Ransomware Tabletop

Day 1

- On Monday morning, your IT staff starts to receive calls that employees are unable to log into their computers.
- After multiple reports of the same issue, your IT staff begins to investigate the issue.
- The initial investigation identifies a ransom note in a .txt file on one of your servers.

RyukReadMe.txt - Notepad

File Edit Format View Help

```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe
```

Questions

- What is your IT staff’s response after identification of the ransom note?
- How is this incident escalated within your organization?
- How does your incident response team (IRT) get notified?
- Any internal or external communications yet?
- Is legal involved yet?
- Is your carrier/broker involved yet?
- How do you notify other third party stakeholders?

Day 1 (continued)

- By noon, all of your systems are inaccessible and employees are unable to work. Your IT staff has pulled remaining systems offline.
- The IRT holds a status call to discuss the following points:
  - Investigation update
  - Downtime procedures
  - Engaging third party stakeholders including incident response vendors
  - Informing the Board
  - Internal employee communications
  - Legal/regulatory obligations

Fact Inject

- The IRT team notifies your broker and Beazley of the incident. After the initial scoping call with Beazley, a privacy firm and computer forensics vendor are engaged to further assist with the incident.
- The forensics vendor recommends deploying advanced endpoint monitoring agents to all of your systems, even those that do not seem to be affected, while IT determines the state of your backup and recovery systems.

Fact Inject

- The IT Staff and forensic vendor continue to analyze the impacted systems. The endpoint monitoring detection starts identifying the existence of malware with credential harvesting capabilities.
- The privacy firm recommends possible engagement with the threat actor (via a third party company that specializes in ransom negotiations) for the decryptor tool in the event recovery from your backups is not possible.
- The privacy firm also contacts local law enforcement to determine if a decryptor tool is readily available for your ransomware variant.

Day 2

- The threat actors reveal a ransom demand for 20 bitcoins.
- Based upon public threat intelligence on this ransomware variant, the risk of data exfiltration and re-extortion is highly likely.
- Your IT staff confirms your encrypted data contains sensitive personal and protected information of former and current customers, and employees. Employee information includes names, full SSNs, driver's license numbers, direct deposit information, salary and bonus information.

Questions

- What is your organization’s position on paying a ransom demand?
- If backups are encrypted, does this impact your position on paying the ransom?
- If you decide to pay the ransom, how will your organization facilitate payment to the threat actors?

Sanctions List

- Payments to sanctioned individuals and/or entities can result in penalties.
- U.S. Department of Treasury's Office of Foreign Asset Control Advisory Sanctions List https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
- What will your organization do if your threat actors are on the Sanctions List?

Fact Inject

- The extortion demand was negotiated down to 14 bitcoin as the best and final offer. The threat actors give your organization 48 hours to make a payment.
- The FBI informs your organization that a decryptor tool is not readily available for the variant identified. They advise you should not pay the threat actors as it encourages future use of criminal behavior.

If your organization decides to pay the ransom demand, click here.

If your organization decides to not pay the ransom demand, click here.

Day 3

- After internal discussion and board approval, your organization decides to pay the extortion demand.
- Your insurance policy works on a reimbursement basis – your policy provides reimbursement for ransomware payments after you pay the demand.
- The ransomware negotiator company has access to cryptocurrency and will make payments on behalf of your organization only after receiving payment.
- How will your organization send payment to the firm?

Fact Inject

- The extortion demand was paid and your organization awaits further instruction from the threat actor.
- Your forensics investigator informs you of their initial findings. The threat actors had been in your system for the last 6 weeks after a successful employee phishing campaign. The investigation also identified evidence of data exfiltration.

Questions

- In the interim, the privacy firm and forensics vendor recommend all employees immediately change their passwords.
- How is this communicated to employees?
- Are you able to do a force reset password to all employees?
- Have you identified employees that are unable to change passwords immediately (i.e. temporary employees, employees on leave, etc.)?
- Does your organization have a password policy? What is your organization’s password policy?

Day 6

- After 48 hours, your organization receives a response from the threat actor.
- The threat actor confirms that all exfiltrated data was deleted with a list of data in .txt files and the decryption tool.

Day 10 - 19

- Your IT staff begins the decryption process. Your employees are brought online and are able to work in a limited capacity. Critical systems are slowly being brought back online.
- The data files exfiltrated contain data on 157 employees and financial information on 275 former and current customers.

Questions

- Due to the nature of the data files exfiltrated, is notification required to affected individuals?
- What legal and regulatory agencies need to be notified?
- Are there any deadlines you must follow?
- Are you required to notify the media or make a statement on your website?
- Do you need to provide credit monitoring to affected individuals?

Day 22 - 31

- The privacy firm along with your IRT begin to draft notices for affected individuals and applicable regulatory agencies.
- A notification and call center vendor are engaged to assist with address look up, printing, mailing, and running the call center.

Day 47

- Your organization begins to notify affected individuals within all applicable state breach notification laws.
- At this time, 87% of systems are back online and your entire employee base was able to change their passwords.

Debrief

- The Board, your IRT, and third party stakeholders hold a debrief to discuss the incident and next steps.
- How can this incident be prevented going forward? Is there an update to employee training protocols?
- What challenges did this scenario present?
- Does your organization need to make changes to your incident response plan?
- What could your organization have done better?

Day 3

- After internal discussion and board oversight, your organization decides **not** to pay the extortion demand and restore from backups.
- Your IT staff determines it will take a few weeks to fully restore the organization from its backups.
- Your forensics investigator informs you of their initial findings. The threat actors had been in your system for the last 6 weeks after a successfully employee phishing campaign. The investigation also identified evidence of data exfiltration.

Questions

- In the interim, the privacy firm and forensics vendor recommend all employees immediately change their passwords.
- How is this communicated to employees?
- Are you able to do a force reset password to all employees?
- Have you identified employees that are unable to change passwords immediately (i.e. temporary employees, employees on leave, etc.)?
- Does your organization have a password policy? What is your organization’s password policy?

Questions

- The data files exfiltrated contain data on 157 employees and financial information on 275 former and current customers.
- Due to the nature of the data files exfiltrated, is notification required to affected individuals?
- What legal and regulatory agencies need to be notified?
- Are there any deadlines you must follow?
- Are you required to notify the media/press?
- Do you need to provide credit monitoring to affected individuals?

Day 22 - 31

- The privacy firm along with your IRT begin to draft notices for affected individuals and applicable regulatory agencies.
- A notification and call center vendor are engaged to assist with address look up, printing, mailing, and running the call center.

Day 47

- Your organization begins to notify affected individuals within all applicable state breach notification laws.
- At this time, 87% of systems are back online and your entire employee base was able to change their passwords.

Debrief

- The Board, your IRT, and third party stakeholders hold a debrief to discuss the incident and next steps.
- How can this incident be prevented going forward? Is there an update to employee training protocols?
- What challenges did this scenario present?
- Does your organization need to make changes to your incident response plan?
- What could your organization have done better?

- The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.