it was open on the network so im alerting you guys of thus Hey Steve & users this is Greg I do Seucrity Work! I have Found severe vulnerabilities n Your Network I'm asking 1 bitcoin to show you guys the 0 day exploit I used to get here I assure You i didnt even touch Your email account i didnt even poke around didnt exfiltrate any data I know this is illegal but you are ripe for the plucking and i dont like that idea seeing its a us gov computer system I have access to the entire network and will not be coming back I am not going to leak this I did not take any data out I did not really poke around I just want You safe and some cash for my troubles have me 1 btc ready by tuesday and have a very nice day stay safe contact me skyline123@tutanota.com

HOAX!

Emails can include user's:

- **Names**
- **Passwords**
- **Emails**
- **Telephone numbers**

Spoofing the victim's email

SAMPLE EMAIL TEXT

Subject: <username> - <password>

I'm aware, <password>, is your pass word ou do t kn y me and you are most

In fact, I actually placed a malware on e a lt vide (porno) web site and guess While you were watching vide lips r bro nitiated operating as a RDP (Re your display and web cam. Imm ely a r that, my software gathered all of your

What exactly did I do?

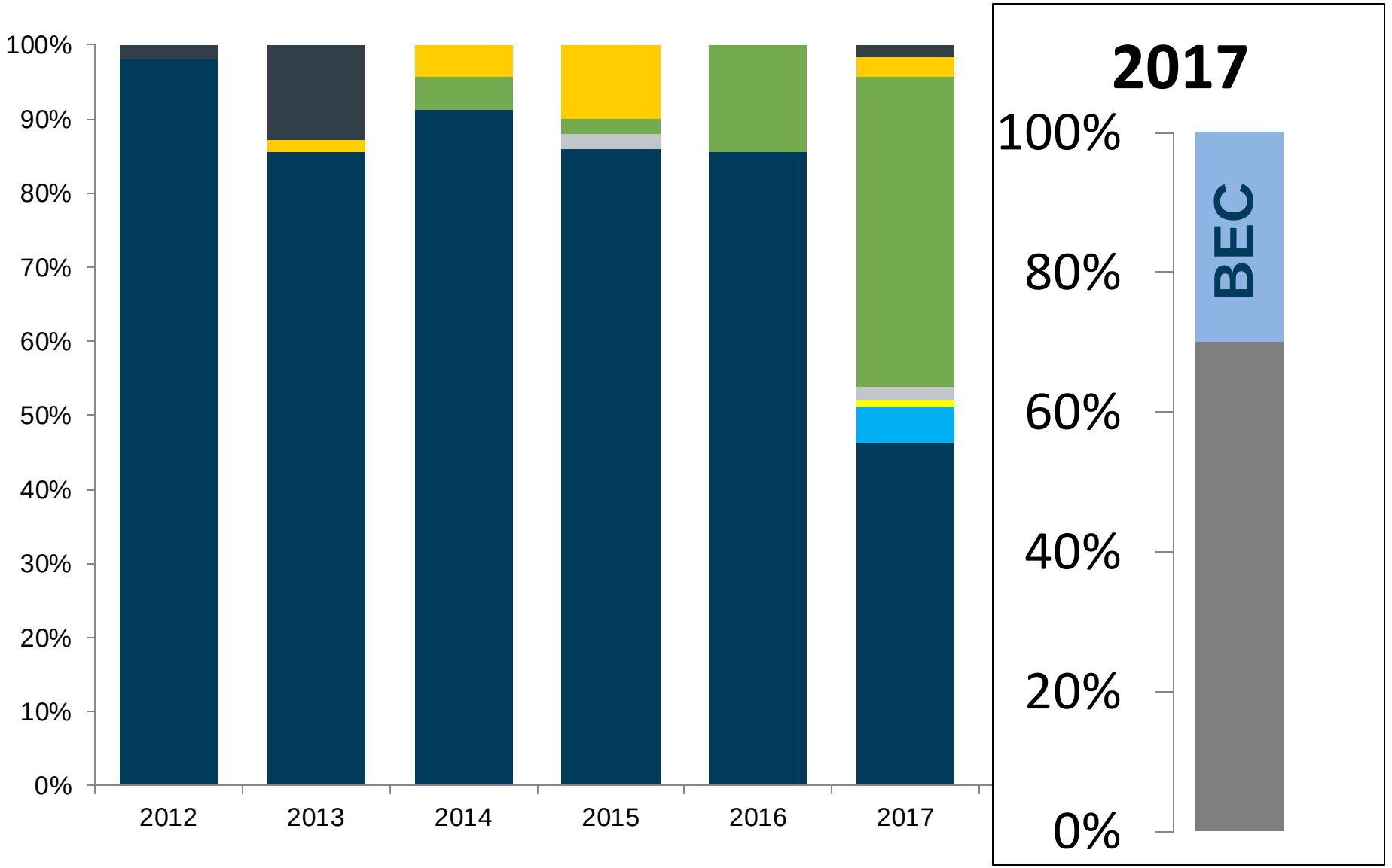
I made a double-screen video. 1st part displays the video you were viewing (you've

What should you do?

Well, I believe, <extortion amount> is a reasonable price tag for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: <address>
(It is cAsE sensitive, so copy and paste it)

SLTT Data Breaches by Vector





Southern Oregon University loses $1.9 million in email scheme

BY THE ASSOC

JUNE 8, 2017

City of El Paso duped out of $3.3 million in phishing

CEO fired after 'fake CEO' email scam cost firm $47m

Liam Tung (CSO Online) on 26 May,

Officials: Galveston County Falls Victim To $525K Scam

Toy Maker Mattel Loses $3M in BEC Scam, Then Fights for It and Gets It Back

by Julie Seymour | March 31, 2016 | News

BEC: CEO Compromise Example

Date:
FROM: CEO ← *From an Executive*
TO: Finance Department ← *To Finance*
SUBJECT: Question

Are you available? Wire transfer needs to go out.Also what is the balance of General Funding Account? Let me know when you are ready.

Formatting error

Don't call. Im in a meeting.

Sense of urgency

Sent from my iPhone ← *Social Engineering*

BEC: W-2 Phishing Example

Date:
FROM: CEO — *From an Executive (spoofed)*
TO: HR Department — *To a member of HR*
SUBJECT: Urgent Request

HR employee, — *By name*

Have you got a minute? I need a soft copy of employees 2016, W-2's Wage and Tax Statement, I need this in my email ASAP in a PDF file type, you can send it as an attachment.

Thank you,

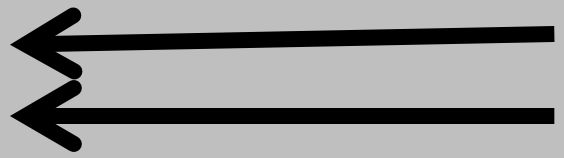
Subtle grammar errors

Executive

Company signature line — *Seemingly correct signature line*

BEC: Direct Deposit Example

Date:
FROM: Executive
TO: HR
SUBJECT: Direct Deposit



Spoofed as if from an Executive

To HR employee

Hi <HR employee's first name>,

I changed my bank and will need to update my paycheck DD details, can the change be effective for the current pay date?

Regards,

<Executive's first name>

BEC: Direct Deposit Scam

HR or Finance is contacted by scammers posing as the CEO requesting urgent direct deposit change

From: Terry Burton [mailto:admin@oitfri.com]
Sent: Monday, November 19, 2018 8:26 AM
To: [redacted]
Subject: Direct Deposit Update!

Hi [redacted]

I changed my bank and will need to update my paycheck DD details, can the change be effective for the current pay date?

Regards,

Terry

Don’t Be Next

- **Have a BEC Incident Response Plan**
  - Establish a policy for reporting BEC and similar phishing emails
  - Know who is involved in the IR
- **Educate**
  - Finance, HR, Legal, Public Relations departments
- **Collaborate**
  - Finance and HR departments to ensure their policies are supported by technological solutions (e.g. encryption)
  - FBI/USSS and ISACs
- **Develop the Culture**
  - OK to ask



© Scott Adams, Inc./Dist. by UFS, Inc.

Don’t Be Next

- Least Privilege
- Add warning banners for emails from external sources
- Implement filters at your email gateway
- Data Loss Prevention tools to stop exfiltration
- Two-factor authentication
  - Technical
  - Physical
- TTX

~72 hours to stop a wire transfer

Report

Report scams and attempts:

