




1



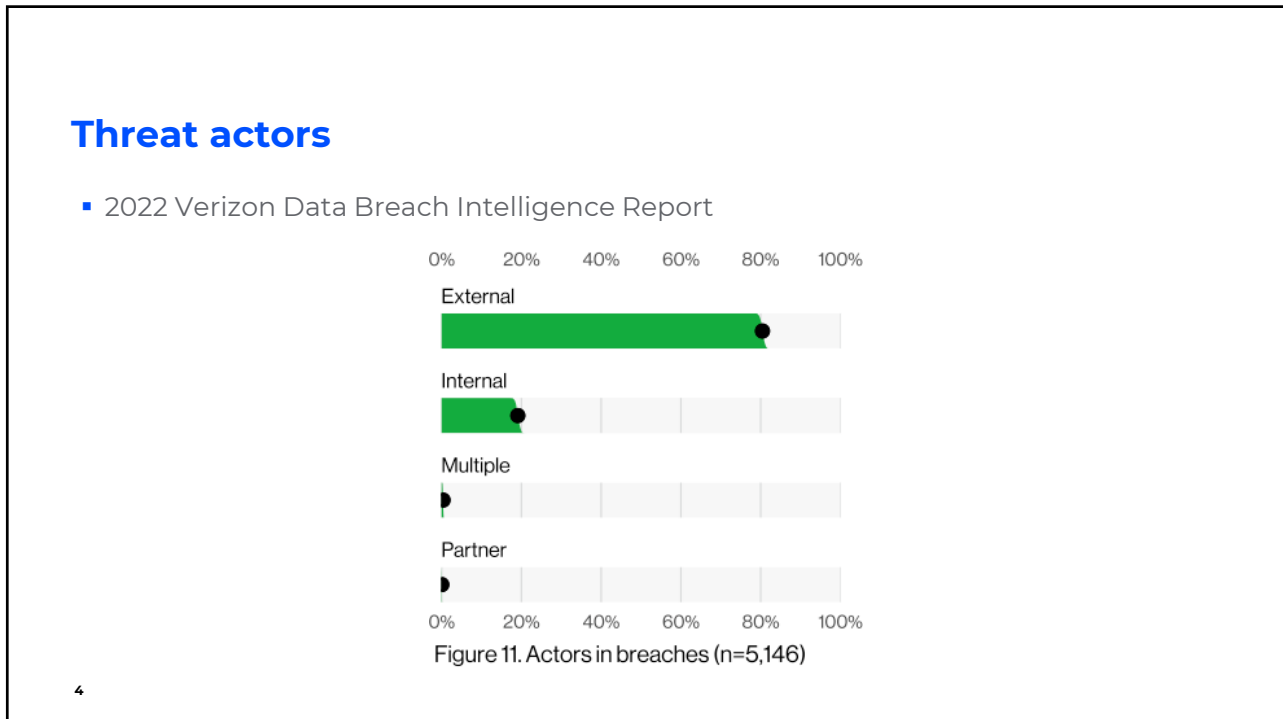
Mark Scholl, Principal, Wipfli LLP
Phone: 815.626.1277 Email: mscholl@wipfli.com

Certified Ethical Hacker (CEH)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Microsoft Certified Systems Engineer (MCSE)

2



3



4

Who are the adversaries?

- Rogue hackers
 - Privateers (organized crime)
 - Nation state-sponsored actors
- Russia
 - Financial scams
 - Election interference
 - North Korea
 - Financial scams
 - Iran
 - Financial scams
 - Election interference
 - China
 - Intellectual property



5

5

State-sponsored threat actors – Sandworm



6

6

Challenges for law enforcement

- Anonymity
 - Originating IP address is difficult to track
 - Dark web users do not use nicknames, usernames, or email addresses from the surface web
- Jurisdictional
 - Safe harbor for “Privateers”
 - Extradition rights
 - Digital crime continues to evolve
- Money trail
 - Cryptocurrencies



