Information Security Updates

Thomas Tyler, Cybersecurity Advisor
05.12.21

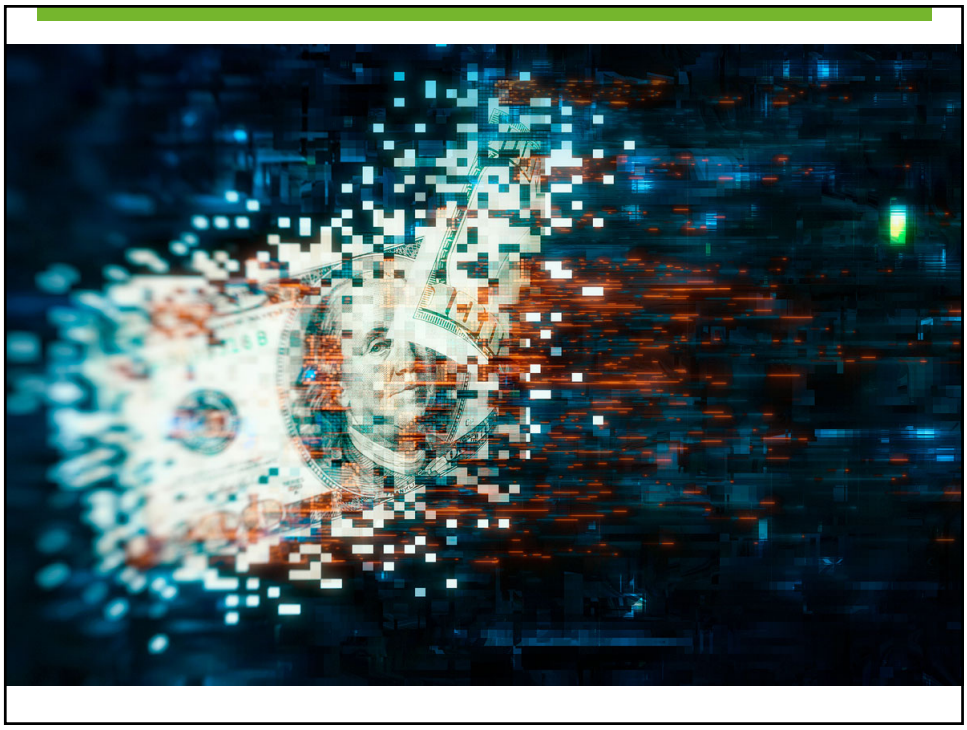
CAPINTECH

1

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

2

3



4

5

MultiCare

Nebraska Medicine

U.S. Cellular

SITA

BONOBOS

T-Mobile

GEICO

STATE OF CALIFORNIA DMV DRIVING CHANGE... DEPARTMENT OF MOTOR VEHICLES

FRESH FOR EVERYONE Kroger

6

UBIQUITI NETWORKS

January 2021

- Device and IoT vendor
- Unauthorized access to database through third-party cloud provider
- Undisclosed number of records
- Not certain that user data was exposed

7

SocialArks

January 2021

- Chinese social media management company
- Unsecured database leak exposing 214m+ records
- Accounts across various social media platforms

8

February 2021

- COMB – “Compilation of Many Breaches”
- Largest of all time
- 3.2 billion unique credentials
  - New and previously breached information
  - Easy to search and well-organized

9

Exchange

March 2021

- Four flaws granted access to 30k+ U.S.-based organizations
- Range from small businesses to city governments
- Total remote control of affected systems

10

Colonial Pipeline Company

May 2021

- Operator of one of nation's largest pipelines
- Precautionarily shut down, work to restore systems continues…
- 2.5m barrels daily – 45% of east coast fuel supply
- Ransomware on corporate systems

