

**USSS Cyber Assets and Capabilities**

**National Motor Freight Traffic Association**

**10/23/2023**

**Mike Alvarez**

**Network Intrusion Forensics Analyst**

**Houston Cyber Fraud Task Force**

**Houston Field Office**



## Cyber Fraud Task Forces

- Prevent, detect, and mitigate complex cyber-enabled financial crimes
- Partner with private industry, SLTT and federal law enforcement agencies, federal and state prosecutors, and academia



- Effectively leverage collective expertise to combat cybercrime
- Arrest the most harmful perpetrators



# Houston Cyber Fraud Task Force



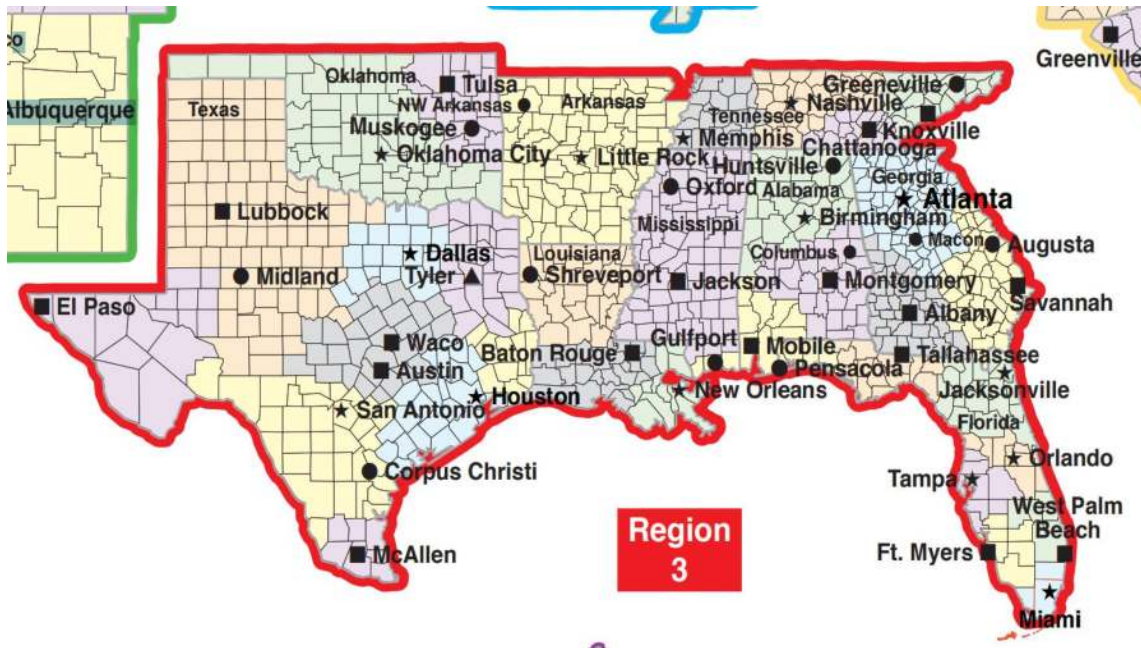


# Jurisdictional Map

Houston Field Office – Covers 39 Counties

Austin Resident Office – Covers 17 Counties

Mexico City Resident Office – Covers all of Mexico



# Cyber Disciplines

## Digital Forensics (DF)

- Dead box forensics
- Computers, cellphones, Internet-of-Things (IOT) devices, vehicle systems, drones, skimming devices
- Identify, preserve, extract and analyze evidence

## Network Intrusion Responder (NITRO)

- Live box response and forensics
- Computer systems, storage servers, Payment Card Industry (PCI) systems
- Identify system compromise
- Preserve, extract and analyze evidence



## Global Investigative Operations Center

- Hub for high impact and multi-jurisdictional investigations
- Common operational picture for investigations that target and dismantle large-scale domestic and international criminal organizations
- Oversight for complex and coordinated field operations
- Oversight and support for undercover operations
- Specialized support through mission desks



# Cyber Intelligence Section

- An investigative and intelligence operations unit focused on transnational cyber activity with significant financial or operational impact to critical infrastructure (private and public sectors)
- CIS personnel collaborate with domestic and foreign law enforcement agencies to address pervasive and evolving cyber threats, and use proactive operational techniques to collect and analyze cyber intelligence
- Focus on Russia and Eastern Europe



# Cyber Assets

- Technical Staff Assistants
- Network Intrusion Forensics Analysts
- DF examiner agents
- NITRO agents
- Investigative Analysts
- Financial Analysts
- CSP (Critical Systems Protection) Agents
- Task Force Officers (SLTT)





## National Computer Forensics Institute

- Established in 2008
- Partnership initiative between Secret Service, Department of Homeland Security, Alabama District Attorneys Association, State of Alabama, and City of Hoover, AL
- Nation's premier federally funded cyber training center for Secret Service CFTF SLTT partners:
  - Law enforcement officers/Prosecutors/Judges



# NCFI Results in Houston

## NCFI Trained Digital Forensic Examiners in Houston

- 40 NCFI Trained State/Local digital forensic examiners
- FY 2020 – 907 exams
- FY2021 – 1687 exams
- FY2022 – 3305 exams
- FY2023 – 3652 exams
- The NCFI recognizes the top forensic examiners each year
  - FY2023 – 640 exams



# Mobile Device Forensic Facility



- A forensic laboratory center at the University of Tulsa specializing in digital forensics of a broad range of mobile electronic devices
- Develops hardware and software solutions for extracting and analyzing digital evidence from mobile devices, to include smart phones, drones, skimmers, and Internet-of-Things (IoT) devices
- MDFF often conducts specialized forensic examinations of devices that were damaged and require expert reconstruction and recovery



# Carnegie Mellon Computer Incident Response Team



**Software Engineering Institute**  
**Carnegie Mellon®**

A federally funded research and development center (FFRDC) as part of the Software Engineering Institute (SEI)

Developing software and systems, designing training curricula, conducting risk assessment and mitigation for critical infrastructure

Providing technical support to complex cybercrime investigations

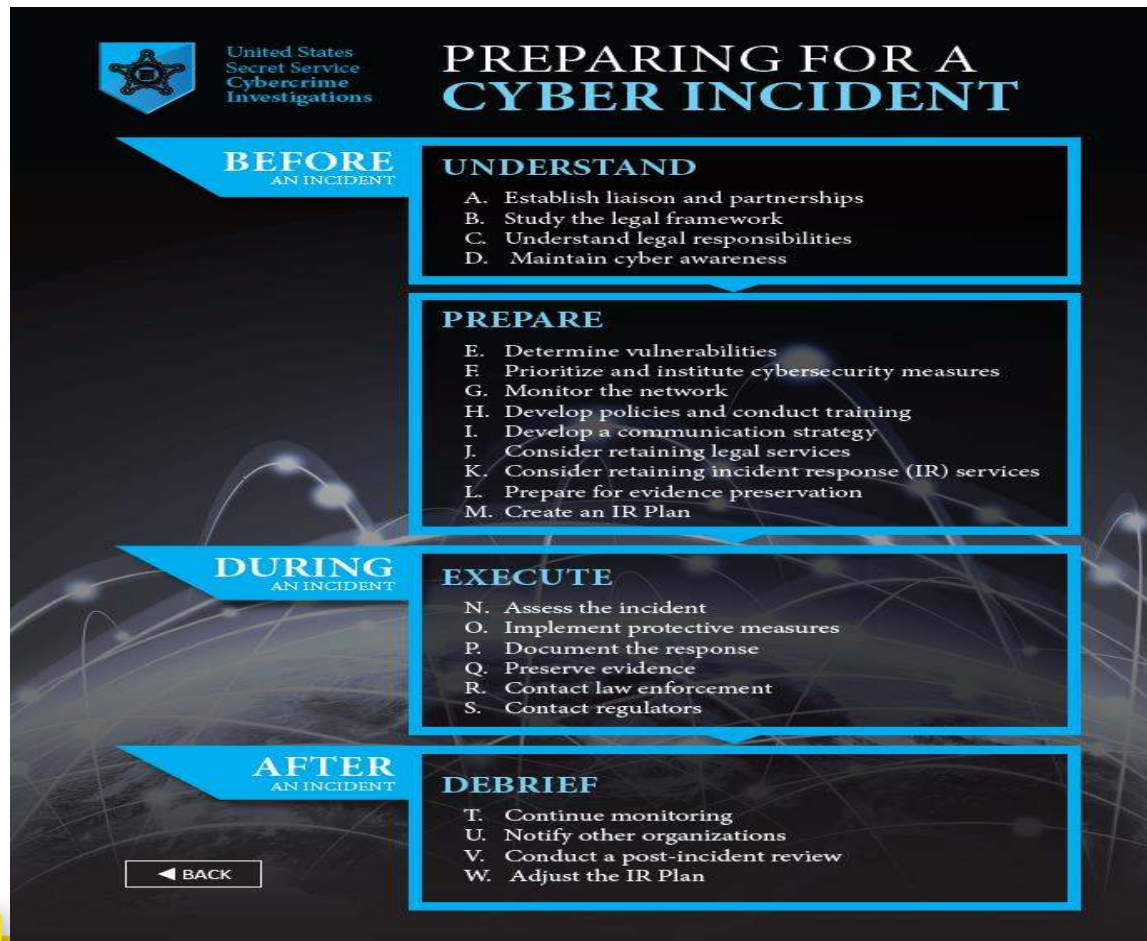
The Secret Service CERT liaison program leverages non-public technology and training to meet emerging cybercrime challenges





# Preparing for a Cyber Incident - Guides

<https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>



# Network Intrusion Response

- TSA (Technical Staff Assistant), NIFA (Network Intrusion Forensic Analyst, or a NITRO Agent (Network Intrusion Response) will respond – may be accompanied by a NITRO trained state/local officer
- No fanfare – lowkey
- Prior to responding we will likely send a consent form for signature, which authorizes the USSS to gather data
- Will request a timeline, network topography map
- Will request memory scrapes and volatile data of the affected system(s), including logs – Can be performed by inhouse or 3<sup>rd</sup> party IR firm, or can be done by a TSA/NIFA/NITRO agent



# What the USSS Does and Does Not Do

## What the USSS WILL NOT do:

- We are not an Incident Response Firm
- We are not a Regulatory Agency
- The USSS will not issue a press release



# What the USSS Does and Does Not Do

## What the USSS WILL do:

- We will work with your Incident Response Team
- We will compare the Indicators of Compromise with other known cases
- We will contact the US Attorney for legal process to determine who is responsible
- We will work with Federal/State/Local Law Enforcement and Foreign Authorities to Identify, Locate and apprehend the human element that is responsible
- Can assist you with managing media, staff and customer briefings





# Responding to Business Email Compromise

- In 2021, the Internet Crime Complaint Center received almost 20k BEC complaints with losses of \$2.4 billion, for comparison, 2021 losses for ransomware were over 3700 complaints that totaled \$49.2 million.
- Ransomware is scary – but BEC's are by far causing the most fraud dollar loss.
- Business Email Compromise is a sophisticated fraud scheme targeting businesses working with other parties that regularly perform wire transfer payments.
- The scam is carried out by compromising legitimate business or personal e-mail accounts through social engineering, malware, or computer intrusion techniques.



# Responding to Business Email Compromise

## **Various means are used to compromise email accounts**

- Phishing attacks both broad and targeted to deploy malware to steal login credentials
- Credential harvesting from dark web scrapes and login credentials from prior data breaches
- Social Engineering used to gain access to email accounts
- Vendor/Invoice Payments
- Payroll Changes
- Using Gift Card
- Impersonating a CEO with a phone call
- Altered Invoice



# Once the Business Email Compromise Occurs

- Once accounts are compromised generally, email rules/auto-forward settings are established to forward out emails to another email account to surreptitiously monitor the compromised email account
- A popular tactic is to create a spoofed look-a-like domain emulating a party in the transaction
- Use of spoofed and/or manipulated personal email accounts is a popular tactic such as Gmail, Yahoo, Hotmail, etc
- Various methods are used to launder BEC funds: Unwitting mules (romance scams), witting mules via shell companies, structured cash withdrawals, purchase of luxury goods, money transmitters, cashier's checks, etc.
- Use of Digital Currency (crypto) is an emerging trend to move and launder BEC derived funds



# BEC Standard Operating Procedure



## Step 1: Regular Email Correspondence

Employees use email correspondence to perform regular business duties, which can include making payments to vendors, processing payroll, or various other financial matters.

## Step 2: Interception



Hackers are able to intercept the email communication, and are able to see who the parties involved are



## Step 3: Spoofed Email Created

Hackers then create a spoofed email address, emulating the client

## Step 4: Send Spoof Email with Instructions



Hackers send a spoofed email address as the client, requesting a transfer of funds – often to newly created bank accounts.



## Step 5: Funds sent to Fraudsters

The instructions appear to be legitimate, and so the business transfers the funds to a fraudster's account





# What Does an attack look like?




Thu 7/18/ [REDACTED]

[REDACTED] <noreplay.s[REDACTED]@[REDACTED].[REDACTED]>

[REDACTED] have 7 new emails

To [REDACTED]

 This message was sent with High importance.

## Office 365

YOU HAVE 7 UNDELIVERED/PENDING MESSAGES

Dear : [REDACTED]

Office 365 has prevented the delivery of 7 new emails

to your inbox as of Wednesday, July 17, [REDACTED]

synchronisation of messages failed due to error in the mail server.

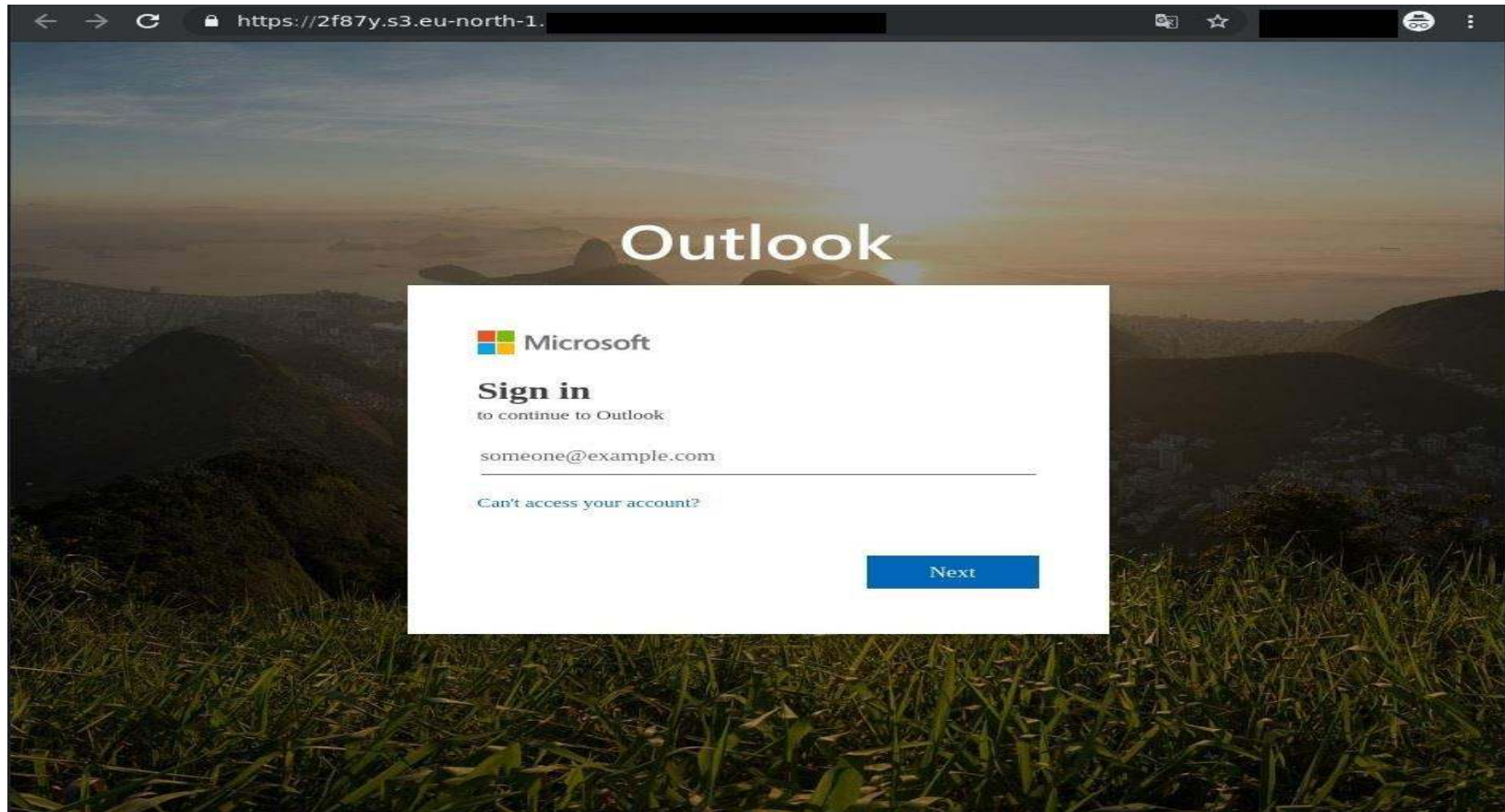
You can review this here and choose what to do with them.