7

7

Cybersecurity threats and trends – Email scam types

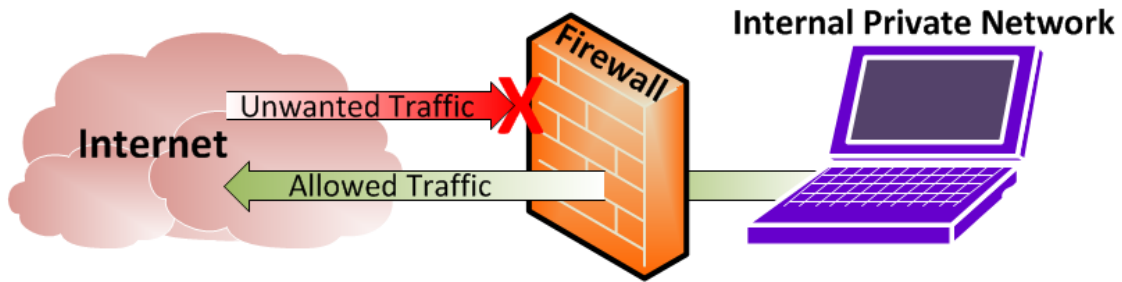


- Email scams are the attack vector!!!
 - Deliver malicious software
 - **Ransomware**
 - **Backdoors**
 - **Keyloggers**
 - Fake websites

8

8

Client-side vulnerability – Email scams

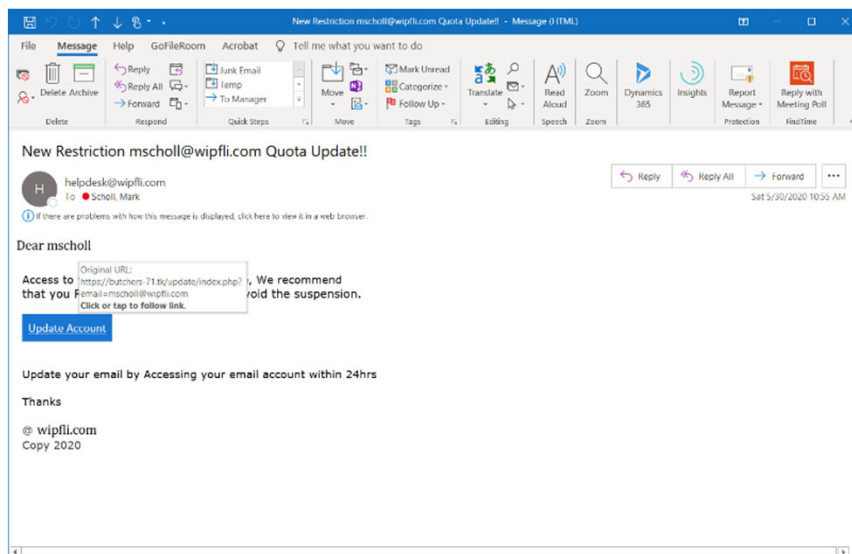


9

9

Email phishing example:

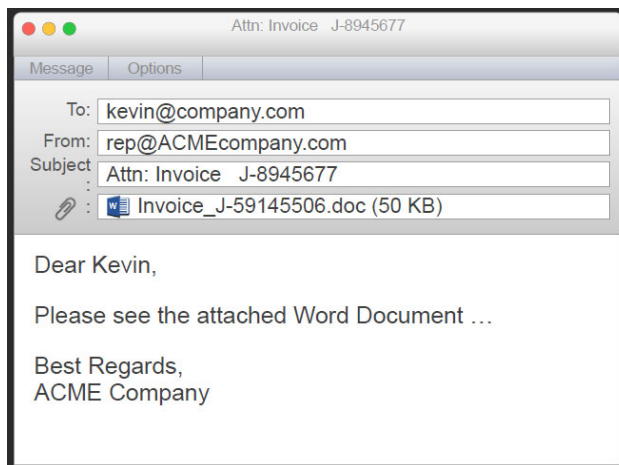
- Password stealing
- Account takeover



10

10

Cyber threat trends – Macro malware



11

11

Payment Fraud – Business email compromise (BEC)

- Attacker targets CxO or business owner; attacker gains access to victim's email account or uses a "look-alike" domain to send a message tricking an employee into performing a wire transfer or other identity scam
 - Fraudulent wire transfer
 - Payroll diversion
 - Gift card scam
 - Tech support scam



12

12

Payment Fraud – Business email compromise (BEC)

From: [REDACTED]
Date: March 23, 2016 at 10:25:39 AM CDT
To: [REDACTED]
Subject: Wire Payment



Mark,

Are you in the office? I'm in a contract meeting til 5pm and i need you to take care of an invoice payment before the cutoff time today.

