Ransomware Playbook

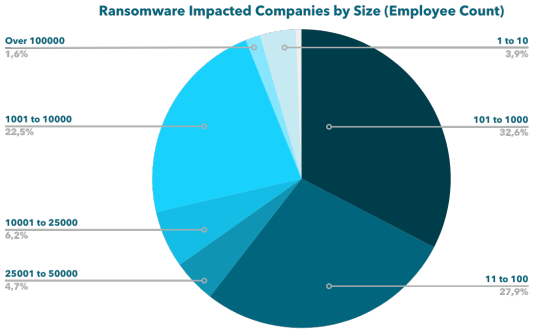
Building your Cyber Resilience

Written by Thomas Dejagere - Senior Cybersecurity Consultant - Toreon

Introduction

In the dynamic landscape of cybersecurity, organizations face an ever-growing threat from malicious actors employing sophisticated techniques to compromise data integrity and operational continuity. A recent study of Van Breda stated that 50% of Belgian companies encountered a cyberattack. One of the most pervasive and damaging forms of cyberattacks is ransomware, which not only encrypts critical data but also demands a ransom for its release. The calculation of these ransoms predominantly hinges on the revenue of the targeted organization. Typically, the average ransom amounts to 1.5% of the company's global revenue.

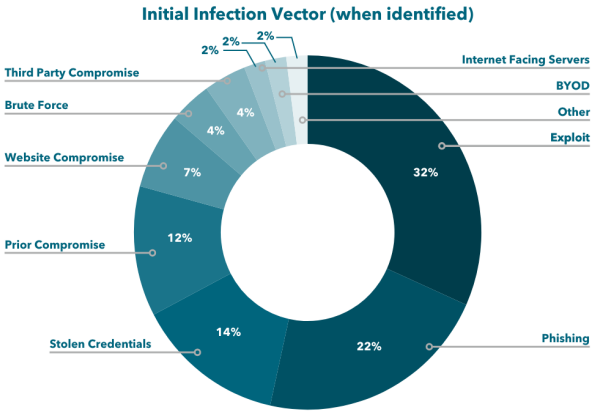
Many companies, often equipped with robust backup facilities, opt against ransom payment. Regrettably, cybercriminals have adjusted to this trend by engaging in data exfiltration of potentially sensitive information. When a victim organization rejects payment, these cybercriminals typically resort to threatening the public disclosure of sensitive information, leading to reputational harm. Adding to the peril, some cybercriminals may even launch Distributed Denial of Service attacks, disrupting operational IT systems that are still functioning, further intensifying the pressure.



Coveware blog New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying

Cybercriminals don't solely target large corporations to optimize their profits. Larger corporations often employ more robust security measures, making the return on investment (ROI) less predictable and potentially less lucrative for cybercriminals. Consequently, these malicious actors diversify their targets, seeking to maximize the ROI of their cyberattacks by targeting a broader range of entities. This strategic approach allows cybercriminals to exploit vulnerabilities across different sectors, increasing the overall effectiveness of their illicit activities.

M-Trends 2023 Mandiant Special Report



M-Trends 2023 Mandiant Special Report

Introducing the Ransomware Playbook

To fortify defenses and respond effectively to ransomware incidents, it is imperative for organizations to have a comprehensive and well-structured Ransomware Playbook. Unfortunately, there is no one-size-fits-all solution to protect against ransomware attacks. These attacks can originate from multiple entry points, emphasizing the importance of implementing a defense-in-depth strategy for robust and comprehensive cybersecurity.

The Ransomware Playbook functions as a comprehensive and adaptable guide, offering both proactive and reactive strategies for addressing ransomware threats. It incorporates guidance for preventing and preparing against ransomware attacks. Following the ransomware lifecycle, which includes stages such as detection, containment, eradication, recovery, and lessons learned, the playbook aims to minimize the impact of an attack. By following this structured approach, organizations can ensure swift and well-informed decision-making during critical moments.

From understanding the evolving threat landscape to implementing robust security measures, this playbook aims to equip organizations with the knowledge and tools necessary to thwart ransomware attacks or efficiently recover from them. By fostering a culture of cybersecurity awareness, establishing incident response processes, and leveraging cutting-edge technologies, organizations can not only defend against ransomware but also strengthen their overall cyber resilience.

As we delve into this playbook, it is essential to recognize that combating ransomware requires a multifaceted approach that integrates technology, training, and collaboration across all levels of an organization. By adhering to the guidelines presented herein, organizations can bolster their cybersecurity posture and significantly reduce the risk and impact of ransomware incidents.