"Our goal is to make money and not creating problems for society." - DarkSide

11

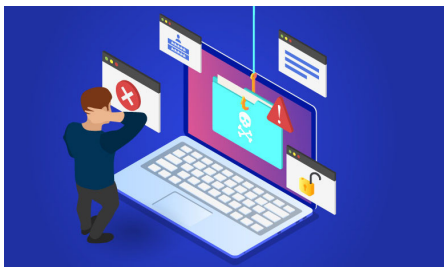
12

13

14

Phishing Background

- Install malware
- Steal credentials
- Obtain information
- Perform a task



15

Phishing Background

- 3% of users will click on any phishing campaign
- 16 minutes until the first click
- 28 minutes until the first report

16

Classic Examples

AD

Allison Davis <box@itservermailbox.net>
Tue 12/18/2018 6:11 AM
Christina Bishop

EXTERNAL

Morning Christina

I would like to update my direct deposit details as i have just switched banks, would the change be effective for the next pay date?

Thanks

Allison Davis

17

Classic Examples

From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2018 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com.
Subject: Please handle ASAP

– External email. Forward any suspicious emails to bad@yourcompany.com –

Hi James,

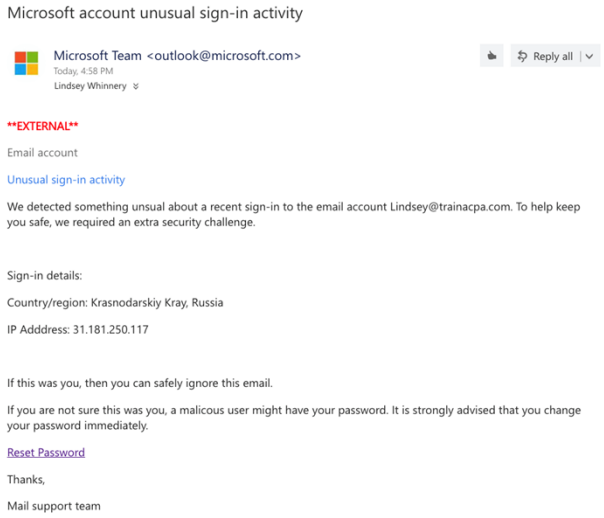
I'm currently tied up in a meeting for the next six hours, but we have a vendor saying we're late on paying an invoice. Can you handle the attached ASAP? I can't take calls, so just email me if you have questions.

Susan Fry
Chief Operating Officer
sfry@yourcompany.com

Sent from my iPhone, please excuse typos

18

Classic Examples



Microsoft account unusual sign-in activity

Microsoft Team <outlook@microsoft.com>
Today, 4:58 PM
Lindsey Whinnery

Reply all

EXTERNAL

Email account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the email account Lindsey@trainacpa.com. To help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: Krasnodarskiy Kray, Russia

IP Adddress: 31.181.250.117

If this was you, then you can safely ignore this email.

If you are not sure this was you, a malicous user might have your password. It is strongly advised that you change your password immediately.