[Read message](#)

[REDACTED] Microsoft Corporation. All rights reserved. | [Acceptable Use Policy](#) | [Privacy Notice](#)



# The Hook is Set





Exchange admin center

Rules

If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. [Learn more about managing Google Chrome cookies.](#)

Rules

- Create a new rule...
- Apply Office 365 Message Encryption and rights protection to messages...
- Apply custom branding to OME messages...
- Apply disclaimers...
- Bypass spam filtering...
- Filter messages by size...
- Generate an incident report when sensitive information is detected...
- Modify messages...
- Restrict managers and their direct reports...
- Restrict messages by sender or recipient...
- Send messages to a moderator...
- Send messages and save a copy for review...

Home

Recipients

Mailboxes

Groups

Resources

Contacts

Mail flow

Message trace

Rules

Remote domains

Accepted domains

Connectors

Alerts

Alert policies

Roles



# Attack Emails

9 messages

[REDACTED] <escrowclosingtitle@[REDACTED].com>  
@ [REDACTED]

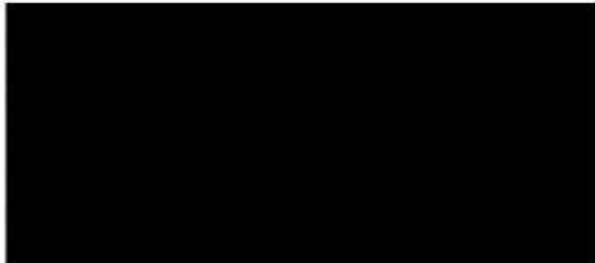
Mon, Mar 28, 2022 at 9:04 AM

Good Morning,

Congratulations on the final steps of your purchase of [REDACTED]  
[REDACTED]

Your closing has been ~~scheduled~~ and CLEARED TO CLOSE, You need to have Cash to close funds wired to our trust account today to avoid closing delay, So that funds can clear in our account on time for closing. I will send the wire instructions once you have acknowledged the receipt of this email, I will be busy with limited access to my phone. You can send an email if you need anything else.

Thank you so much!!



RESIDENTIAL TITLE | COMMERCIAL SERVICES | LOCATIONS [REDACTED]

CONFIDENTIALITY NOTE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is strictly prohibited. If you are not the intended recipient, contact the sender via reply email and destroy all copies of the original message. The sender believes that this E-mail and any attachments were free of any virus, worm, Trojan horse, and/or malicious code when sent. This message and its attachments could have been infected during transmission. By reading the message and opening any attachments, the recipient accepts full responsibility for taking protective and remedial action about viruses and other defects. The sender's employer is not liable for any loss or damage arising in any way from this message or its attachments.





[REDACTED]@tittle.com>

Thu, Mar 10, 2022 at 9:29 AM

Hi [REDACTED]

Thanks for the heads up, having the closing funds earlier prior to closing would actually ensure a smooth closing. I will recommend you using the closing funds out today. Attached is our wiring instructions for your use only. Let me know if we should be on a lookout for the closing funds today .

Best regards,

CLOSER

[Quoted text hidden]