IC3/FBI: https://bec.ic3.gov/

MS-ISAC: soc@msisac.org

Tax-related to IRS

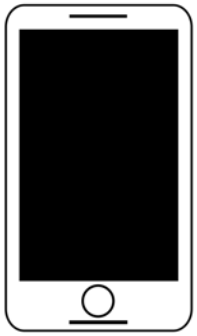
Don’t Be Next - 2FA/MFA

2 Factor Authentication / Multi-Factor Authentication



Something you know
e.g. password





Something you have
e.g. smartphone



Something you are
e.g. biometrics

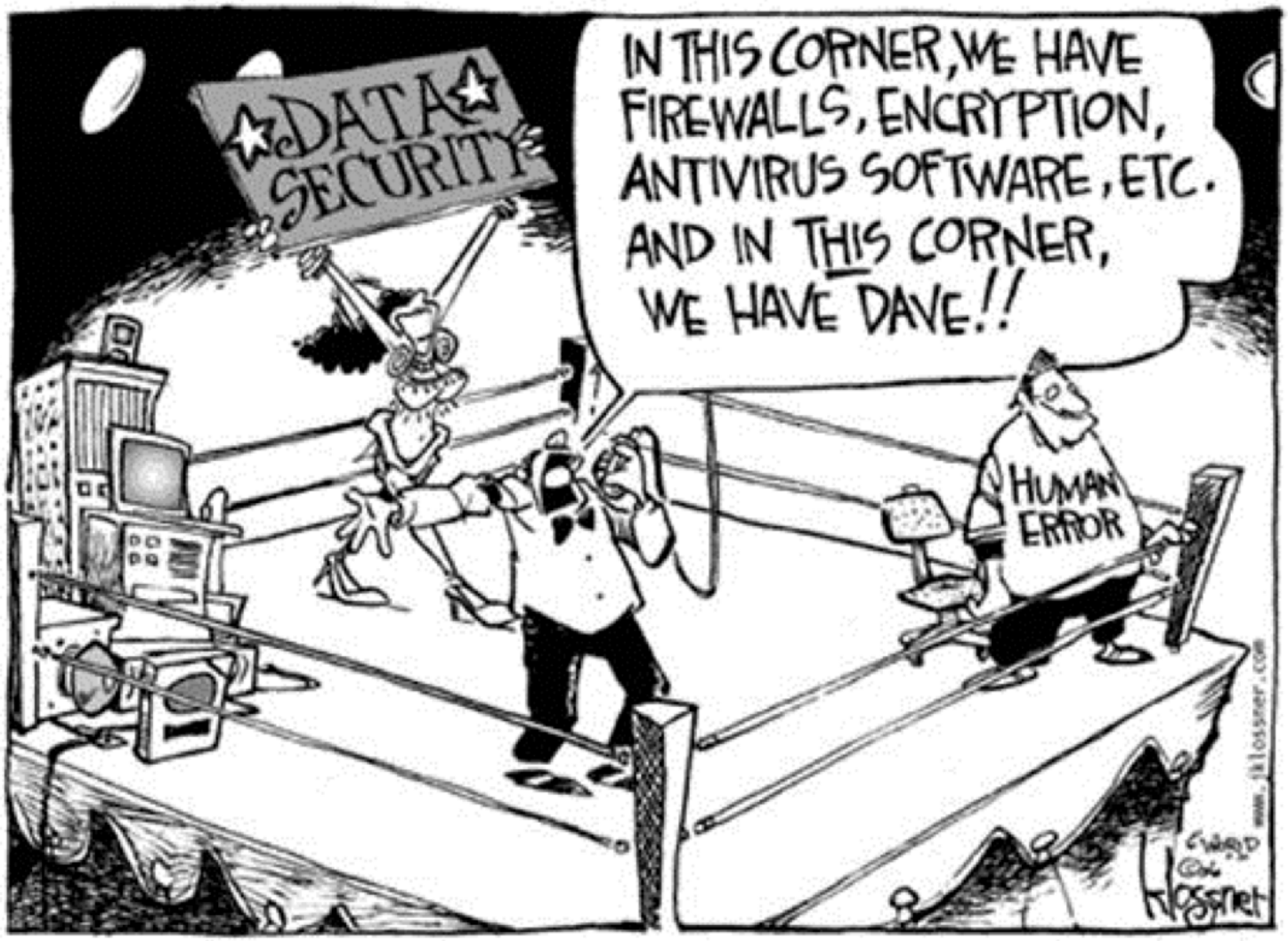


Someplace you are
e.g. GPS location

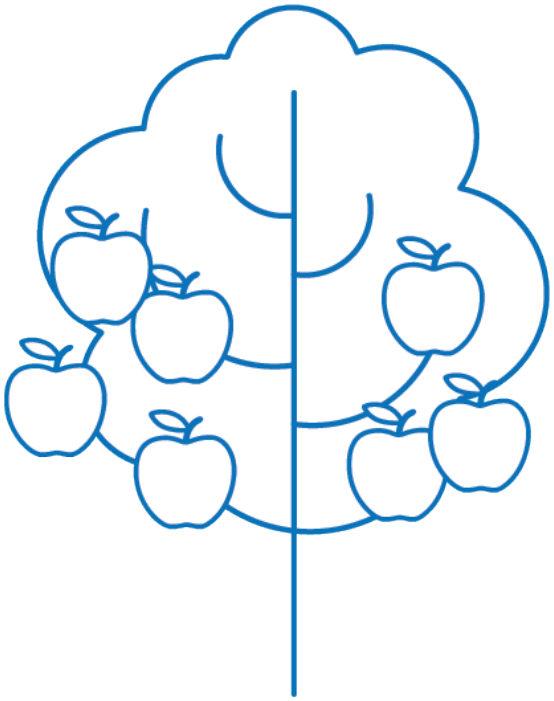
Financial Fraud Kill Chain (FFKC)

- **Minimum $50,000**
- **International Transfer**
- **<72 Hours Since Wire Transfer Initiated**
- **FBI, USSS, FINCEN, NCFTA, FS-ISAC**

Don’t Be Next - Train Users



What Can You Do?



1. PATCH!
2. Use defensive software
3. Train users
4. Enforce passwords standards & 2FA
5. Share intelligence
6. Create a culture where it's OK to ask
7. Work with the MS-ISAC

Who do I call?

To join or get more information:

https://learn.cisecurity.org/ms-isac-registration



Security Operations Center (SOC)

SOC@msisac.org - 1-866-787-4722

31 Tech Valley Dr., East Greenbush, NY 12061-4134

www.cisecurity.org

Eugene Kipniss
Sr. Program Specialist
Eugene.Kipniss@cisecurity.org

Matt Grieco
Intelligence Analyst
Matthew.grieco@cisecurity.org

TLP: WHITE