The playbook is designed with a structured framework that identifies specific junctures to implement cybersecurity measures, fostering the development of a resilient ransomware strategy. Each section is dedicated to addressing unique phases, providing a strategic roadmap for enhancing defenses and ensuring effective responses throughout various stages of a potential ransomware incident.

Prevention

Before going into depth on how to handle a ransomware attack, it's imperative to ensure that the required controls to prevent a ransomware attack have been implemented. It's crucial to recognize that the cybersecurity measures listed below provide a general guidance for enhancing digital defenses. However, cybersecurity is not a one-size-fits-all endeavor. Each organization possesses a unique set of risks, challenges, and processes that demand a tailored approach to security. But, it's important to note that risks within a sector are often comparable, highlighting the significance of leveraging a cybersecurity partner with specialized sector knowledge. Customization with sector knowledge is the key to robust protection.

Secure Configuration

- Ensure all on-premises, cloud services, mobile, and personal (BYOD) devices are properly configured and security features are enabled. (1)

Account and Access Management

- Implement MFA for externally-exposed applications, remote network access, administrative access. (2)
- Implement a password manager (3)
- Implement least privilege (4)
- Implement least privilege for third parties (5)

Vulnerability Management

- Implement vulnerability management and scanning (6)
- Regularly (automated) patch and update software and operating systems to the latest available versions. (7)

Email and Web Browser Protections

- Implement an anti-phishing filter at the email gateway on domain, URL and IP level (8)
- Implement email security best practices (9) Such as SPF, DKIM, DMARC, disabled macro scripts, attachment filters,…
- Consider browser sandboxing. (10)
- Implement protective DNS services or web filter (19)

Malware Defenses

- Implement an Endpoint Detection and Response solution. (11)

Data Recovery

- Maintain offline, immutable, encrypted backups of critical data/infrastructure and test these regularly (12)

Network Infrastructure Management

- Implement a zero trust architecture (13)
- Limit your exposure (14)
  Don't expose servers, services to the internet if it isn't required.
- Implement network segmentation (15)

Network Monitoring and Defense

- Implement an Intrusion Detection System (IDS) to detect command and control activity and other potentially malicious network activity from inside and outside the network. (16)

