Ransomware Incident Response Playbook

1.0 PREPARATION

1.1 Establish a Dedicated Incident Response Team (IRT): Roles & Responsibilities.

- **1.1.1** Incident Response Team Leader: Oversees the entire response process.
- **1.1.2** *Security Analyst*: Investigates the technical aspects of the compromise.
- 1.1.3 *Legal & Compliance*: Ensures adherence to regulations (e.g., GDPR, CCPA).
- **1.1.4** *Communications*: Manages internal and external communications.
- **1.1.5** *HR/Management*: Manages potential internal employee involvement.

2.0 STEPS

2.1 Log The Incident Immediately initiate an incident log. It is better to log and be wrong than to not have the incident being tracked from the beginning.

- **2.1.1** Go to forms in the Galactic Portal
- **2.1.2** Open the Security Incident Log form and add a new submission
- **2.1.3** Enter pertinent information within the form. You may also attach the audit logs. This is a good location to aggregate data about the incident so that you have all records in one place.
- **2.1.4** Update this form as necessary throughout the rest of the response process.
- **2.1.5** WARNING: When doing this, ensure that you are not using any devices that are potentially impacted by the ransomware event
- **2.1.6** Determine Impact Determine the impact and scope of the ransomware attack.

2.2 Engage IT Resources

- **2.2.1** Initiate procedure for informing team and IT vendors of a security incident
- **2.2.2** Reach out to the cybersecurity team to assist with next steps, including determining the scope of the infection

2.3 Determine the Scope of the Infection Analyze logs (server, firewall, workstation) and check for signs of encryption.

- 2.3.1 Look for incidents on: Mapped or shared drives
- **2.3.2** Up-to-date version at: https://portal.galacticscan.com
- **2.3.3** Analyze the information you have
- **2.3.4** Look at logs for each server and confirm if the attacker got in If available, review firewall logs; find out which computers were connecting to the beacon
- **2.3.5** Review workstation logs to determine which ones were impacted
- 2.3.6 Check logs and M365 DLP software for signs of data leaks
- 2.3.7 Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files
- 2.3.8 Look for malware, tools, and scripts which could have been used to look for and copy data
- 2.3.9 NOTE: One of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen

2.4 Determine Ransomware Strain Gather a sample executable and research based on characteristics
    2.4.1 Confirm the strain/type of ransomware (For example Ryuk, Dharma, SamSam, etc)
2.5 Disconnect Everything
    2.5.1 Disconnect any devices that are suspected or known to be infected. Turn off wireless functionality (WiFi, Bluetooth, NFC, etc.)
    2.5.2 Disconnect from the network
    2.5.3 Disconnect from VLANs
    2.5.4 Stop internet traffic to everything except the RMM (be careful here, you will want to have a tested process documented) Notify partners or vendors that are connected to the network that you are disconnecting everything from the network
    2.5.5 Log in to the hypervisor or Azure and disconnect network cards Disconnect from the internet during this process

3.0 COMMUNICATION

3.1 Communication Internally
    3.1.1 Refer to and activate the applicable internal procedure for notifying the appropriate internal resources (including a crisis team if applicable) of a ransomware event
    3.1.2 Determine other internal communications as needed to notify employees of the ongoing issue

4.0 ENGAGE RESPONSE TEAM

4.1 Determine the need for a third-party incident response team, forensics team, or ransom negotiator.
4.2 Response 1: If data or credentials are stolen determine if ransom should be paid to prevent data or credentials from being released by hackers
4.3 Response 2: If the ransom is not paid and backup restore is required locate backups and confirm all files are present
    4.3.1 Verify integrity of backups (i.e. media not reading or corrupted files)
    4.3.2 Check for shadow copies if possible (may not be an option on newer ransomware)
    4.3.3 Check for previous versions of files that may be stored in the cloud Remove the ransomware from your infected system
    4.3.4 Restore your files from backups
    4.3.5 Determine infection vector and address Confirm remediation
4.4 Response 3: Try to decrypt, if possible, determine the strain and version of the ransomware
    4.4.1 Locate a decryptor (there may not be one for newer strains)
    4.4.2 If decryptor is located: Attach storage media that contains encrypted files (hard drives, USB sticks, etc.)
    4.4.3 Decrypt files Determine the infection vector address Confirm remediation
4.5 Response 4: Do nothing (lose files)
    4.5.1 Remove the ransomware

4.5.2 Backup encrypted files for possible future decryption (optional)
4.5.3 Suggestion: Purchase new media, replace it, and reimage the devices Response

