ECKERT SEAMANS

Preparing for the Inevitable: Cyber Incident Response Exercises

Presented by:

Matt Meade

August 7, 2024

2024 Joel Lennen Legal Primer

Mini Cyber Scenarios

IT SUPPORT

- A threat actor finds a Company executive's profile on LinkedIn and sees that he is speaking at an industry conference in Arizona.
- The threat actor calls the tech support service desk impersonating the executive and asking for immediate access to his company account.

IT SUPPORT

- The caller says it is an extreme rush to get immediate access to the network as it relates to a big capital development project that he is working on.
- At first the service desk operator refuses telling the caller that he must follow the Company's end user verification procedure.
- The caller is extremely angry and threatens to fire the service desk operator who eventually gives in.

IT SUPPORT

- What are the consequences of this event?
- Ask MGM!! This is how the TA's claim to have gotten in
- After initial entry, the TA's gained administrator rights and proceeded to deploy ransomware.
- What are your procedures at the tech support desk for these types of calls?

THE CALL

Late on a Friday afternoon the Company receives a call from CISA that it has identified outbound traffic from the Company to known IP addresses used by Threat Actors.

THE CALL

- What steps should the Company take once it learns of this call?
- Should you notify cyber insurance carrier?
- What steps should be taken to contain the incident?
- What steps would you take to verify this event?

DIRECT DEPOSIT

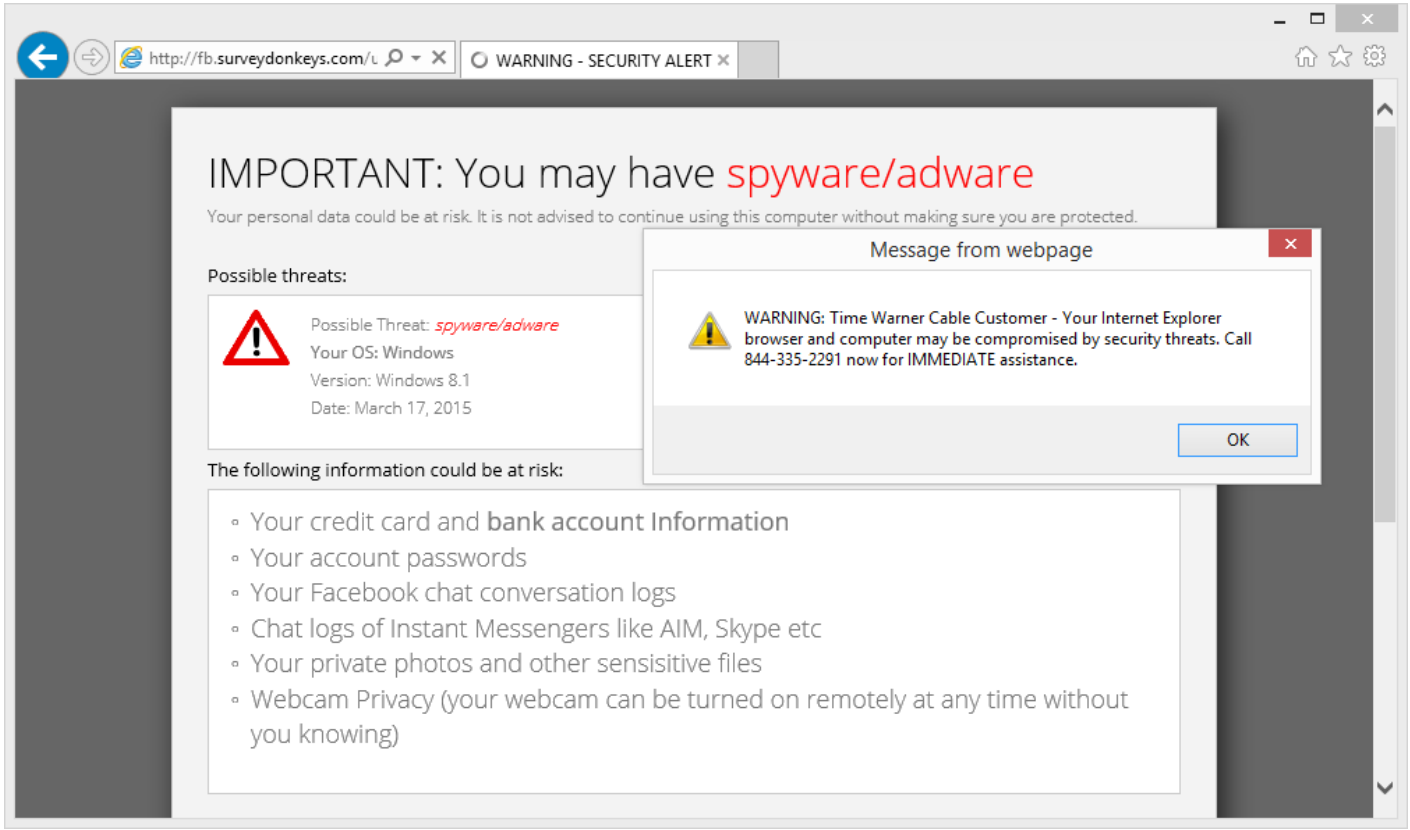
- An employee emails Payroll and asks that her direct deposit be changed to her account at GreenDot Bank. The employee fills out the required paperwork.
- Payroll calls the phone number on the email to verify and processes the request.
- 2 weeks later the employee calls Payroll and demands to know why she did not receive her paycheck in her PNC account.
- What is the role of the Response Team in investigating this incident?