I'm very busy, Email me.

[REDACTED]
Chairman Emeritus

[REDACTED]
Phone [REDACTED]

[REDACTED]
Fax [REDACTED]
[REDACTED]

13

13

Evolution of ransomware – Dual threat

TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~ 415 USD
Your Bitcoin address for payment: 1LyW9wyajpsC3jSRiZDjp6cDcZ7jMG5

PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash
In case of payment with PaySafeCard or Ukash your total payment is € 400

PURCHASE PRIVATE KEY WITH PAYSAFE CARD OR UKASH

Payment verification may take up to 12 hours.

Support
Message Center

Try to decrypt your file here
You can test the decryption service once for FREE.

Browse...

14

14

Evolution of ransomware – Dual threat

- Encrypt organization's data and require ransom to be paid for encryption key
 - Backup for recovery as a reactive control
- Doxing - Name and shame
 - Threat of leaking the organization's data on the internet
- Average downtime of a ransomware attack is between 19 and 23 days
- Extortion demands have drastically increased – many are demanding six-figure sums to release the data
- Financial institutions can face OFAC violations for paying ransom

15

15

Strong authentication – Passwords

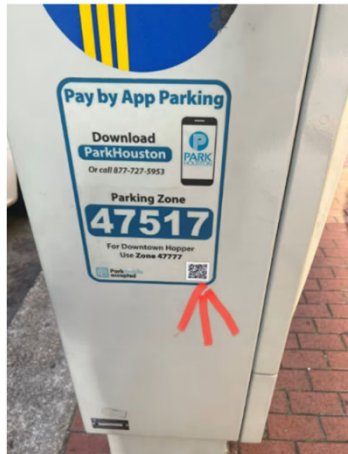
- Hackers continue to use stolen and/or weak passwords
 - Default credentials
 - Common passwords
 - Credential stuffing
 - Malicious software (keyloggers)
 - Tricking victims to disclose password
- Adding two numbers to the end of passwords does not make them stronger



16

16

QR Code Phishing (Quishing)



17

17

Cyber threats – Employee misuse

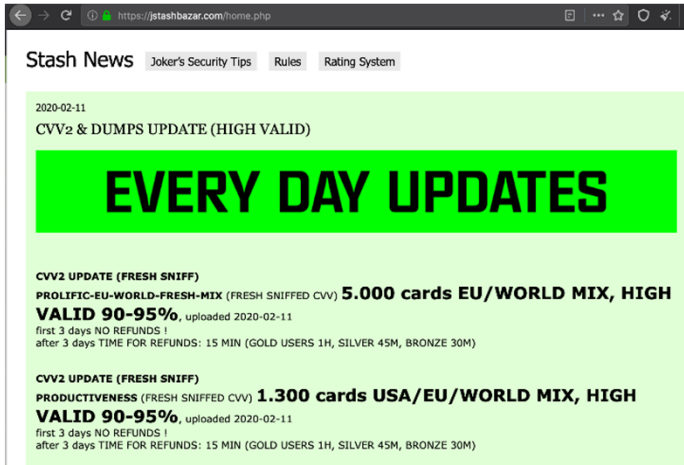
- Lost/stolen laptops, mobile devices, or USB storage devices
 - For nonencrypted devices, the determination of a breach can be difficult, given that you no longer have custody
- “Shadow IT”
 - Rogue systems
 - Not supported



18

18

Cyber Black Market: Joker's Stash



19

19



20

Payment fraud scam detection giveaways

- Purchase gift cards
- Requests financial transaction or change in account number
- Asks for password, credit card/account information, or other private data
- Requests access to your computer
- Urgent!
 - Short deadline
 - Consequence if the requested action is not performed on time
- Don't tell anyone!
 - It's a surprise
 - Victim will face embarrassment