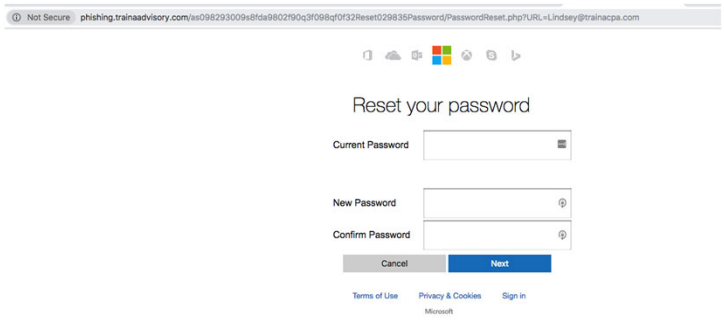
Reset Password

Thanks,

Mail support team

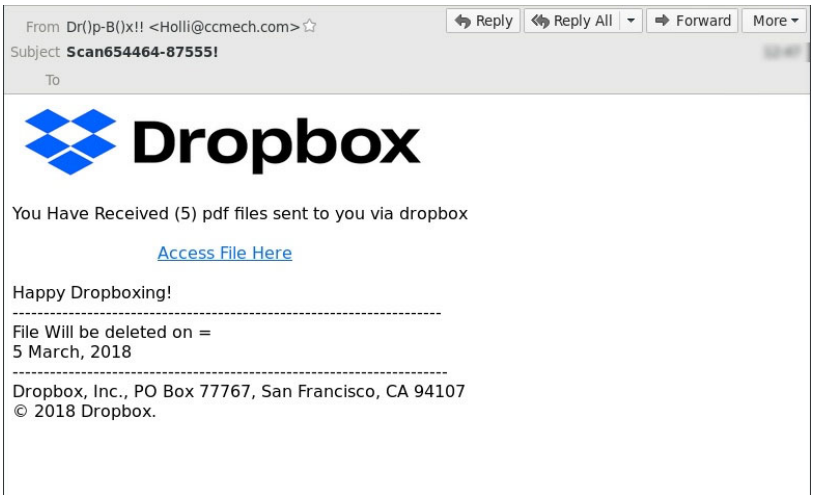
19

Classic Examples



20

Classic Examples



21

Classic Examples

22

Classic Examples

From: [redacted]
Date: Wed, Nov 14, 2018 at 1:06 PM
Subject: Re[2]: Follow up
To: [redacted]@nyu.edu>

I'm in a meeting right now and that's why i'm contacting you through here. I would have called, I don't know when the meeting will be rounding up. And i want you to help me out on something very important right away.

i need you to help me get an Amazon gifts card from the store, I will reimburse you when i get to the office.

I need to send it to someone and it is very important I need to get it sent Asap.

It's one of my best friend son's birthday!

The amount i want is $100 each in two (2) piece making it a total of $200 I'll be reimbursing back to you. I need physical cards which you are going to get from the store. When you get them scratch off the cardboard take a picture of them and attach it to the email then send it to me here okay.

--

[redacted]

23

Classic Examples

From: Donna <donna.xxxx@alttitle.com>
Sent: Wednesday, May 16, 2018 2:08 PM
To: xxxxxxx@gmail.com
Cc: closingagent29@gmail.com
Subject: 2 Meadowvlew Mont

Dennis,
Your cash to close is $30,518.97, And we don't accept cashier check for down payment above 10,000.Can you wire today?
Advise Asap so that i can forward you the title wire instructions.
I advise you wire today.

Thank you,

From: Dennis [mailto:xxxxxxx@gmail.com]
Sent: Wednesday, May 16, 2018 2:13 PM
To: 'Donna' <closingagent29@gmail.com>
Subject: RE: 2 Meadowvlew Mont

Ok please give me the address to wire it to

24

Classic Examples

Subject: Your account is being used by another person!

EXTERNAL

Hi, stranger!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy (you know what I mean).

While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people),
and the second part shows the recording of your webcam.

What should you do?

Well, I think $670 (USD dollars) is a fair price for our little secret.
You will make a bitcoin payment (if you don't know, look for "how to buy bitcoins" on Google).

BTC Address: 1GjZSJnpU4AfTS8vmre6rx7eQgeMUq8VYr
(This is CASE sensitive, please copy and paste it)

Remarks:
You have 2 days (48 hours) to pay. (I have a special code, and at the moment I know that you have read this email).

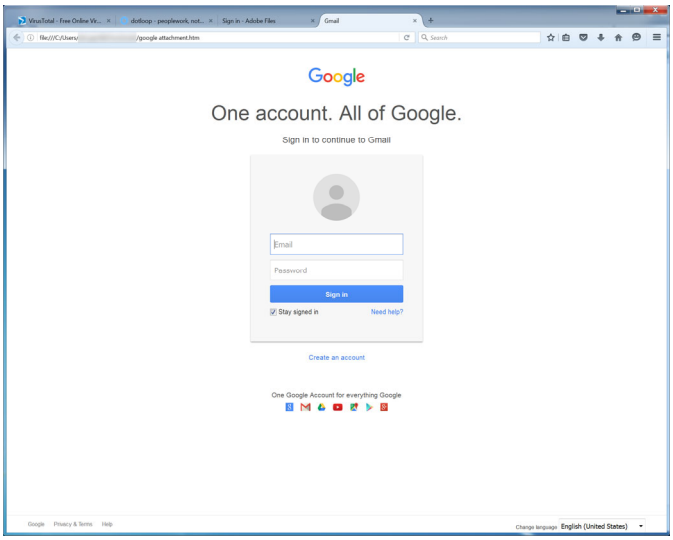
If I don't get bitcoins, I will send your video to all your contacts, including family members, colleagues, etc.
However, if I am paid, I will immediately destroy the video, and my trojan will be destruct someself.