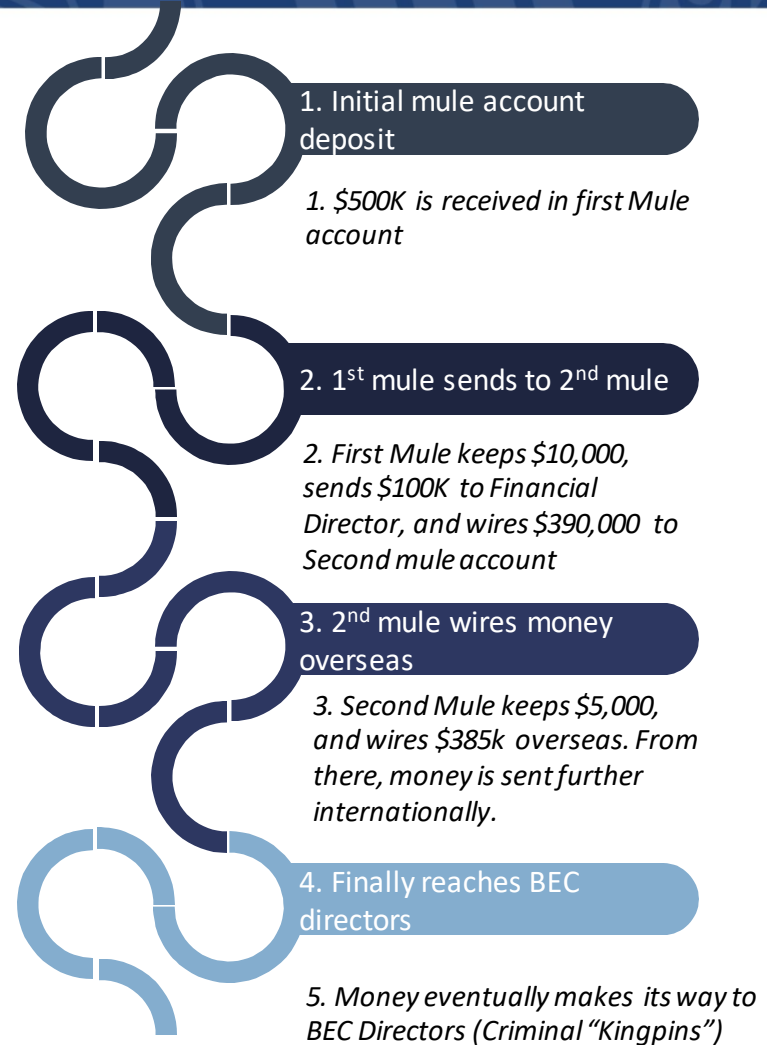


[REDACTED] Wire Transfer Instructions - [REDACTED].pdf

70K




# The Money Laundering Process



# Enterprise Business Model

Operate as businesses – Top to bottom model

Department	Description
 <b>C-Suite</b>	Sets design and targets businesses – Eastern Europe, West Africa
 <b>IT Wing</b>	Carries out hacking, malware, email monitoring – Global
 <b>HR/Recruitment</b>	Recruits IT wing, financial actors – Eastern Europe, West Africa
 <b>Finance/Banking</b>	Sets process for wire transfers and Money Laundering – Global, Local
 <b>Enforcers</b>	Ensures financial cooperation and following of orders – Global
 <b>Admins</b>	Maintain shell companies and legitimate business liaisons – Local
 <b>Burn party</b>	After successful schemes, enterprise burns all materials – Global



# What To Do

- **TIME IS MONEY.** Immediate response is needed, funds are moved within minutes of BEC Fraud
- Contact **BANK**
- Contact **FINCEN**
  - If funds are transferred internationally, FinCEN can initiate a Kill Chain to the Foreign FIU
    - Over \$25,000; Within 72 Hours; Must go international
    - Contact Federal Law Enforcement to initiate
- Contact **LOCAL LE**
- Contact **FEDERAL LE** – USSS (<https://www.secretservice.gov/contact/field-offices>)
- **IC3** – [www.ic3.gov/complaint/splash.aspx](http://www.ic3.gov/complaint/splash.aspx)
- IT CYBER **SECURITY ANALYSIS/PHISHING REPORTING**
- **REPORT REPORT REPORT – HELPS TO PREVENT FUTURE ATTACKS**



# Cyber-Enabled Fraud Prevention

- Register all similar domain names that can be used for spoofing attacks
- Create email rules that flag and delineate emails received from unknown domains. Also monitor creation of new email rules within the email server and cloud environments
- Authenticate all financial transactions through use of dual factor authentication methods – **ENABLE MULTI-FACTOR AUTHORIZATION!**
- Confirm all changes in payment methods with source using trusted and authenticated information, establish out of band comms methods
- Update All software to current versions and security patches
- Educate employees, clients, vendors, etc. on Business Email Compromise
- Conduct a Business Email Compromise drill similar to anti-phishing exercises
- Prepare <https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>



