
S-RM

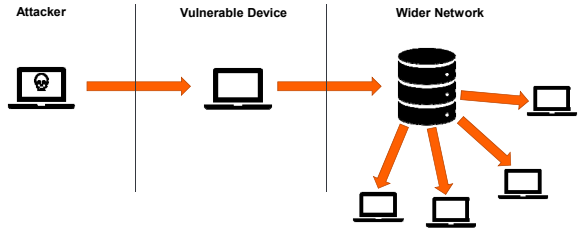
## WHAT IS RANSOMWARE?

- **A type of malware that locks access to systems or files and demands a ransom in order to regain access**
- **Modern versions are known as crypto-ransomware and lock systems by encrypting select files and demanding a ransom in exchange for the decryption key**
  - Comes in a variety of "strains", each with their own idiosyncrasies
- **Agenda:**
  - Ransomware demo
  - Recovery options
  - Ransom negotiation
  - IR Process & Forensic investigation

2

S-RM

## WHAT WE WILL DEMONSTRATE




3

S-RM

## THE ATTACK CHAIN


4

S-RM

## WHAT NEXT?

- Call for support
- Isolate the network
- Recovery options:
  - Backups
  - Pay the ransom
  - Full rebuild
- It's a ***cost benefit analysis***…

5

S-RM

## TO PAY OR NOT TO PAY

Whether to pay the ransom is a complex risk assessment, based first and foremost on **the value of the data**. You have to assess:

**Legal Risks**

**Ethical Risks**

**Other Considerations**

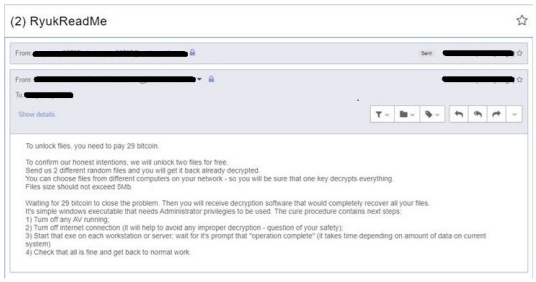
- Public relations impacts
- Insurance terms
- Sanctions

**At the end of the day it is a business decision…**

6

S-RM

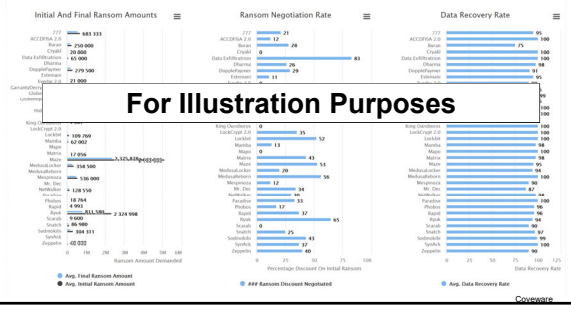
## THE RANSOM






S-RM

## NEGOTIATION






Coveware

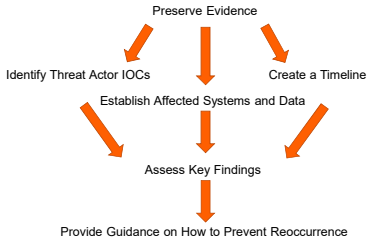
S-RM

## INCIDENT RESPONSE PROCESS

| Onboarding | Detection & Containment | Forensic Analysis | Negotiation & Recovery | Restoration | Data Mining |
|---|---|---|---|---|---|
| • Understand incident details and establish scope<br>• Provide immediate recommendations<br>• Establish communications protocol | • Deploy EDR and provide enhanced monitoring (24/7 if required)<br>• Perform threat intelligence sweeps across Dark & Deep Webs | • Collect and analyze forensic evidence<br>• Provide clients with continuous updates and material findings of the analysis | • Support clients in assessing and restoring backups<br>• Support clients end-to-end through the negotiation process<br>• Support clients in decrypting data | • Establish order of priority for the restoration of services<br>• Define secure restoration strategy and support clients in the restoration of systems and services | • Provide visibility on sensitive data exposure in mailboxes and files<br>• Reconcile and consolidate exposed data to assist in meeting notification obligations |

S-RM

## INVESTIGATION




10

S-RM

## HOW TO PREPARE

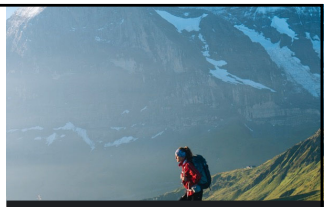
**Performed in succession, these tasks will increase your ransomware resiliency and overall cyber security maturity.**

- **Document your incident response plan**
- **Include a ransomware playbook in your response plan**
- **Exercise your response plan with a ransomware scenario**
- **Test your security controls for ransomware defense effectiveness**

11

S-RM

- 24/7 Hotline: +1 646 895 6538
- IR Mailbox: cyberIR@s-rminform.com



**FOR MORE INFORMATION:**

www.s-rminform.com

hello@s-rminform.com



CONNECT WITH US: LinkedIn Twitter