HANDLING A CYBERSECURITY INVESTIGATION

An Interactive Tabletop Exercise

THE BRIEFEST OF INTRODUCTIONS

SHAMOIL SHIPCHANDLER
Regional Director
SEC
Fort Worth, Texas
817.978.3821
shipchandlers@sec.gov

CHAD PINSON
Executive Managing Director
Stroz Friedberg
Dallas, Texas
214.377.4553
cpinson@strozfriedberg.com

JAY JOHNSON
Partner
Jones Day
Dallas, Texas
214.969.3788
jjohnson@jonesday.com

OUTLINE: HANDLING A CYBERSECURITY INVESTIGATION

COMMON THREATS

REGULATORY LANDSCAPE

TABLETOP EXERCISE

Common Threats

Malware	Brute Force Attacks
Lost Laptops, Backup Tapes	Denial-of-Service (“DDoS”)
Fraudulent Wire Transfers	Ransomware
Advanced Persistent Threats	Phishing
Industrial Espionage	Spyware & Other Invasive Software
Third-Party Vulnerabilities	Insider Threats

REGULATORY LANDSCAPE

- FTC
- SEC
- States
- DOJ

HYPOTHETICAL INCIDENT

SCCE, Inc.

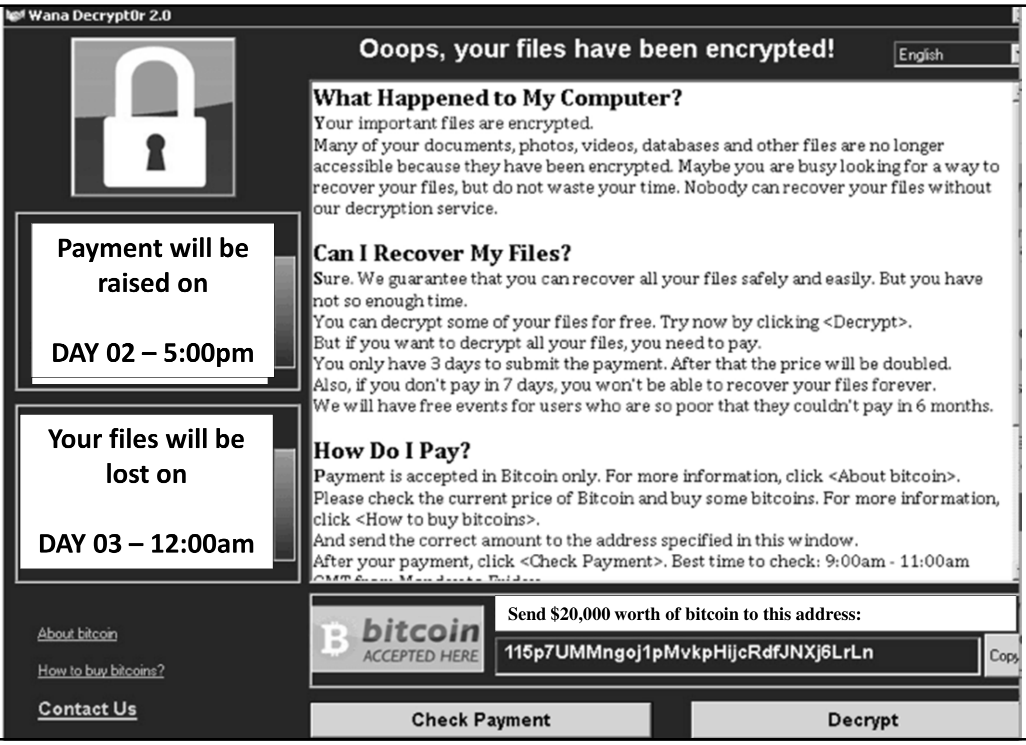
A provider of compliance-related educational services.

Regulated by the National Compliance Education Agency (NCEA)

DAY 01

- Karl works at SCCE and reports to IT that his laptop is “locked on a scary screen” and is asking for “a bunch of bitcoins or something.”
- Others report that SCCE’s files containing forward-looking financial information and HR data are no longer accessible.
- Karl’s computer is locked on the following screen:

□□□



Ooops, your files have been encrypted!