If you want to get proof, answer "Yes!" and resend this letter to youself.
And I will definitely send your video to your any 11 contacts.

This is a non-negotiable offer, so please do not waste my personal and other people's time by replying to this email.

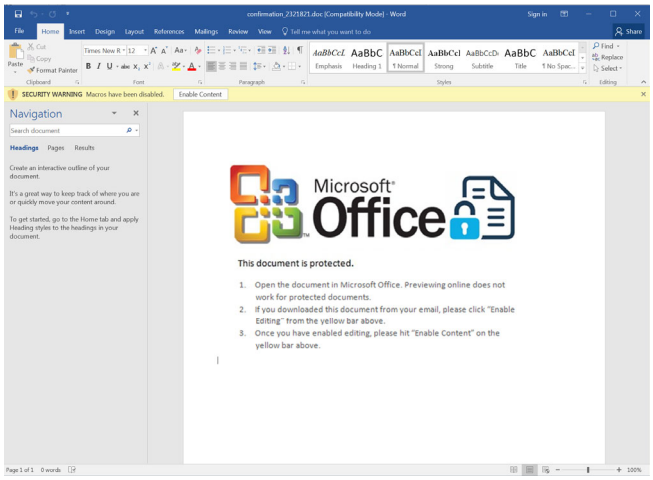
25

Malicious Attachments



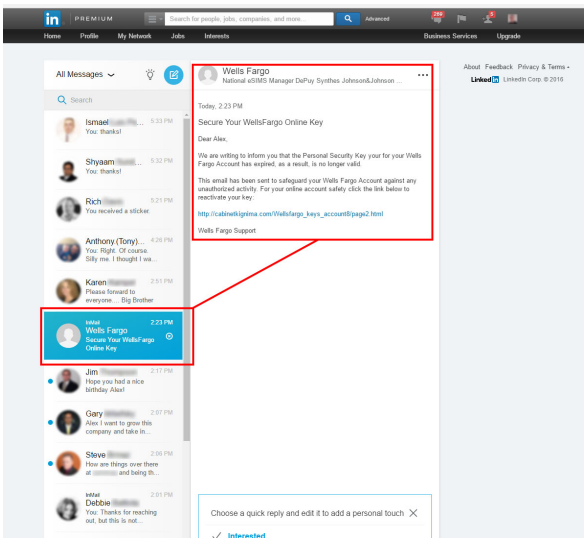
26

Malicious Macros



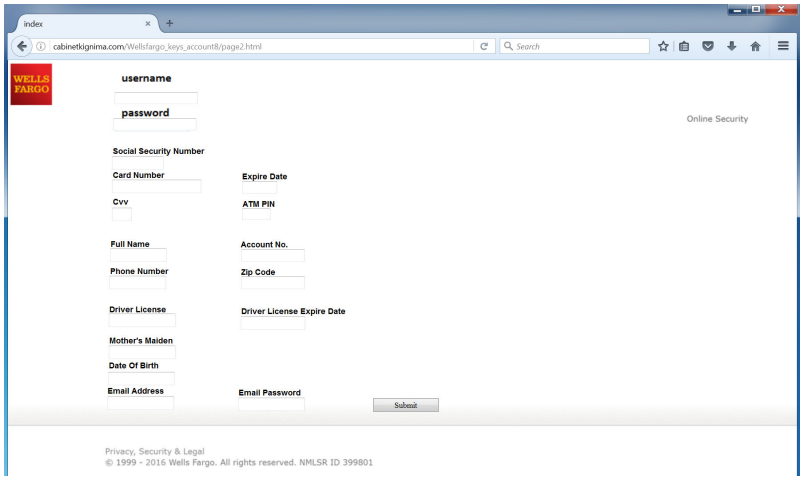
27

Social Media Exploits



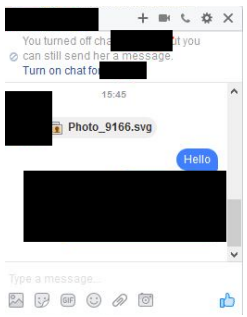
28

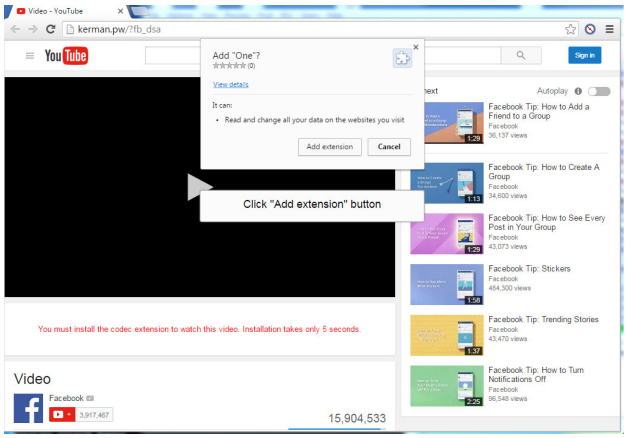
Social Media Exploits



29

Social Media Exploits





30

Other Examples

- Posing as vendor to change bank account information
- Use similar domain name
  - joe@alliedconsulting.com
  - joe@alliedconsulting.com
  - aliiedconsulting.com

31

32

33

Phishing Attempts

- Inspect for typos
- Check email address and domain name
- Click correctly
  - Hover over link
  - Right click and copy
  - Visit website manually

34

Phishing Attempts

- It doesn't feel right
- Tone is off
- Urgent/threatening
- Unfamiliar or unexpected

35

Account Takeover

CAPINTECH

36

Account Takeover

- Criminals gain access to business finances
  - Unauthorized transactions or funds transfer
  - Creation of new/fake employees
  - Stolen customer information
- Criminals gain access to bank information

37

Account Takeover

- How is this accomplished?
  - Lack of security
  - Phishing/malware
  - Credential stuffing
  - Business email compromise

38

Account Takeover

- Lack of security
  - Logged into Internet banking
  - Password management auto-populates passwords
  - Sends code to text or email on device

39

Account Takeover

- Phishing & Malware
  - Exploited devices allow access
  - Sensitive information obtained
- Credential Stuffing

40

Account Takeover

- Business Email Compromise (BEC)
  - Emails appear legitimate
  - Requests seem normal
  - Utilize spoofed/fake email accounts or malware

41

42

Protection & Prevention

- Banking Controls
  - Multi-factor authentication
  - New user alerts
  - Device authentication/restriction
  - Enhanced high-risk transaction controls

43

Protection & Prevention

- Organization Controls
  - Employee education
  - Proper security
  - Monitor for suspicious activity
  - Understand responsibilities

44

45

Security Concerns

- Third-party vendors
- Organization responsibilities
- End-user assistance

46

Third-Party Vendors

- Business, financial, and reputational risks
- Data loss via deletion, corruption, or alteration
- Comingling of data
- Unauthorized access
- Malware
- The list continues…

47

Third-Party Vendors

- Initial and ongoing due diligence
- Critical vs. non-critical vendors
  - Managed service providers
  - Accounting platforms
  - Customer/client management
  - The list continues…

48

Third-Party Vendors

- Annual risk assessment
- Financial condition
- Security controls
- Business continuity and disaster recovery planning
- Incident response (breach notification, insurance)
- Fourth-party vendor management
- Compliance (PCI, GDPR, Identity Theft)