5.0 NEGOTIATE AND/OR PAY THE RANSOM

5.1 WARNING: Just because a ransom is paid does not mean data will be restored, If possible, attempt to negotiate a lower ransom and/or longer payment period
5.2 Determine acceptable payment methods for the strain of ransomware (Bitcoin, Cash Card, etc.)
5.3 Obtain payment (likely Bitcoin): Locate an exchange where you wish to purchase Bitcoin (time is of the essence) Set up account/wallet and purchase Bitcoin
5.4 Re-connect encrypted computer to the internet Install TOR browser (optional)
5.5 Determine Bitcoin payment address (this is either located on the ransomware screen or on a TOR site that has been set up for this specific ransom case)
5.6 Pay the ransom
5.6.1 transfer Bitcoin to the ransom wallet
5.6.2 Ensure all devices containing encrypted files are connected to your computer File decryption should begin within 24 hours, but often within just a few hours
5.6.3 Determine infection vector and handle PAYING THE RANSOM: If you have to pay the ransom, this is considered part of the containment steps.
5.6.4 DO NOT log in to check your backups from a domain-joined computer, or any computer that could have been infected (In one recent event, an IT Director checked his backups and watched as they were deleted one-byone because when he logged in he gave up the password to the backup device)
5.6.5 Just because you pay doesn't mean you aren't going to have to pay more.
5.6.6 Make sure to communicate that 40% of the time ransomware attackers are now asking for more money before providing the data.
5.6.7 Finally, attackers know you've been investing in better backups, and they are happy to contact all of the clients of the company that were attacked to tell them about the ransomware event. If you have to pay the ransom, start the restore process as soon as you can.
5.6.8 WARNING: Do not wait to complete the next steps. Restoring from ransomware attacks should be thought of as part of the containment phase.

6.0 **INSURANCE ENGAGEMENT**

6.1 Based on the impact of the event, determine the necessity of involving the insurance company.
6.2 Consider the following timeline as part of the insurance team engagement evaluation:
6.2.1 Engage forensics team – 1 business day
6.2.2 Forensics evaluation – 3 to 5 business days
6.2.3 Ransomware negotiation – 2 business days If insurance engagement is required, contact the insurance agent. Be prepared with all of the data that has been recorded up to this point, including the time of the event, attack vector, and remediation status.

6.2.4 NOTE: Do not start the claim process until the size of the breach has been determined and further threat action has been stopped.

7.0 **RECOVERY**

7.1 Remember to make the move from containment to recovery cautiously. It is critical that you stop the spread before you start cleaning it up. Why? If you don't fully identify all of the infected machines before pushing forward, the attackers will continue lateral spread you will be back to identifying what they accessed.

7.2 Upgrading

7.2.1 Before we start with eradication, consider the long-term strategy for the network. Is now the time to consider any network upgrades? Ransomware events are expensive, and you are going to be rebuilding. Don't rebuild without a solid foundation. Are there any major changes that should happen to the network while going through the rebuilding process?

7.3 Create a Clean Network

7.3.1 Stand up a new authentication source (Active Directory / AAD)

7.3.1.1 start by standing up a clean network…no one gets to join this network unless they are clean

7.3.1.2 Use a brand-new firewall for this network

7.3.1.3 Ensure the firewall is configured with antivirus, SSL DPI, and IPS/IDS Ensure the network is on a separate VLAN (if you don't have the capability of setting up VLANs, there are several inexpensive switches out there that can do this. Buy one and get it delivered to the affected site.)

7.3.1.4 Identify your shopping list items: Consider having a shopping list ready to go. It is going to take you a day to get through the first couple of steps, so by the time you are ready to go with eradication you can have the equipment in hand.

7.3.1.5 If you have viable backups, restore a domain controller from an uninfected state.

7.3.1.6 If you do not have viable backups OR you are concerned that you do not know, start building a new domain.

7.4 Stand Up Servers

7.4.1 Rebuild and transfer data from backups or restore them. You can turn them on in the staging network.

7.4.2 Validate the logs data out

7.4.2.1 WARNING: Do not move it to the new server yet. First, it is best to get your new environment up completely. Then start connecting clean devices. These are devices that were either not impacted or were replaced.

7.4.3 Remember when replacing devices, you will want to preserve the logs for 13 months. The easiest way to do this is to pull the drive and put a new one in. Then reimage the drive you put in.

7.5 Make sure your antivirus is working

7.6 Run a Galactic Scan in the environment to make sure you didn't forget IoT Devices

7.7 REMINDER: when you are building your new network it is the perfect time to put IoT devices on a separate network. Configure IPS / IDS between IoT devices and the rest of the computers

7.8 Transfer Data

- 7.8.1 Put data in place on the new network.
- 7.8.2 Copy data to the new network.
- 7.8.3 Work through any database corruption at this point.
- 7.8.4 NOTE: You may have to go back to the transaction logs from the servers
- 7.8.5 Run manual antivirus scans
- 7.8.6 Monitor the logs and firewalls closely for any further indicators of compromise Do not log in to any management devices from computers that users have access to

8.0 **REVIEW**

8.1 Determine what should be improved for next time.

8.2 Document answers.

- 8.2.1 How did this happen?
- 8.2.2 How could the event have been identified faster?
- 8.2.3 What was the overall impact on an organization?
- 8.2.4 How can the possibility of doing this again be minimized?
- 8.2.5 What can be done in the future to improve the response?

8.3 REMINDER: Talk in terms of systems and technology rather than people. The goal here is not to assign blame.

8.4 Update checklists, processes, and documentation

8.5 Update the incident response form