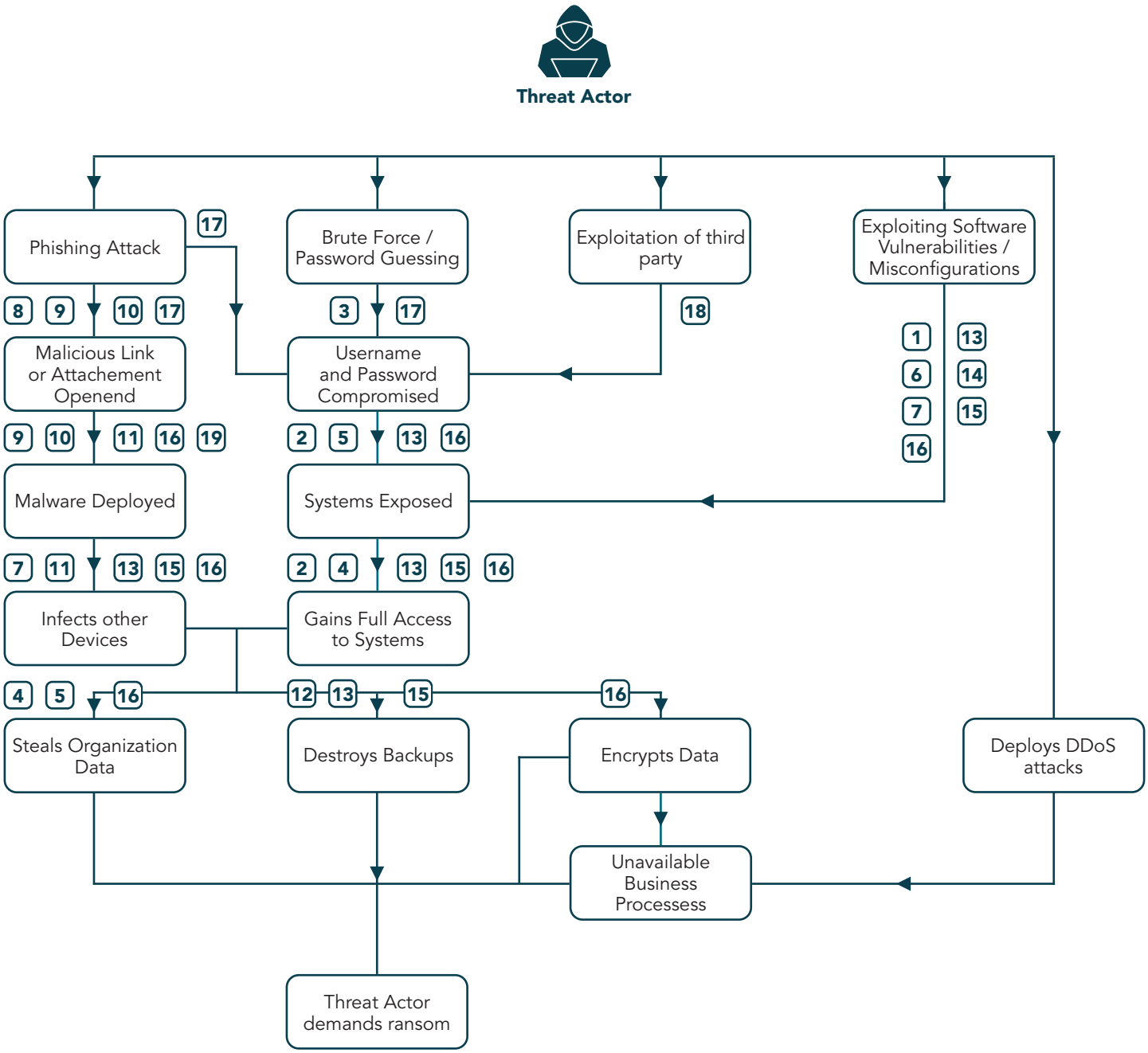
Security Awareness and Skills Training

- Implement a cybersecurity user awareness and training program (17)

Service Provider Management

- Implement Supply Chain Risk Management (18)

Impact of implementing preventative controls on ransomware attack vectors



Preparation

The question isn't '**if we are going to get hacked**' the question is '**when are we going to get hacked**'. When this happens, you want to be prepared and have a clear plan and vision on how to tackle the situation. A cybersecurity hack tends to be very stressful. By having a clear plan you take away parts of that stress to achieve effective and efficient security incident handling

Security Incident Response Partner

Who are you going to call when cybersecurity crisis strikes and you have no clue what's what? Battling against cybercriminals during a ransomware attack requires coordination, efficiency and, most importantly, competence. Cybersecurity incident response is a sport on its own which takes years of practice and learning to master. It is highly recommended to outsource these capabilities to skilled professionals.

Cybersecurity Insurance

Financial impact of a ransomware attack can't be ignored. An insurance can be of help in this situation. A cybersecurity insurance defends an organization not only against ransomware but also other kinds of cybersecurity incidents such as phishing, blackmail, data breaches, viruses, GDPR fines and expensive assistance.

A cybersecurity insurer can help in many aspects of a ransomware attack. They can provide assistance in crisis management, legal assistance and PR assistance. A negotiator can be introduced when needed to negotiate with cyber criminals about the demanded ransom, if required.

Insurers naturally aim to minimize the likelihood of making payouts. This explains the often high premiums or the refusal to provide insurance if the existing security measures within an organization are deemed insufficient. Hence, emphasizing the prevention phase becomes crucial to enhance the security posture, ultimately resulting in reduced premiums.

Ethical decision on paying the ransom

There might come a situation where critical data is encrypted which endangers the further existence of your organization. In that case you might consider paying the ransom to retrieve the critical data and continue your business processes. Cybercriminals have intensified their ransomware tactics in recent years, not only encrypting data, but also stealing it. Refusal to pay the ransom could lead to threats of releasing stolen data, resulting in reputational damage, lawsuits from customers, non-compliance of laws and regulations (such as the GDPR, which might result in fines). If that doesn't convince you paying the ransom, cybercriminals might escalate attack on unaffected services with attack types such as launching a DDoS attack, to maintain pressure until the ransom payment is made.

However, cybersecurity professionals advocate against ransom payment for several reasons:

- There is no assurance of receiving the decryption key.
- Payment doesn't address the root cause of the breach.
- Cybercriminals might have installed backdoors for future exploitation.
- Payment paints a target on your organization within the cybercriminal community.
- With proper preventive measures, ransom payment shouldn't become the sole resource, even in the event of a ransomware infection.

If preventive measures aren't fully implemented or failed to stop the attack, you may be inclined to consider paying the ransom. In such a scenario, it's advisable to consider the following factors:

- Engage a professional ransomware negotiator to guide you through the process.
- Ensure that the negotiator verifies the theft of confidential data from your servers by requesting samples of the data from the cybercriminals.

As an organization, it's essential to carefully consider this ethical dilemma before encountering such an incident. Opting not to pay the ransom under any circumstances should lead to the decision to implement the appropriate countermeasure outlined in the 'Prevention' phase.

