SURVIVING CYBER THREATS FOR BUSINESS, BRING A FRIEND!

PRESENTED BY MIKE WILLBURN

September 26, 2024

AGENDA

- Small and Medium Sized Business Common Risk Profile
- Case Study: Incident Response to Ransomware
- Summary
- Questions and Answers

COMMON RISK PROFILE: BY THE NUMBERS

- According to a CNBC survey, 56% of small business owners said they are not concerned about being the victim of a hack in the next 12 months
- 59% believe they can quickly resolve any cyberattack
- 87% of small businesses have sensitive customer data that could be compromised in an attack
- 28% have a cybersecurity incident response plan in place
- 51% of small businesses have no cybersecurity measures in place at all
- More than half of small businesses close their doors for good within six months of a cyber-attack

COMMON RISK PROFILE: TECHNOLOGIES

- Point of Sale (POS)
- Inventory Management Systems (IMS)
- Staff time tracking
- Accounting software or cloud service
- Productivity, communication, and user account management (e.g. Microsoft Office)
- Local or cloud data storage
- Customer Relationship Management (CRM)
- Content Management Systems (CMS)
- Social Media Marketing
- Computer Aided Design (CAD)
- Computer Aided Manufacturing (CAM)

COMMON RISK PROFILE: RANSOMWARE

- 82% of ransomware attacks are against companies with fewer than 1,00 employees
- 37% of companies hit by ransomware had fewer than 100 employees
- 55% of people in the U.S. would be less likely to continue doing business with companies that are breached
- 50% of SMBs report that it took 24 hours or longer to recover from an attack
- Cloudwards.net found that of all companies of any size that fell victim to ransomware, 32% pay the ransom but only get 65% of their data back

COMMON RISK PROFILE: THE CHALLENGE

- Cybersecurity is a business cost before and after an incident:
  - Staff salary and benefits
  - Technology
  - Ransom payments
  - Downtime
  - Equipment damage/replacement
- How can a small or medium sized business afford cybersecurity:
  - An incident could easily mean closing their doors permanently
  - They cannot compete with larger businesses for salary and benefits
  - Contract with smaller providers of security services, like an MSSP
  - Finding a comprehensive cybersecurity solution is still a challenge

CASE STUDY: THE ORGANIZATION

- Community not-for-profit organization

- Employees:
  - Five full time staff
  - 20-25 volunteers who all had limited access
  - Many of them had email accounts on the company's domain

- Cybersecurity Posture:
  - They had recognized the need prior to the incident and taken steps
  - Initial Configurations of Network systems had been done with security in mind
  - Staff cybersecurity training was required

CASE STUDY: THE INCIDENT

- One of the volunteers received an email, spoofing their supervisor's name and title
  - They then clicked on a malicious link in the message
  - Even though they had received training!
  - The attack was already past most of the defenses
  - No one is invulnerable
- The link immediately downloaded and ran an encryption program
- The malware then sent a message requiring payment to decrypt the files

CASE STUDY: SCREENSHOT

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]

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] *can decrypt your files*

Don't trust anyone except [redacted]

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

CASE STUDY: THE INCIDENT

- Resiliency is a key part of defense in depth
  - Backups and redundancy
  - Tabletop exercises
  - Rehearsals

- Training is always useful – training in depth
  - The user was alarmed but remembered the training
  - This included steps to take should an incident occur
  - The policy was to inform supervision as soon as possible
  - The supervisor called us, and we went into action

CASE STUDY:
ON THE LINE WITH INCIDENT RESPONSE

- Triage and response begin during the travel to the site:
  - Over the phone on we provided instructions to limit the spread of the incident including:
    - Disabling the network devices
    - Inform all staff to the situation and have them disconnect their devices
    - Checking the integrity of backups
  - We reviewed the latest results of vulnerability scanning using the Tenable® portal
- We logged into their O365 as a security administrator remotely - a role we assigned for just such a situation
- We began reviewing and tracing incoming and outgoing emails based on the malicious email's characteristics

CASE STUDY: ON SITE

- When we arrived on-site we established communications with the organization's operations manager

- We set up the Incident Response support laptops and wireless access point
  - The support laptops are predefined systems that receive the latest version of the organization's backups
  - They function as stand-in systems to get back to minimally acceptable operational conditions
  - They connect to a separate wireless access point to prevent lateral movement of attackers, bots, or malware

- This allowed the organization use the support laptops to resume productivity as soon as possible

CASE STUDY: INVESTIGATION

- We took the affected system into custody and removed the system's hard drive

- We cloned the hard drive and installed it in our sandboxed testing system to determine whether it was in fact ransomware and which type
  - Analysis identified the malware as "777"
    - 777 shares many similarities with ransomware-type malware such as Locky, Shade, MISCHA, Crypren, etc
    - Typically uses Cobalt Strike stagers to deploy the ransomware, conduct C2, and move laterally
  - A list of file names and other known characteristics of the malware and were derived
    - Encrypted Files are given a new file extension of "{original_file_name}.777"
    - A plain text file named "read_this_file.txt" is created in which additional instructions are included for the amount of the ransom and how to pay