21

21

Risk management and oversight

- Board involvement!!! Ensure cybersecurity moves from the backroom to the boardroom
 - Is the Board updated on cybersecurity issues?
 - Does the Board understand how you are mitigating cyber threats?
 - Make “cybersecurity” a standing agenda item for IT committee, audit committee, and Board meetings
 - Involve the Board members in IT committee meetings

22

22

Top cybersecurity controls

- Use strong authentication
 - Strong passwords
 - Multi-factor authentication (MFA)
 - Out of band authentication
 - **Call backs are best**
- Employ a data backup and recovery plan for all critical information
 - Air-gap/Offline backup media
- Vulnerability management program

23

23

Top cybersecurity controls

- Encrypt sensitive data in transit and at rest
- Endpoint protection (i.e., malware protection and monitoring)
- Managed detection and response (MDR)
 - Uses AI and machine learning for detection and response
- Don't forget physical security

24

24

Third-party risk management

- Must have a strategy to identify, monitor, and mitigate the risks of third-party relationships (based on complexity of the relationship)
- Due diligence for vendor selection
- Ongoing vendor monitoring program
 - It is important to ensure vendors have adequate controls for protecting customer information
 - It is important to understand what a breach at a vendor's operation means to your institution – vendor responsibilities

25

25

Employee training

- Cybersecurity is a team sport!!!
- Understand safeguards
 - Policies and procedures
- Incident response
 - When and how to respond to an incident
 - Who to report the incident to
- Ongoing training works best
 - Shorter and more frequent is better

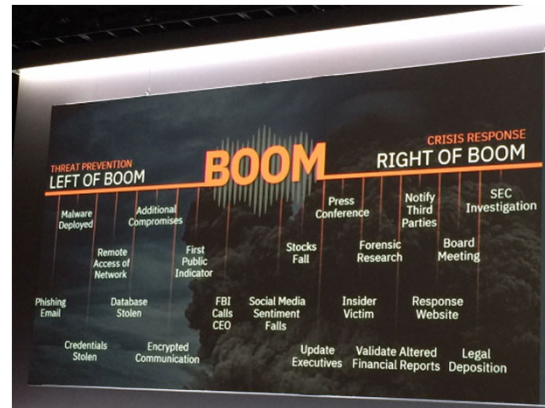


26

26

Cyber incident management and resilience

- Think not “if”, but “when”
- Create a positive cybersecurity culture
- Don't be afraid to admit “I think I just clicked on something bad.”
 - Report suspicious activity immediately
- Know who to report suspicious activity to internally and externally



27

27

Cyber incident management and resilience, continued

- Have enhanced incident response plans
 - Have arrangements with vendors who can work with your institution to implement incident response – a proactive approach, not when an incident has occurred
 - Work with regional crime taskforces
 - Ensure plan includes how you will notify customers
- Ensure there is periodic tabletop testing of your incident response program

28

28

Cybersecurity insurance

- Fee is increasing mostly due to ransomware attacks (74%???)
 - Drastic increase in extortion demands
 - Mandated notifications
- No more blanket coverage
 - Multi-factor authentication
 - Security monitoring
 - Other established safeguards
- Pay attention to exclusionary language

29

29

Cybersecurity testing

- IT Controls Review
- Perimeter Testing
- Internal Vulnerability Assessment
- Cloud Configuration Assessment
 - AWS, Azure, M365
- Social Engineering Training and Testing
 - Email spoofing
 - Pretext calling
 - Physical penetration

