deepwatch™

5 Phases of Coordinated Incident Response to Ransomware

Prepare and adapt your security program to address future threats.

www.deepwatch.com

Introduction

How quickly an organization recovers from ransomware is heavily dependent on preparation before an attack, vigilant visibility across the environment, and a clearly defined incident response plan. Organizations must anticipate ransomware risk, withstand and recover from attacks, and continuously adapt their security program to address future threats.

When ransomware tools and techniques successfully infiltrate your environment, coordinated plans and playbooks are critical to withstand and recover from the attack. In this eBook, we outline five critical phases of ransomware incident response for any size SecOps team:

Phase 1: Preparedness

Phase 2: Identification and Verification

Phase 3: Containment

Phase 4: Eradication and Recovery

Phase 5: Evaluation and Adaptation

The number of reported ransomware attacks declined slightly in 2022. Better awareness and improved security controls have played a factor. The war in Ukraine focused cybercriminals on geopolitical issues, and the FBI and private companies offered decryption tools that helped companies recover.

By most estimates however, 2023 has seen a resurgence in volume and the extent of damages. Cryptocurrency tracing firm Chainalysis reported victims have paid ransomware groups $449.1 million in the first six months of this year. For all of 2022, that number didn't reach $500 million. This could signal 2023 to be the second biggest year for ransomware revenue since 2021, when Chainalysis estimated attackers extorted $939.9 million from victims.[1]

To avoid lost revenue, damaged brand reputations, regulatory fines, or paying ransoms outright, assess your team's readiness and coordination in responding to a ransomware incident. To improve your organization's cyber resilience, teams must approach ransomware incidents quickly, in a coordinated effort that prepares for their inevitability, then learn from attacks to improve defenses.

Phase 1

Start with Ransomware **Preparedness**

For proper ransomware preparation, there are three things that everyone on the management team or the incident response team needs to know.

Know the **IR Playbooks**

IR Playbooks for ransomware are critical for the investigation phase. When dealing with Ransomware, recovery cannot happen until the IT team finds how the attacker got in. Otherwise it's like bailing water out of a boat before plugging the leak. The quicker the IR team can assess the scope of the attack and plug the hole, the quicker the business can get back to normal operations. One authoritative guideline for creating an IR response plan is the NIST SP 800-61. For detailed info on IR planning, check out the SANS Incident Handlers Handbook.

Clearly define all of your disaster recovery options and make sure that they are separated from the affected network devices. If you have alternate infrastructure to use or even a Hot/Warm site that can be employed, make sure that the scope of the infection has not spread into the other facility or set of devices.

A well crafted business continuity plan includes all relevant stakeholders and the actions they need to take. One of the biggest challenges is communication. A ransomware IR plan must include detailed escalation trees and RACI (responsibility assignment matrix) models for coordinating efforts. If your engineering team puts something back online too soon, for example, you might have to start the whole process over again.

Knowing the playbooks extends to exercising the playbooks. There's a reason football teams scrimmage against each other: plans on paper are meaningless until they've been practiced over and over to identify the practical issues that the theoretical playbook overlooked.

With the Deepwatch Managed Security Platform, every customer has access to Deepwatch security experts to assist in creating incident response plans or refine existing ones. For ransomware preparedness, Deepwatch experts often participate in interactive table-top incident response exercises with customers to ensure alignment with stakeholders.

Start with Ransomware **Preparedness**

Know Your **Legal Requirements and Restrictions**

Most organizations are legally required to demonstrate compliance with state and federal laws surrounding protection of data, and the disclosure of an incident in a timely manner. In July 2023 the U.S. The Securities and Exchange Commission adopted new rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies.2 The new rules will require public U.S. companies to disclose incidents within four days. In Europe, the General Data Protection Regulation (GDPR) already requires organizations to disclose a data breach involving customers' personal Information within 72 hours. Depending on your type of business, you may have to comply with one or more of the following requirements:

- PCI-DSS
- HIPAA
- GDPR
- SOX
- State breach requirements (i.e.,Virginia's CAN SPAM law)
- Gramm-Leach-Bliley Act

Often vendors, customers, and partners include disclosure requirements in their contracts. Have your legal team review all contracts or SLAs thoroughly to understand your liability.

The U.S. Treasury Department warns against the payment of ransomware to threat actors. They have placed sanctions on potentially state sponsored ransomware groups that, if paid, could bring legal action against the company that paid the ransom. Ransomware attack victims should not try to negotiate ransom on their own and should contact their cybersecurity insurance company, their managed security services provider if one exists, and the FBI.

Know Your **Environment**

The more your team knows about the details of your network environment, the quicker they will be able to assess the scope of an attack and begin remediation and recovery. Working with a managed detection and response partner that understands your unique environment is critical. Security teams can be far more prepared for outside DFIR engagements if they already have teams in place to provide details on log ingestion, endpoint monitoring, or network configuration.

Phase 2

Ransomware **Identification & Verification**

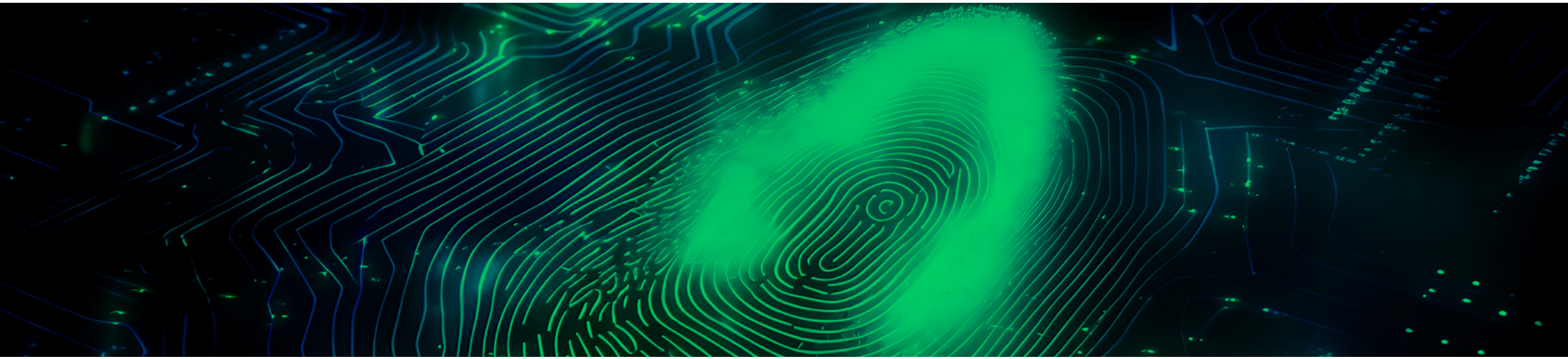
When a ransomware attack occurs, awareness starts with either an alert to the security team, or reporting from other departments. Before an incident response begins, the threat must be verified as a true positive and clearly identified for what it is. More than mere technical tasks, identification and verification are critical Risk Management steps.

Before shutting down the network or dramatically taking an axe to the network cable, security teams should first verify any incident.

The critical step of incident verification allows teams to investigate whether an attacker has actually performed the intended actions on the network before declaring a formal incident or kicking off the incident response process.

Many network events and even other malicious attacks can look similar to ransomware. Malicious web pages may mimic ransomware in an attempt to trick victims, but don't actually infect the host device.

Once an incident has been verified, containment and remediation actions of the team must be defined and focused on the scope of the attack. The scope of the initial attack, initial identification and triaged investigation of affected devices would happen in this phase.



Phase 3

Containment of an Active Ransomware Attack

Notification

Ransomware comes with a high degree of social impact, and must be handled properly to minimize both unnecessary disclosure as well as protect reputational damage to the organization.

When an incident occurs, the first step is to notify stakeholders using the defined RACI matrix in the IR documentation. Management, Legal and ultimately Marketing or Public Relations must coordinate notification to other stakeholders.