CASE STUDY: REMEDIATION AND DECRYPTION

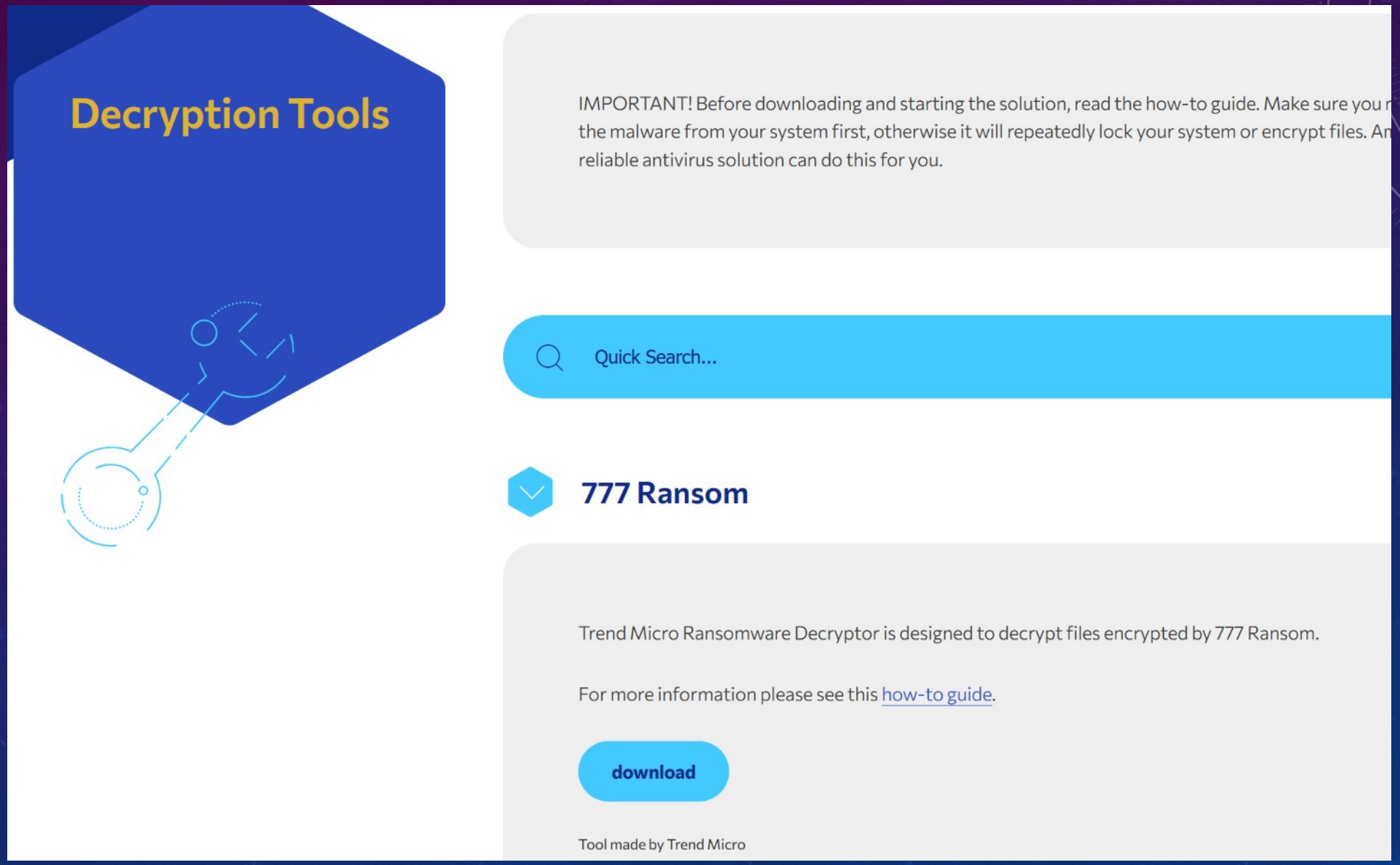
- Each of the operational systems were then scanned locally to identify and eradicate any associated files and processes

- Our MSSP partner, Trend Micro™, provides a tool to decrypt many types of ransomware
  - There is an open-source project at The No More Ransomware Project
  - Trend Micro™ provides many decryption keys for known forms of ransomware

- Using the tools, we recovered all files from the three systems that had locked or latent files as a result of the 777 ransomware

- We followed through and ensured that there were no further indications of compromise before returning the organization's environment back over to them at full functionality

CASE STUDY: SCREENSHOT



CASE STUDY: SUMMARY

- The total time our team took from arriving on-site to eradication and restoration of full operations was four hours
  - The organization only lost one hour between the time they disabled their wi-fi to the resumption of operations using the IR support laptops
  - This was well within their defined Recovery Time Objective (RTO)

- When all systems and operations were restored, the organization conducted an after-action review
  - They decided to increase their cybersecurity posture through additional network monitoring services
  - This established a dashboard for us to help the organization monitor activity on their network

Questions