An Example of a Destructive Malware Event Recovery Scenario

This section presents a scenario that uses the guidelines provided in earlier sections of this document to effectively recover from a cyber event and subsequently use information gained during the recovery process to improve its cybersecurity processes. The scenario is fictional and not meant to be all inclusive or exhaustive of cyber events, but to provide a means to demonstrate how to apply the document's recommendations and utilize the ransomware playbook to recover from a destructive malware attack.

Cyber-attacks have continued to evolve, with many now focused on monetary gain. One recent evolution has emerged in the form of ransomware [15]. Ransomware is a type of malicious attack where the attackers encrypt the organization's critical data, such as personal data or business data, after they have infiltrated the systems, then demand a monetary payment in digital cash formats, such as bitcoin [16]. The data is inaccessible by the organization, so it disrupts the business workflow and prevents the users and organization from performing their business functions. If the organization or individuals do not pay the attackers, then the data remains encrypted or is deleted. The malware may also discover other systems and data stores to spread to and take additional hostages to repeat the same process.

This scenario describes an organization that has experienced one of these ransomware attacks on its network. The event was discovered when users saw pop-up messages that their data had been encrypted and the only way to regain access is to pay a fee to the attacker. While the method of entry and the specific type of ransomware are not directly relevant to the recovery team, it is important to note that such a breach could compromise the availability of the business unit and IT management systems if the ransomware spreads. The organization has adopted the policy of not paying ransoms, due to concerns of proliferating the criminal business model and a concern that the attackers would not provide the decryption keys after payment.

For this scenario, system monitoring tools confirm that a significant percentage of end user systems have been encrypted by the ransomware. Additionally, there is the possibility that the ransomware could spread to other systems.

7.1 Pre-Conditions Required for Effective Recovery

The organization understood the need to be prepared and conducted planning to operate in a diminished condition. The ransomware playbook includes the following critical elements:

- A description of a set of formal recovery processes to use if the organization experiences a ransomware attack.
- A list of the critical people, facilities, technical components, and external services that are required to achieve the organization's mission(s). The playbook enumerates the ransomware recovery team personnel, including system administrators, desktop support, backup administrators, managers, general counsel, and public relations personnel as required.
- A current set of functional and security dependency maps that helps to explain the order of restoration priority. These maps should include control, business function, and user systems, with specific attention to systems that store data backups.
- Metrics and other factors used to effectively plan for restoration priority may include:
    - Legal costs;
    - Hardware, software, and labor costs;

- Amount of lost revenue due to business downtime to include loss of existing and future business opportunities;
- Instantiation of new services to restore customers’ trust;
- Accuracy of the dependencies maps;
- Gaps identified in the playbook;
- Internal users, external business partners, and customers satisfaction;
- Service level agreements with internal business teams;
- Confidence level around quality of the backups; and
- Quality of the overall recovery plan and process used to develop the ransomware attack playbook.

- Metrics needed to effectively plan for restoration priority include: legal, hardware, software, and labor costs; business downtime resulted in lost productivity; loss of existing business and future business opportunities; instantiation of new services to restore customers’ trust; accuracy of the dependencies maps; gaps identified in the playbook; internal users and external business partners and customer satisfaction; service level agreement with internal business teams; quality of the backups; and quality of the overall recovery plan and process used to develop the data breach playbook.
- A list backup and restoration tools that have been authorized after being tested in the exercises.
- A comprehensive recovery communications plan with fully integrated internal and external communications considerations. Internal communications will be between members of the recovery team and management for recovery activity and status updates, while external communications will include information sharing criteria informed by recommendations in NIST SP 800-150 [11]. It includes specific elements that are included in the content to communicate with the management team including the board, the general counsel, public relations, law enforcement organizations, the IT team, the employees, and external service providers.
- Results and lessons learned from periodic trainings and exercises that have occurred to validate successful system restoration capabilities and to ensure timely recovery team coordination.

Because the organization has formally implemented cyber event recovery exercises and tests with realistic scenarios and clear roles and responsibilities, the organization is prepared to tackle the recovery task with limited assistance from external entities.

7.2 Tactical Recovery Phase

The following steps summarize the activities of the recovery team in the tactical recovery phase. The ransomware playbook is utilized in order to aid in the effective recovery throughout this phase.

7.2.1 Initiation

- It was determined that only user systems were affected and that network-based communications are still trusted. The team agrees to communicate with a combination of in-person meetings, telephone conversations, and email.

- The incident response team works collaboratively with the recovery team to confirm that the adversary's motivation is monetary. The incident response team informs the recovery team that the ransomware attack has only affected a number of end user systems, shares indicators of compromise for the ransomware, and provides specific remediation steps that will be performed as part of the recovery playbook used in this cyber event. This will include procedures for identifying the malware, safely cleaning the system, and strengthening the system and user account posture. The collaborative teams determine that the ransomware attack has not yet affected key assets.

- Knowing that ransomware can spread through an organization and infect backup systems, the recovery team needs to verify their backups have not been encrypted. The team begins a comprehensive inventory and integrity check of all backups to include all backup systems and processes. They identify and map all backup storage devices and enumerate the backup points available for restoration.

- The recovery team has identified the systems that have been infected by the adversary's ransomware campaign and customize the ransomware playbook accordingly in order to isolate them from the rest of the organization's systems. The IR team has collected forensics data and artifacts.

- Based upon the criteria in the ransomware recovery playbook, the defined personnel determine that the recovery process is ready to begin because all members of the team have a good understanding of the situation. All people with responsibilities for recovering from a ransomware attack as defined in the pre-conditions are informed that the recovery activities have been initiated.