All required notifications must comply with regulatory and contractual obligations.

If there is an MSSP or MDR partner, they should be notified of the confirmed incident and can often lighten the load of analysis, and decrease the overall time to containment and remediation.

Isolation

Isolation is a bit more difficult in ransomware scenarios, as the infection is often widespread. Isolation can help prevent further spread and help speed remediation efforts. Isolation provides system administrators the ability to segment and remediate a group of devices at one time.

Containment is the critical action phase where remediation efforts start. Here security teams must follow defined incident response plans to the letter, as deviation from them could have financial and legal consequences.

Collection

Incident Responders and Forensic Analysts

Device forensic data: memory dumps, hard drive images, etc. Legal requirements of ransomware incidents and the involvement of law Enforcement may include extra chain-of-custody requirements that the team must follow. The legal department should provide guidance on any extra DFIR measures.

Security Analysts

While the IR team is focused on collecting volatile data off of the infected devices, the security analyst team assists with the investigation by looking at the timeline of the ransomware attack, looking for any indicators of initial compromise as well as persistence actions. If using an MSSP, they should be informed that incident response is underway, and enlisted to help where relevant and required.

Technical Leadership and the IR Team Lead

Technical leadership and incident responders must provide status updates on progress made by the team, keeping all other stakeholders informed. Ransomware attacks create high stress levels and stakeholders will need continuous updates. The IT and IR teams must collect the necessary information and communicate its meaning, as well as act on recommendations and develop an on-going roadmap for risk mitigation activities.

Phase 4

Eradication & Recovery from the Ransomware Attack

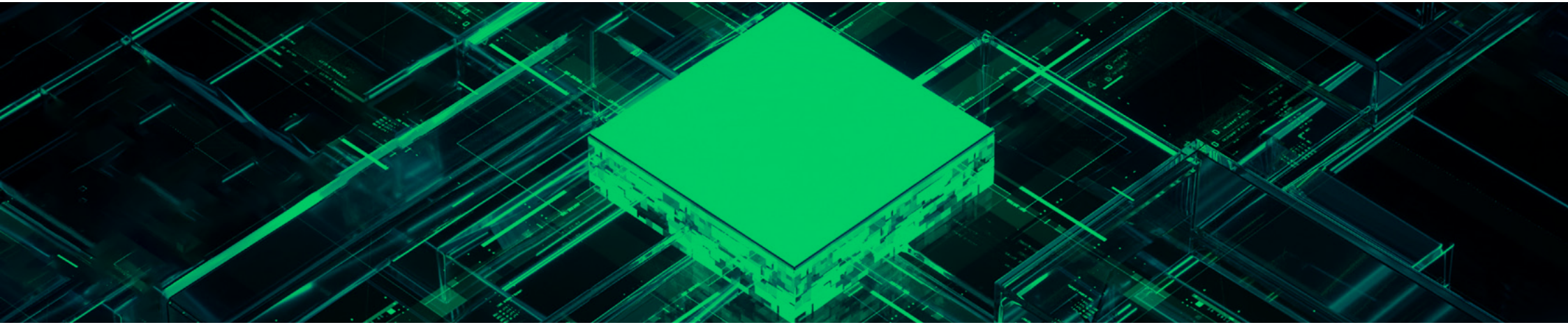
Before remediation, teams must determine the root cause of the infection and fix it. This prevents reinfection of the target devices. While getting devices back online may seem like a top priority, a responder must confirm the confidentiality and integrity of the data first. Teams should first check the most popular attack vectors for ransomware including phishing, open RDP ports, or high profile vulnerabilities. They should then identify the type or strain of ransomware and any previously identified vectors. Responders can then utilize documentation sourced from other security analysts who have shared IR plans with the community.

Back-up data storage and testing is part of overall security governance. After a ransomware attack, while managing backup restoration and remediation, Deepwatch experts monitor your environment, continuing to identify any transient issues while backup recovery is underway.