# BEC Prevention Strategies

- USSS combats BEC by investigating financial flows, stopping outgoing wires, mapping BEC actor networks, cyber analysis exploitation, and by providing intelligence, education and awareness on the issue
- USSS employs strategic public/private partnerships to combat BEC through various means of collaboration
- USSS CFTFs and GIOC work in conjunction with other federal law enforcement agencies, state & local partners, and foreign law enforcement to combat BEC
- 42 Cyber Fraud Taskforces around the globe focus on BEC and related cases





# BEC's – USSS Requested Info

- Timeline of events
- Details of the fraudulent wire/ACH (date/amount/routing #/account #)
- A contact at your bank to request the wire/ACH to be reversed
- Copies of emails related to the fraud, including full email header information
- A copy of the o365 Audit Log records from affected accounts
- List of affected email accounts
- Copies of specific malicious emails
- Any suspicious IP's
- Disc images of affected endpoints (if possible)
- Access to Incident Response firms analysis (if applicable)



# Ransomware





# Ransomware

- Is a malicious software (malware) which denies access to systems or encrypts data and/or exfiltrates data
- Non encrypting ransomware locks the computer screen and restricts access to files
- Encrypting ransomware prevents computers from being booted in a live environment by encrypting the Master Boot Record (MBR)
- Criminals hold data hostage until a ransom is paid for a decryption key
- Paying the ransom does not guarantee regaining access or that exfiltrated data will not be sold on the dark web



# Ransomware Response

- Do not power down or shutoff any systems affected by ransomware
- Isolate the infected device from your network
- Secure backups by taking them offline and ensure they are free of malware
- Use out-of-band methods of communication, do not trust your network's email system
- Collect and secure partial portions of the ransomed data that might exist
- Collect all available log information
- Change online account and network passwords after removing the system from the network



# Ransomware – USSS Response

- Threat Detection of the USSS to Ransomware
  - Scope Assessment – What are we facing
  - Data Acquisition - Collect Compromised Data
  - Forensic Analysis – Investigate the data
  - Threat Detection – Finding out what the threat is/was
    - Steps 1 -4 can be repeated as additional threats are discovered
  - Containment and Remediation – Isolate and make corrections as needed.



# Ransomware – USSS Requested Info

- Ransomware variant name
- What systems are affected
- Original emails with full headers and any attachments, if attack was executed by phishing
- Copies of executables or other files dropped onto the system after accessing malicious attachments, including a splash page
- Any domains or IP address communicated with just prior to or during infection
- Virtual currency addresses to which payment is requested
- Memory captures
- IR Reports/Network Topology Map
- The USSS will share this info with the FBI





# Ransomware – USSS Requested Info

- Needed for the Investigation of the compromised system:
  - Filenames and directory structures
  - File Signatures, such as hash values and strings
  - Registry Keys and Values
  - Log messages
  - User Account Information
  - Process names and paths
  - Network Connections



# Critical Infrastructure Compromise

- Highway and Motor Carrier encompasses more than 4 million miles of roadway, more than 600,000 bridges, and more than 350 tunnels. Vehicles include trucks, including those carrying hazardous materials; other commercial vehicles, including commercial motorcoaches and school buses; vehicle and driver licensing systems; traffic management systems; and cyber systems used for operational management.



# What can be done

- Transit agencies can prevent ransomware attacks by ensuring that technical measures receive due attention. Network segmentation, endpoint anti-malware software and routine patching can help kick ransomware to the curb. Implement zero trust with remote devices or even devices within the company.
- Build backup systems. Ransomware attacks can ruin computer systems, leading to long-term disruption. While the problem is being investigated, it could cost the organization hours, days or even weeks at a time of lost revenue and work. A backup can help beat ransomware by offering a quick means through which to restore files, accounts and access.
- Audits of cyber security infrastructure to test systems and exploit vulnerabilities.
- Create an Incident Response Plan and include Legal.



# Questions?



*U.S. Department of  
Homeland Security*

United States  
Secret Service



**Office of Investigations  
Houston Field Office**

THE OVERALL CLASSIFICATION OF THIS PRESENTATION IS:  
UNCLASSIFIED/FOR OFFICIAL USE ONLY/ (U/FOUO)