Define and implement an Incident Response Plan

Creating an incident response plan wel upfront is crucial for organizations to effectively navigate and mitigate the impact of cybersecurity incidents. Such a plan provides a structured framework for timely detection, containment, eradication, and recovery from security breaches. By outlining specific roles, responsibilities, and procedures, an incident response plan enhances your organization's readiness, reduces response times, and minimizes potential financial and reputational damage associated with cyber threats. Ultimately, it is a proactive measure that bolsters overall cybersecurity resilience.

It's advised to get professional assistance when making this incident response plan. In-depth knowledge of evolving threats, industry best practices, and regulatory requirements are required to draft an incident response plan that is tailored to the specific needs and risks of your organization. The incident response plan should be regularly tested in various setups, like a table-top exercise.

Define and test a Business Continuity and Disaster Recovery Plan

While an incident response plan is specific to cybersecurity incidents and focuses on the rapid response to mitigate damage, a Business Continuity and Disaster Recovery Plan takes a more comprehensive approach, addressing a variety of potential disruptions to ensure your organization's critical business processes' continuity and recovery across various scenarios. Both plans are essential components in the implementation of cyber resilience.

This comprehensive plan ensures your organization's ability to maintain essential operations during and after a disaster, minimizing downtime and financial losses. It's advised to get professional assistance in making this Business Continuity and Disaster Recovery Plan. You should at least make a plan with the scenario of a ransomware infection in your organization.

Roles and responsibilities should be documented in the Incident Response Plan and BC/DRP

A key aspect of both the Incident Response Plan and the Business Continuity and Disaster Recovery Plan is the definition and communication of roles and responsibilities. A ransomware attack doesn't only involve IT staff, but at least also management, finance, legal and communications. The expectations, tasks, responsibilities and mandates should be talked through and documented before a cybersecurity incident occurs.

Log retention

A vital aspect in the identification, analysis , containment and eradication of a ransomware attack is the availability of logs. We see that most of the times log retention of vital services is too limited to be of use during a ransomware incident. It's important to know that most of the time the cyber criminals are already active on your network for months before they activate the ransomware virus. If your log retention is e.g. only one month you might never know how they breached the organization's cybersecurity measures. It's advised to set the log retention period for significant and critical services to at least 6 months.

Necessary detection capabilities

Detecting anomalies can be useful in preventing actual encryption for ransom. This can be done on several levels, starting with the endpoints, on network level, server and storage infrastructure monitoring or with log correlations on all levels. There are several products on the market that can help to detect ransomware at an early stage or to the point where it just started to encrypt data with an automated response to shut it down before it can encrypt all data.

NextGen EDR (End-Point Detection and Response) solutions can be used to detect user-based behavior anomalies on endpoints. Where it can detect reconnaissance, privilege escalation and at last stage mass change of data. NDR solutions can detect anomalies via analyses of network traffic over a longer time period where it can detect "call-home" traffic for C&C infections. Identity firewalls are able to detect and stop unusual use of user or service accounts. Finally, SIEM/SOAR or other log correlation tools can be used to analyze input from all relevant systems to detect, warn or isolate threats before they become a problem.

Identification and analysis

In the identification and analysis phase, ransomware gets detected and presence confirmed by intrusion detection and behavioral monitoring. Assess the extent of the compromise, identify the ransomware variant, and determine the entry point and tactics used by threat actors. This phase provides essential insights for developing a targeted response and recovery strategy.

1. Identify Infection

- Check for unavailable or corrupt files
- Check for ransom messages
- Check for text or HTML files on the desktop / home or root folder

2. **Disconnect** infected devices from the network, don't turn them off for evidence purposes.

3. Check for known solutions*

- Get ransomware note and two encrypted files
- Go to 'No Ransom Project' and fill in the necessary information.
- Go to 'ID Ransomware' and fill in the necessary

4. Communicate to stakeholders

- Organization management / crisis group
- Internal Incident Response Team
- External Incident Response Team
- Cybersecurity insurance
- CSIRT / Police

5. Determine delivery method

- Exploitation of vulnerability or misconfiguration
- Compromised account
- Phishing
- Initial malware infection
- Social engineering
- Third parties (e.g. supplier with network access)

6. Gather detailed evidence

Run the ransomware in a sandboxed environment logging all incoming and outgoing connections. By doing so, try to determine the chain of events.

Document al Indicators of Compromise in to identify other infected devices.

7. Identify other infected devices

Given the identified delivery method an analysis can be done to determine which devices might be impacted by the ransomware attack.

8. Identify of lateral movement

- Check open network connections on the infected system
- Identify connections with ESTABLISHED state
- Identify known ports for lateral movement like NetBios, SSH, SMB, RDP or FTP
- Use AD event logs on the infected

9. Containment and eradication phase

* TIP: Researchers are constantly analyzing known ransomware in an attempt to break the encryption. By doing so the encrypted files can be recovered without paying the ransom. These methods are centralized in websites such as 'No Ransom Project' and ID Ransomware

Containment and Eradication

In the Containment phase, the primary goal is to prevent the further spread and impact of the ransomware. Cybersecurity teams isolate affected systems, disconnect compromised devices from the network, and implement access controls to limit lateral movement. These measures are crucial for minimizing the ransomware's reach while maintaining essential business operations.

1. Disconnect all infected devices identified in identification & analysis phase

- If several systems or subnets appear impacted, take the network offline at switch level. It may not be feasible to disconnect individual systems during an incident.
- For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigations.
- Shut down the devices if it is not possible to temporarily shut down the network or disconnect affected hosts from the network.

2. Gather evidence

Take a system image and memory capture of a sample of affected devices.

3. Backup encrypted files of critical systems

A solution might be found to crack the ransomware encryption resulting in potentially recovering the files.

4. Research trusted guidance (e.g. No Ransom Project and ID Ransomware) for the particular ransomware variant and follow anv additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

5. Block all traffic related to the ransomware

- Emails, URLs, domains, IP addresses,…
- Command and Control traffic

6. Perform threat hunting activities to determine the impact or points of entry

7. Run EDR/XDR tools to detect other potential malicious activity on the network and/or endpoints.

8. Disable all user accounts involved in the infected devices.

9. Mitigate the vulnerability or point of entry discovered in the detect phase of the playbook.

10. Communicate to the employees a ransomware infection is happening in the organization.

Give them the instructions if they see a ransom note or other identification parameters to disconnect the device and contact IT support.

Recovery

During the Recovery phase, cybersecurity teams work on restoring affected systems and data to normal operations. This includes leveraging backups to recover essential files and configurations. Teams verify the integrity of the restored data to ensure it is free from compromise. The goal is to minimize downtime and restore business continuity after a ransomware attack.

1. **Prioritize critical systems for restoration on a clean network following the Business Continuity and Disaster Recovery Plan.**

   If a new VLAN has been created for recovery purposes, ensure only clean systems are added.

2. **Re-image or restore** from backup following the backup policy. Ensure that the backups aren't compromised.

3. **Change passwords** from the blocked accounts, implement MFA (if not already implemented), and monitor the activity on these accounts.

4. **Recover** encrypted files using a decrypter (if available).

Lessons learned

In the Lessons Learned phase, cybersecurity teams conduct a comprehensive analysis of the incident response. This involves evaluating the effectiveness of containment, eradication, and recovery strategies, identifying areas for improvement, and refining incident response plans. The insights gained during this phase inform future incident prevention measures, ensuring the organization is better prepared to defend against and mitigate the impact of potential future ransomware attacks.

1. **A ransomware playbook** is useless unless it is practiced and up to date.

2. **Document** the root cause and what measures have been implemented.

3. **Review and document** the process followed to detect, mitigate and recover from the cybersecurity incident. Adjust policies and procedures where required.

4. **Consider sharing** lessons learned and relevant indicators of compromise with the industry.

Summary

Your organization faces a persistent threat from ransomware, which can wreak havoc on your operations by disrupting product and service delivery. The consequences may include financial losses, data breaches, and damage to your reputation. Taking proactive steps to safeguard your network, connected devices, and information is crucial for effectively responding to and recovering from ransomware incidents.

Implementing the identified gaps outlined in this ransomware playbook is crucial for strengthening your security posture. However, you don't have to tackle this task alone. It is advisable to collaborate with a cybersecurity partner possessing specific sector knowledge to offer tailored guidance and support in effectively addressing the ransomware challenge.

When selecting a cybersecurity partner, it's essential to consider the following criteria:

- Expertise and experience in cybersecurity for your specific sector.
- Ability to provide comprehensive maturity assessments tailored to your business.
- Be vigilant for 'do-it-all's, cybersecurity is a specialized field. Instead, seek out a cybersecurity partner with a diverse ecosystem each with their own specializations, such as incident response.
- Encompasses the entire cybersecurity journey, extending beyond just creating roadmaps and offering advice.
- In the intended field of knowledge, there is sufficient critical mass to prevent capacity issues in the event of any incidents.
- A cybersecurity partner fluent in risk management, customized to the business context, is vital for ensuring business enablement and intelligent decision-making.

Written by Thomas Dejagere - Senior Cybersecurity Consultant - Toreon