Re-imaging and restoring data from backups is often an organization's best option. This step is time-consuming, however, and there can be some data loss. On the other hand, if the network has been penetrated so far that devices are completely locked up, it's safe to assume that most data is lost on that device and should not be recovered.

This step often combines both eradication and recovery actions. *Note on Backups: Off-line backups are critical. Tapes or drives in a vault disconnected from the network are sometimes the only way to ensure they weren't part of the event. Backing up the index info and having copies of the backup/restore software suite are key as well. IR responders should review the timeframe of the attack and ensure a backup is restored before the initial compromise occurred.

Ransomware reinfection is a serious concern, and backups are a top target if they are not separated from the rest of the network. Responders must be aware that any files from personal removable media or cloud storage could also be compromised.



Phase 5

Ransomware
IR Lessons Learned

Failure to learn from the past ensures its repetition in the future. No matter what phase of the lifecycle an attack is discovered, once cyber criminals find a way into the network and initiate a ransomware attack, a full digital forensics investigation must be conducted to confirm how the attack happened, and how to prevent similar attacks in the future. All identified gaps in security must be addressed to prevent reinfection. A post-mortem investigation of a ransomware attack can reveal security gaps. Considering the high probability that cyber criminals will attack again, security leadership must fill the gaps and set new standards to maintain security outcomes in the future.

1. Review the vulnerability management program as a whole for growth opportunities
2. Review the device hardening standards and firewall rules.
3. Conduct wide-spread phishing training and educate all staff
4. Conduct a post-mortem assessment with your MSSP or MDR team to address lessons learned and fill security gaps.

Withstanding and recovering from a ransomware attack takes time, effort, and money. In addition to any post breach remediation, companies should make additional investments to ensure all security gaps are fixed, because now the likelihood of another attack has just increased. When a ransomware attack hits, leadership should work together with trusted experts to ensure the cybersecurity program can protect and defend against the next attack.

Lessons

- Review the vulnerability management program as a whole for growth opportunities.
- Remediate the vulnerability that was used for the initial compromise.
- Identify and patch new vulnerabilities.
- Review the device hardening standards and firewall rules.
- Go beyond simply blocking an RDP port to a sensitive device and implement detection use cases that would catch any violations of these restrictions.
- Establish strong firewall rules and increase device hardening standards to mitigate risks.
- Conduct wide-spread phishing training and educate all staff.
- Help non-technical employees learn how to report and block the email address of a phishing sender.
- Implement a phishing program so staff know how to report suspicious emails to the Security team. A phishing program enables the in-house team to detect when a real phishing attack is occuring within the network, and to track down any users who may have fallen victim to the phishing campaign.
- Work with an MSSP or MDR team to address “lessons learned.”
- Develop new threat detection use cases to map to new tooling or data discovered after the incident.
- Conduct a post-mortem review with the IR team to review identified security gaps, create remediation tasks to fill those gaps, and improve the IR plan.

deepwatch™

About the Deepwatch Managed Security Platform

Deepwatch® is the leading managed security platform for the cyber resilient enterprise. We partner with your team to help you anticipate, withstand, recover from, and adapt to threats in your unique environment. We operate as an extension of cybersecurity teams by delivering unrivaled security expertise, unparalleled visibility across your attack surface, precision response to threats, and the best return on your security investments.

The Deepwatch Managed Security Platform includes our threat management capabilities, Deepwatch Security Center engagement technology, and Deepwatch Experts including named analysts, engineers, and threat hunters that serve as an extension of your organization.

SOURCES

“Ransomware Attacks Are on the Rise, Again,” Wired, July 12, 2023

“SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies,” SEC.Gov, July 26, 2023 SP 800-61 Rev. 2:

Computer Security Incident Handling Guide, NIST

Incident Handler’s Handbook, SANS Institute

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, the U.S. Department of the Treasury’s Office of Foreign Assets Control

Blue Team Handbook: Incident Response Edition, Don Murdoch

Larry Greenblatt CISSP 2020 Exam Tips video, YouTube