- The recovery team sets a goal for recovery measured by percentage of affected systems restored in time increments of 12 hours. These metrics are recorded and tracked by the responsible parties until the recovery is terminated.

7.2.2 Execution

- The recovery team executes the modified ransomware recovery playbook for this particular event. System restoration is tracked to understand the time it takes for 100 percent of affected systems to be recovered.

- In coordination with the incident response team, the recovery playbook is updated to include the time of infection, so that the corresponding backups can be identified and checked for data integrity.

- In order to minimize the likelihood that the ransomware continues to spread throughout the organization, the infected machines are contained to a different network in a coordinated effort to not alarm the attackers during the eradication process and before the recovery process starts. The recovery team begins to restore user systems from the identified backups that have been checked and passed acceptance criteria identified in the playbook.

□ The recovery team continues restoration by validating and implementing remediation countermeasures in coordination with the incident response team and other information security personnel to ensure that the underlying system weaknesses are not re-introduced.

• The organization continues to execute its recovery plan, preparing its communication strategy in accordance with the pre-existing communications criteria and in coordination with the legal and public affairs offices regarding the restoration status, as well as the appropriate law enforcement offices.

• During restoration, the recovery team tracks the user systems that were unusable compared with the agreed-upon service levels and recovery times. The team tracks the recovery progress by comparing current metrics with metrics gathered at the beginning of the event. As an example, the percentage of users or systems were back online within 24 hours. Based on the volume of impacted systems and resources available to return the systems and associated data to their original state, the recovery team may provide the impacted users access to alternate systems that have the minimum set of capabilities to allow them to perform their daily functions. This allows the organization to continue to operate with diminished capabilities while full restoration is being performed.

• Designated staff document any issues that arise, and newly identified dependencies, to help expand on documentation later in the recovery process or immediately after recovery is achieved. Indicators of compromise are continuously captured, updated, and documented. Restoration techniques, tools, and procedures are customized and refined for the current cyber event.

• While the user systems are being restored, other members of the recovery team work with business unit managers and senior leadership, in coordination with representatives from HR and legal, to discuss appropriate notification activities. Using the pre-agreed recovery communications plan, the team drafts notices for the appropriate parties. As a critical component of this step, additional surge support has been added to the organization's support center and employees are kept abreast of the status of recovery, sharing status accurately while abiding by the pre-agreed decisions regarding what information may be shared with whom, and when.

• The recovery team asks the organization's security personnel, the incident response team, and external subject matter experts to confirm that the newly restored systems are free from the indicators of compromise and are ready to be returned to service. The team validates the restored assets are fully functional and meet the security posture required by the security team before it receives approval to re-introduce the systems back to normal operation.

7.2.3 Termination

• The personnel determine that the ransomware no longer persists in the organization, the attack vector that the ransomware exploited has been remediated, and all of the affected user systems have been restored. The personnel declare the end of the tactical recovery event.

• The team stands down and staff returns to executing their normal job functions.

• The organization continues to monitor the infrastructure and user systems for potential persistency of ransomware indicators and continue to inform the incident response and recovery team. The goal is to make sure the organization has fully eradicated the ransomware from the infrastructure and has exclusive control of the operational environment.

- The recovery team finalizes the metrics collected and lessons learned during the event.

7.3 Strategic Recovery Phase

The following steps summarize the activities performed during the strategic recovery phase.

7.3.1 Planning and Execution

- The recovery continues to support the internal communication teams as they interact within the internal users.

- The recovery teams close the loop with the external entities, such as law enforcement, who have been involved during the tactical phase.

- A plan is developed to include longer-term goals to fully remediate the ransomware and other classes of ransomware. These actions will involve vetting and approval from the management, business units, and IT teams, as they will include changes in the business workflows, personnel training, IT architecture, and operation of the backup systems. This plan includes improving the organization's backup policies and infrastructure by enforcing a regimented backup schedule for all users, including a comprehensive backup infrastructure that provides redundant copies of backups in different physical and offline locations. Deploying application whitelisting technology and implementing container or virtual isolated environment to execute Internet-exposed general purpose client applications such as web, email, and productivity applications will help protect the endpoints from software-based attacks in addition to the traditional countermeasures such as running anti-malware software and patching systems. Adding web and email filtering solutions and intrusion prevention systems help mitigate known common attacks across the organization network. IT security policies and processes will be modified to include regular awareness and training campaigns to ensure employees are aware of phishing attacks that may contain a ransomware payload.

- The IT team, with assistance from the recovery team, will start the execution and implementation of the long-term improvement plan once the changes to the architecture and enhanced capabilities have been approved and funded by the organization.

7.3.2 Metrics

- Upon formal completion of the event, the recovery team meets for an after-action review. During that meeting, members of the recovery team discuss the metric of percentage of systems restored over time.

- The debriefing reviews the efficacy key milestones that were developed in planning activities, including those that identified interim recovery goals, to share with the team. The team reviewed other relevant metrics regarding assumptions made, recovery objective performance, and stakeholder communications achievement.

7.3.3 Recovery Plan Improvement

- Comparison of the performance of the team during the recovery against the estimated performance defined in the plans enables the organization planners to consider what adjustments should be made to the plans. For example, adding additional staff to support restoring systems from backups. The organization must continue to be prepared in case there is a recurrence of the issues.

- These post-recovery steps help to continually improve cyber event recovery plans, policies, and procedures by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves.