Cyber Claim Walkthrough
NJ GMIS – 2018 TEC

Introduction to Kivu

- Kivu - Founded 2009
- Headquartered in San Francisco, with offices in Los Angeles, Denver, NYC, Washington DC, Toronto and Amsterdam
- Expertise in Digital Forensics, Incident Response, and Cyber Risk Management Services (e.g. Risk Assessment, CISO-as-a-Service, Vulnerability and Penetration Testing)
- Testify as experts in post-breach litigation, appear before multiple Federal and state regulators, work heavily with law enforcement
- Pre-approved cyber forensic vendor for US, E.U. & Canadian insurance carriers
  - Pioneered high value remote work (claims managers like that)

Introduction to Speaker

- Shawn Melito, Management Analyst, Kivu Consulting, MBA, CIPP/US, CSP
  - 10+ years of cyber case management experience
    - Have handled 100's of cases from a forensics, notification, call center and identity theft services point of view
    - Started Kroll Canada's Breach Response Group
    - Worked for the Office of the Privacy Commissioner of Canada
    - Ran NPC's Immersion Data Breach Response Group for 5 years
    - Currently in charge of Kivu's relationships with all of the leading cyber insurance companies, brokerages and data breach coaches.

What Attacks Do We See?

- ☹ Ransomware/Extortion (60% - open RDP ports #1 way in)
- ☹ Office 365 / AWS Attacks (20%)
- ☹ Network Penetration (5%)
- ☹ Collateral Damage in Credential Theft/Social Engineering (5%)
- ☹ Lost Devices (5%)
- ☹ Other (5%)

Epidemic of Data Insecurity

- Hacking is a business… and business is great
- Automated tools and techniques available
  - Like Software as a Service (SaaS):
    - Hacking as a Service (HaaS)
    - Ransomware as a Service (RaaS)
    - Distributed Denial of Service as a Service (DDoSaaS)

Anatomy of a Compromise

- Investment in tools and service
- Automate reconnaissance (bots)
- Identify and exploit vulnerabilities – access to system
- Opportunities for lateral movement
- Identify ways to monetize (ROI)
  - Data
  - Disruption
  - Destruction

Cyber Claim Set-up

1. Our client is very cyber savvy, so this will be a best case scenario with the client doing all the right things. Jim will be covering how things can potentially go wrong after.
2. With the City of Atlanta's SamSam attack top of mind, and over 50% of the claims Kivu is currently seeing, let's assume this is a ransomware attack.
3. While our client is cyber savvy, they stored their back-ups locally, and they are also encrypted.

Ransomware

- A typical **ransomware infection** is where some or all of the files on a computer become “locked”
- The attacker leaves behind a **ransom note** with instructions for how to restore the data
- Usually this attack is accomplished by delivering **malware** to the victim computer
- However, some attackers lock the entire hard drive using **legitimate encryption software**, like DiskCryptor or BitLocker

KIVU

☠ YOUR FILES ARE ENCRYPTED! ☠

ALL YOUR IMPORTANT DATA HAS BEEN ENCRYPTED.

To recover data you need decryptor.
To get the decryptor you should:

Send 1 test image or text file [redacted]net.
In the letter include your personal ID (look at the beginning of this document).

We will give you the decrypted file and assign the price for decryption all files

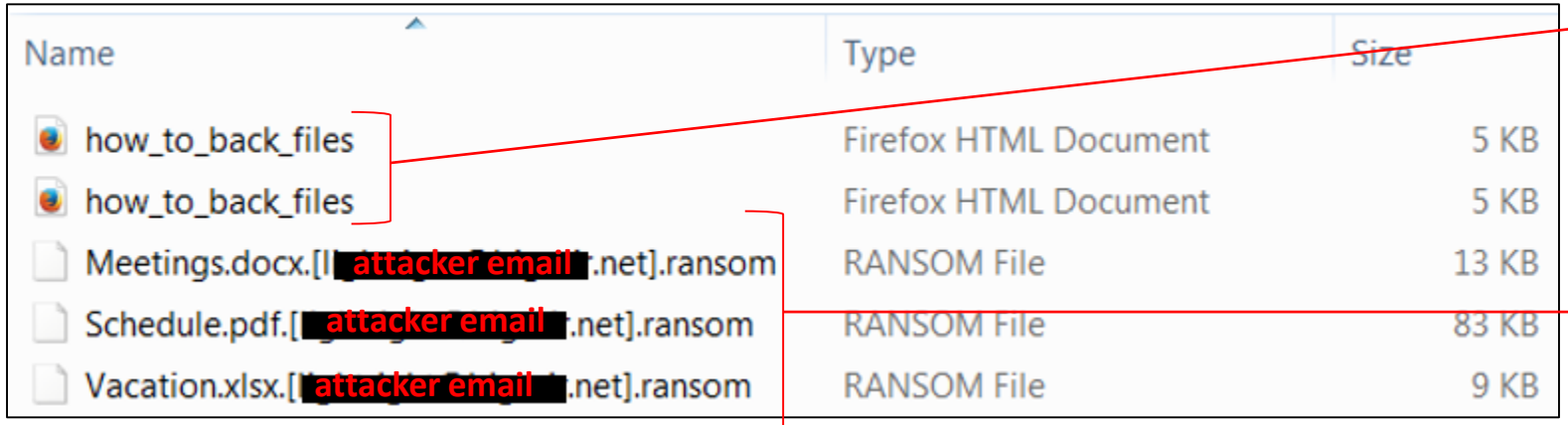
After we send you instruction how to pay for decrypt and after payment you will receive a decryptor and instructions
We can decrypt one file in quality the evidence that we have the decoder.

Attention!

- Only [redacted]net can decrypt your files
- Do not trust anyone [redacted]net
- Do not attempt to remove the program or run the anti-virus tools
- Attempts to self-decrypting files will result in the loss of your data
- Decoders other users are not compatible with your data, because each user's unique encryption key

Before ransomware:

After ransomware:



Ransom notes

Locked files with ".ransom" file extension

KIVU

Stages of the Incident

1. Realization of the Breach:
   - Ransomware note on all computers on start-up
   - Files are locked with ".ransom" extension
   - Email doesn't work properly
2. Segregate infected computers and servers:
   - Shut off Wi-Fi (if you can), unplug hard wire connections, power down
   - DO NOT wipe computers or restore from back-ups without full images, as essential forensic data could be deleted
3. Get out Incident Response Plan (IRP):
   - Call together (using phone or text) response team for emergency meeting (IT, HR, PR, C-Level, G.C., Risk Management, etc.)

Stages of the Incident

4. Review Cyber Insurance Policy:
   - Most (MEL JIF) have a manned 24/7 toll free number for incidents
     - 3rd party claims admin. company, insurers claims group or law firm
     - DO NOT call your brother-in-law or Nerds on Wheels (not on panel)
   - Most policies immediately put you in touch with a "breach coach"
     - Experienced in handling breaches (100's of cases)
     - Privilege is established
     - Eventually, an opinion on incident vs. breach will be needed
5. Initial Incident Response Team Meeting:
   - Gather the "what we know now"
   - Discourage any "investigative techniques" that could potentially destroy forensic data

Stages of the Incident

6. Initial Call with Breach Coach:
   - Relay what you know, and what has been done up to this point
   - Legal agreement to be signed, set-up privilege
     - May want to do this ahead of time (ask insurer who is on panel)
7. Breach Coach starts work:
   - Contacts experienced forensics provider like Kivu and others
     - Breach Coach – “can you be on a call in next hour?”
     - Kivu - Responder – form preliminary team (e.g. industry/sector, technology, location)
   - Contacts insurance claims team (if not done already) to open claim

Stages of the Incident

8. Scoping Call:
   - Who, what, when, where, why relayed
   - Data collected by us for SOW
   - Initial steps to take to defend yourself
9. SOW prepared, sent to breach coach:
   - Sign off by client, breach coach and Kivu
10. Commence Work:
   - Gather evidence remotely, investigate what we can
   - Alternatives to paying ransom – unknown back-ups, rebuild systems
   - Open line of communication and potentially negotiate with attackers

Stages of the Incident

11. Work Continues:
    - Test decryption capabilities of attacker
        - Send five encrypted files to hacker to prove tool works
        - Note - Triple M (MMM), Rapid, Thanatos and Sigma strains all being used by unsophisticated hackers
    - Section 219 check (Sanctions Report)
        - We don’t want to be paying terrorists
12. Decision on Pay or Not-to-Pay:
    - Weigh all data collected above, business decision
    - Wire transfer initiated, Kivu makes payment in bitcoin, wait…

Stages of the Incident

13. Keys Received from Hacker:
    - Decryption tool is also received
        - Place in “sandbox” and tested for further malware (hackers are sneaky)
    - Decryption is tested
        - Sometimes you have to “giggle” the key to make it work
14. Decryption Plan and Instructions Prepared:
    - Key systems first
    - Kivu can provide remote or onsite assistance
15. Real Investigation can Begin:
    - If any evidence outside of ransomware is found, further investigation is necessary
    - Launch KECT (Kivu Endpoint Collection Tool) and analyze findings

Stages of the Incident

16. Determination of breach:
    - Weigh evidence collected
    - Breach coach and client make decision on whether a breach occurred.
17. If decided PII exposed, then:
    - Kivu prepares notification list
    - Breach coach contracts with services providers
        - Notifications written, NCoA performed, letters sent
        - Call center scripts written, call center opened
        - If PFI breached, usually credit monitoring and other IDTheft services offered
18. Reporting to client and breach coach
    - Daily verbal (or more at first)
    - Budget update to claims group
    - Written report (?), report to regulators/third parties
    - Potential testimony (class actions, regulator investigations, etc.)

Current ransomware landscape

- A ransomware attack may be a symptom of a network that's been compromised for months or even years
- It doesn't matter the size of your organization, the value of your data, or the type of industry you are in, if you have a internet facing device you are a target.
- A ransomware attack in the current threat landscape often means there is a breach to investigate, and a determination to be made about notification

Questions?

KIVU