30

30



31

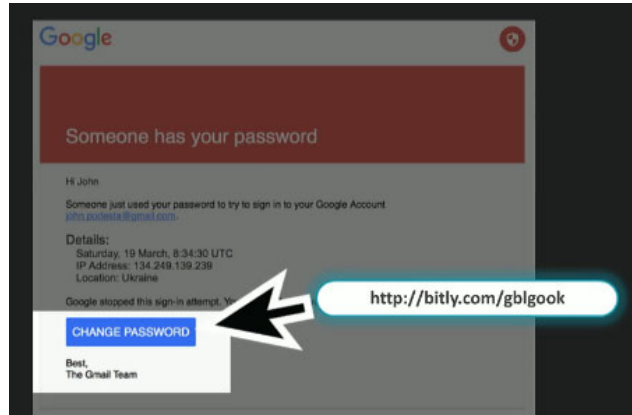
Case study – Targeted phishing attack

The screenshot shows a phishing email designed to look like an official Google notification. At the top left is the Google logo, and at the top right is a red shield icon with a white exclamation mark. Below this is a red header bar with the text 'Someone has your password' in white. The main body of the email is white and contains the following text: 'Hi John', 'Someone just used your password to try to sign in to your Google Account', and a blue link to 'john.podesta@gmail.com'. Underneath, it lists 'Details:' with the date 'Saturday, 19 March, 8:34:30 UTC', 'IP Address: 134.249.139.239', and 'Location: Ukraine'. A warning follows: 'Google stopped this sign-in attempt. You should change your password immediately.' Below this is a blue button with the text 'CHANGE PASSWORD'. The email ends with 'Best, The Gmail Team'. At the very bottom, in small grey text, it says: 'You received this mandatory email service announcement to update you about important changes to your Google product or account.'

32

32

Case study – Targeted phishing attack, continued

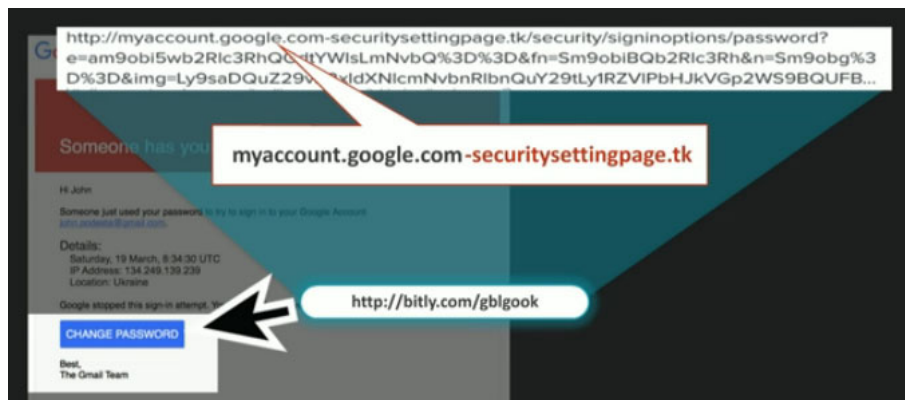


Shortened URL

33

33

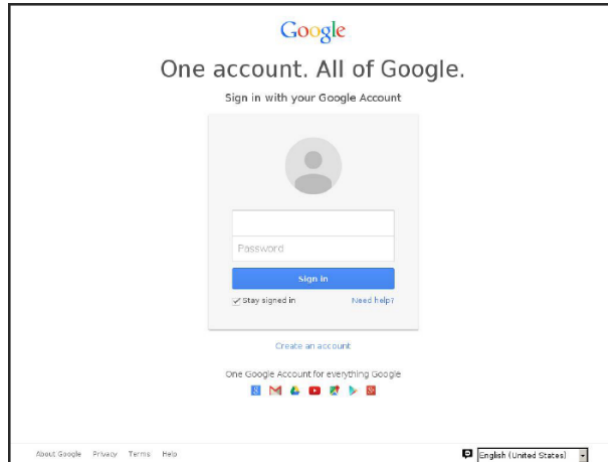
Case study – Targeted phishing attack, continued



34

34

Case study – Targeted phishing attack, continued



35

35

Cybersecurity threats and trends

- Threat actors are interested in you – everyone is a target
 - Small business, large business, individuals...

152%

The increase in data breaches at small businesses globally during 2020 and 2021, compared with the two prior years, according to RiskRecon. Breaches at larger organizations rose 75% in the same period.

RiskRecon Report 2022
WSJ June 7, 2022

36

36

Questions?

37

37