49

Third-Party Vendors

- Contract review
  - Confidentiality, InfoSec, and breach requirements
- Vendor evaluation
- Product/service/technology risk assessment
- Approval, modification, termination

50

51

52

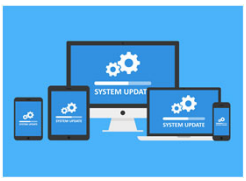
Device Management

- Centralized system
  - All devices receive latest updates or definition files
  - Remediate issues
- Limit access
  - Application and browser add-ons
  - Avoid sharing devices

53

Device Management

- Personal Devices
  - Update and secure across home network
    - Patch and anti-malware management
  - Router, streaming devices, voice assistants, appliances, smart home devices
  - Establish Acceptable Use Policy (AUP)
  - Obsolete software



54

Mobile Devices

- Inherent threats for devices
- Maintain inventory, regardless of ownership
- Enforce restrictions
  - Passwords/biometrics
  - Encryption
  - Remote wipe

55

Mobile Devices

- Consider mobile device management (MDM) software
- Establish data removal procedures
- Cloud data restrictions

56

Mobile Devices

- Recently released: iOS 14.5
- Focus on Privacy
  - “Privacy Nutrition Labels”
  - App Tracking Transparency
- Unlock with Apple Watch

57

IoT Devices

- Inventory devices in use
- Layered security controls
  - Strong passwords
  - Evaluate data and analytics sharing
  - Patching procedures
  - Disable features
  - Segmented network

58

Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often, and when compromised
- # of characters (8…12…??)

59

Password Security

- Unique and private passwords
  - Password manager?
- Business ≠ Personal
- Account lockout and inactivity threshold
- Biometrics
- Layered security

60

Multi-Factor Authentication

- Critical for all cloud applications
  - Remote access
  - Email
  - AWS/Azure
- Consider IP address, time, and day restrictions
- Mobile devices, email message, tokens

61

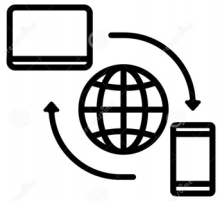
User Provisioning and Access

- Minimum rights for users
- Review regularly
  - Job transfers
  - No longer needed

62

Remote Access Tools

- VPNs, LogMeIn, GoToMyPC
- Increase in end-users
- Require proper security measures
- Quick fixes vs. long-term solution



63

Wi-Fi Networks

- Use properly secured Wi-Fi at work and home
  - Encrypt network appropriately (at least WPA2)
  - Secure password for access
  - Guest network
- Be wary of public Wi-Fi (VPN)
  - Mobile hotspots

64

Shadow IT

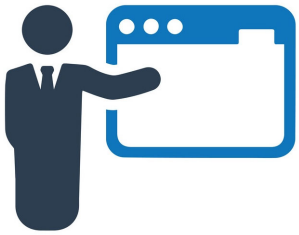
- Apps or devices that are utilized without IT knowledge
  - Personal or mobile devices
- Rogue cloud services
  - Personal email, document scanning, cloud storage
- Appropriate authorization procedures

65

66

Training

- All employees should participate
- Methods will vary — webinar, email, newsletters, etc.
- Review policies and procedures
- Real-world examples
- Build culture of awareness



67

Key Takeaways

- New threats to consider that weren't on our radar 12 months ago
- Loss of reputation can be significant
- Maintain adequate security controls
  - Provide critical tools for users
  - Doesn't have to be expensive!

68

Join Us for Our Next Cyber Series Webcast

The State of Ransomware and Enhanced Controls
Wednesday, June 23
1:00 – 2:00 p.m. EDT

Learn more and register at capincrouse.com

69

You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2021 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced in December

70

Thanks!

Thomas L. Tyler, Jr.
Cybersecurity Advisor

ttyler@capincrouse.com
505.50.CAPIN ext. 2009

© 2021 Capin Technology LLC

CAPINTECH

71