Payment will be raised on

DAY 02 – 5:00pm

Your files will be lost on

DAY 03 – 12:00am

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

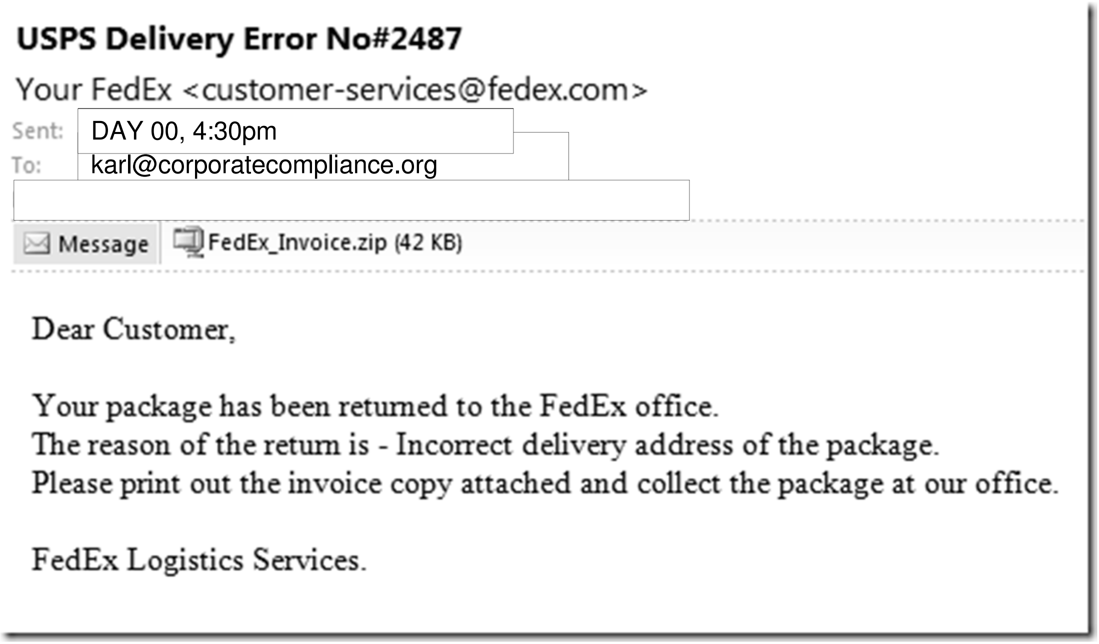
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $20,000 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

DAY 02

- IT quickly reviews available network logs and detects unusual network activity.
- IT identifies a malicious email that was sent to Karl on DAY 00.



USPS Delivery Error No#2487

Your FedEx <customer-services@fedex.com>

Sent: DAY 00, 4:30pm

To: karl@corporatecompliance.org

Dear Customer,

Your package has been returned to the FedEx office.
The reason of the return is - Incorrect delivery address of the package.
Please print out the invoice copy attached and collect the package at our office.

FedEx Logistics Services.

DAY 03

- A well-known blogger blogged.
- An anonymous tweeter tweeted.

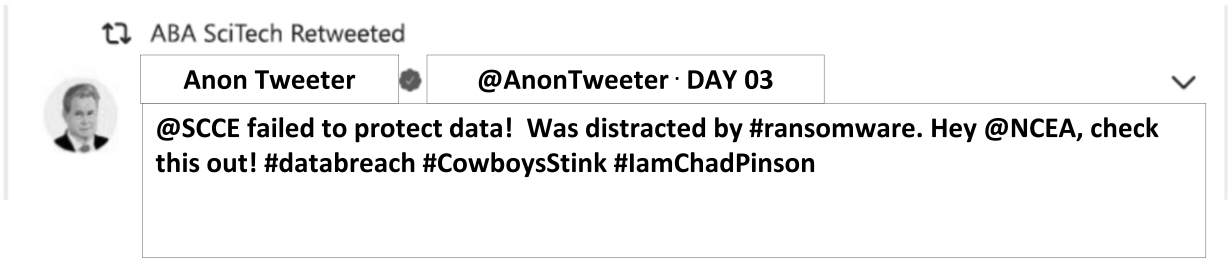
Johnson Speaks – You Listen

Thoughts from a well-known blogger.

Compliance-Related Education Providers Attacked

DAY 03, 2:30pm

Compliance-related education service providers are being targeted in a phishing and ransomware campaign. The phishing emails carry ransomware and malware known as Compliance.exe, capable of exfiltrating HR, finance, and other data. Sources confirm that SCCE has been targeted.



ABA SciTech Retweeted

Anon Tweeter @AnonTweeter · DAY 03

@SCCE failed to protect data! Was distracted by #ransomware. Hey @NCEA, check this out! #databreach #CowboysStink #IamChadPinson

DAY 04

- FBI contacts SCCE to arrange an immediate "conversation" about confirmed data loss. FBI requests all written information concerning the incident.

- SCCE's forensics firm confirms that the phishing email to Karl led to the ransomware attack, and that the email also included the malware Compliance.exe. The firm confirms data loss.

DAY 35 (Post Incident Notification)

- Access Letter from NCEA requests “documents sufficient to identify the cause of the security incident” and “documents evidencing SCCE’s software patching process.”
- NCEA requests interviews with Karl and other key SCCE employees and executives.

DAY 60

- NCEA issues Civil Investigative Demand (CID) requesting all information related to the security incident.

DAY 90

- NCEA files a complaint against SCCE for inadequate data protection practices.

QUESTIONS?

SHAMOIL SHIPCHANDLER
Regional Director
SEC
Fort Worth, Texas
817.978.3821
shipchandlers@sec.gov

CHAD PINSON
Executive Managing Director
Stroz Friedberg
Dallas, Texas
214.377.4553
cpinson@strozfriedberg.com

JAY JOHNSON
Partner
Jones Day
Dallas, Texas
214.969.3788
jjohnson@jonesday.com