DIRECT DEPOSIT

- What procedures does the Company have in place for requests to change payroll? How are they verified?

- If the email to change banks came from the employee's Gmail address would this be a data breach at the Company?

- If the email to change banks came from the employee's email account what would the IRT do to determine whether there had a been an email compromise?


http://fb.surveydonkeys.com/
WARNING - SECURITY ALERT
IMPORTANT: You may have spyware/adware
Your personal data could be at risk. It is not advised to continue using this computer without making sure you are protected.
Possible threats:
Possible Threat: spyware/adware
Your OS: Windows
Version: Windows 8.1
Date: March 17, 2015
The following information could be at risk:
Your credit card and bank account Information
Your account passwords
Your Facebook chat conversation logs
Chat logs of Instant Messengers like AIM, Skype etc
Your private photos and other sensisitive files
Webcam Privacy (your webcam can be turned on remotely at any time without you knowing)
Message from webpage
WARNING: Time Warner Cable Customer - Your Internet Explorer browser and computer may be compromised by security threats. Call 844-335-2291 now for IMMEDIATE assistance.
OK

POP UP MESSAGE

- While working at home you receive this popup message.
- Because you are concerned about Spyware on your computer you call the number and provide access to the representative who assures you that this shouldn't take long after you pay with a credit card.

POP UP MESSAGE

- Once payment is received, the representative asks to access your email and the word documents stored on your laptop to ensure the spyware is gone
- The job is finished after about an hour. Once you get back on the computer you contact IT because your laptop is not working properly.

POP UP MESSAGE

- Is this a data breach?
- It depends. Providing access increases likelihood of unauthorized access to Company systems including email and network data
- Only allow access to authorized Company IT

CYBER SCENARIO

SCENARIO #1
BUSINESS EMAIL COMPROMISE (BEC)

On Monday morning Acme Builders, a construction contractor that the Company has been working with on a building improvement, asks about the status of a $250,000 payment that was due June 17, 2024.

The Company has a record of wiring the money to Acme on June 13, 2024.

BEC - QUESTIONS

- Would the IRT have any role in connection with this incident at this time?
- How would the Company's legal team find out about this?
- What would the investigation be focused on at this time?

REVIEW

Upon further review of the email account of the employee who made the wire transfer, it appears that Acme sent an email on June 13, 2024 changing payment instructions from prior transactions.

The employee called the number on the email and verified the new instructions.

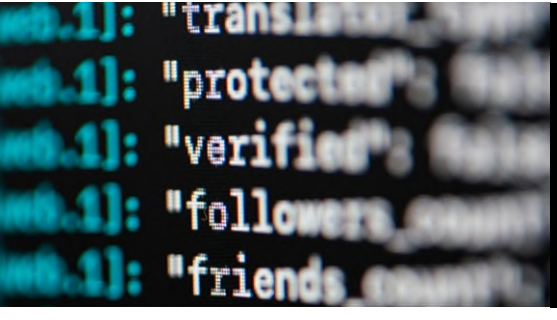
IT investigates the incident and determines that the June 13, 2024 email came from accounts@acmebuilderz.com rather than accounts@acmebuilders.com.

MORE QUESTIONS

- Should insurance be alerted to this situation?
- What is the role of the IRT?
- Is this incident a data breach?
- Should outside counsel be contacted?
- Who is responsible for the lost payment?

INVESTIGATION

The forensic investigation determines that the employee responded to a phishing email and provided his credentials. Shortly after giving up the credentials, the bad actor accessed the employee's email account and set up forwarding rules so that all legitimate emails from Acme Builders were sent to the user's deleted email folder.



The employee had 6 GB of data in his email account including tax information related to the payment of vendors.

CONSIDERATIONS

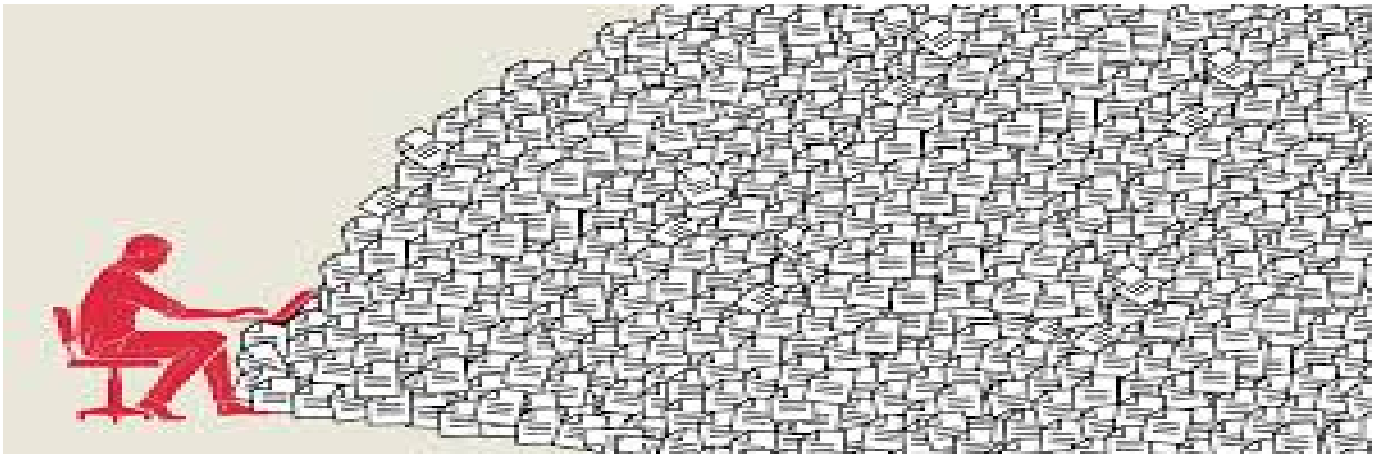
- How would you determine whether this is a breach?
- Who would conduct the investigation of the nature of the access by the bad actor?
- If the forensic investigator finds evidence of copying or synching of the employee's email box what are the next steps?
- If there is no evidence of synching what are the next steps?

TAKEAWAYS

- Failure to verify caller
- Lack of a sense of urgency or awareness who to report to and the need to take immediate action
- Absence of procedures in Incident Response Plan on how to address incidents reported by third parties
- DELAY CAN BE CATASTROPHIC!!

TAKEAWAYS -ROW THE BOAT IN THE SAME DIRECTION

TAKEAWAYS - DATA HOARDING



Questions?

Matt Meade
Cyber Group Chair
412 566 6983
mmeade@eckertseamans.com

ECKERT SEAMANS