deepwatch

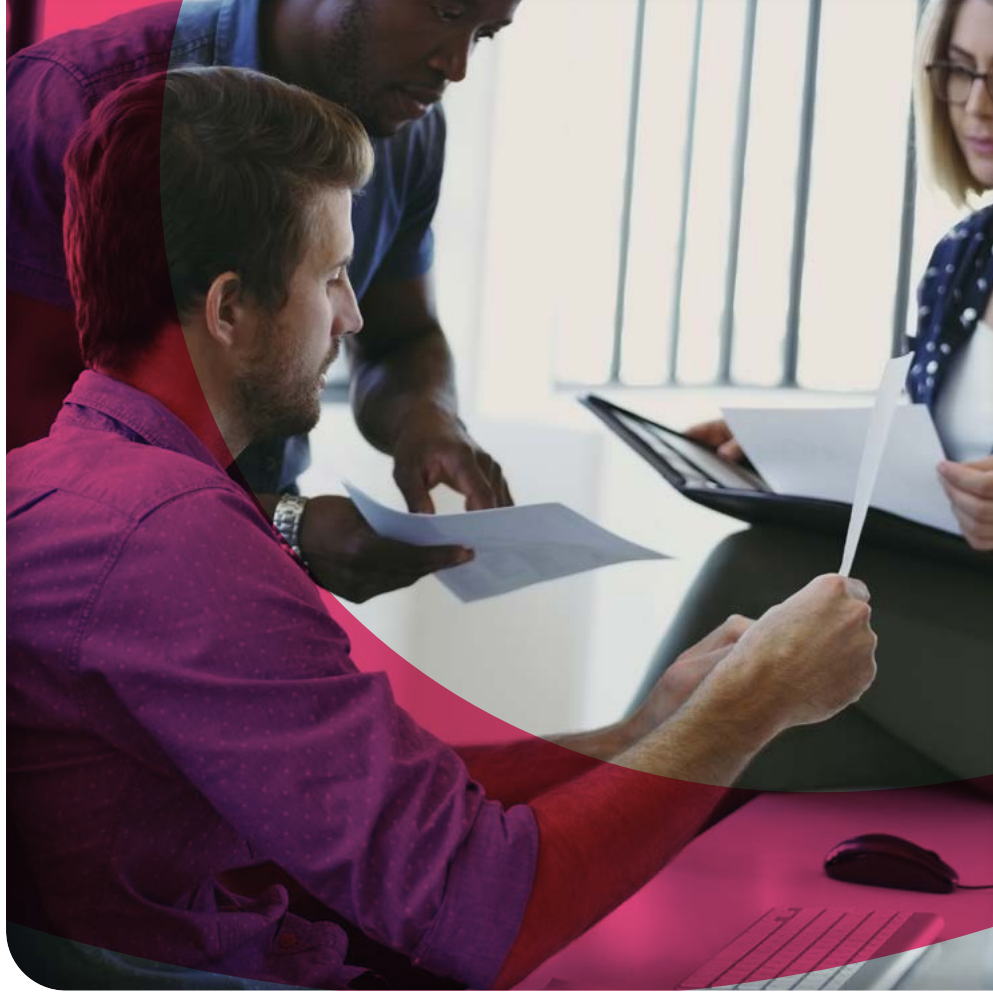
5 Phases of Coordinated Incident Response to Ransomware

Introduction

Recovering from ransomware is a process that is heavily dependent on the preparation an organization does prior to a ransomware attack, and often long before the attack has happened. The amount of ransomware preparedness a team has invested in prior to an attack has a direct impact on the speed and efficiency of the organization's response to the ransomware attack.

The impact of ransomware can be readily measured in dollars lost due to downtime of critical company operations, as well as the direct costs of remediation which may or may not include paying a ransom or fines associated with having paid a ransom. Ransomware preparedness takes the guesswork out of "what if" so companies can begin to mitigate these costly ransomware risks.

Beyond preparedness, the attack and recovery from a ransomware crime can have devastating effects on a business' bottom line in terms of reputational damage, 3rd party legal proceedings, and other secondary results. The following five phases describe preparation and what an actual attack will require for full remediation. By focusing on preparedness, the time to respond to an active attack has been proven to reduce the financial impacts of recent estimates of $4.6M in ransomware breach costs.



Business leaders have increased their investments in security operations. It's critical to evaluate how that return is delivering on outcomes, especially when delivered by a Managed Detection and Response provider.

This MDR Buyer's Guide is focused on the outcomes that security leaders can expect from their Managed Detection and Response provider to support and improve the overall security program.

PHASE 1

Start with Ransomware **Preparedness**

For proper ransomware preparation, there are three things that everyone in 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 and has it remediated. 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.
- A well crafted business continuity plan will have all of the actions, from each relevant department, that they need to take in a given scenario. One of the biggest aspects of a business continuity plan is communication. This plan will have detailed escalation trees and RACI (responsibility assignment matrix) models for coordinating efforts. If the engineering team puts something back online too soon, you might have to start your whole process over again.
- Beyond the communication, 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.
- 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.

Your Managed Services Security Provider or MDR Provider is a great resource for IR preparedness. With Deepwatch Managed Detection and Response services, every customer gets an assigned team of security experts, called the "Squad," to monitor each customer's environment 24/7/365. Beyond monitoring, the Squad also assists customers with creating incident response plans and refining existing ones. To further advance ransomware preparedness, Deepwatch Squads participate in interactive incident response table-top exercises with customers to ensure alignment with stakeholders.

Know Your Legal Requirements And Restrictions

- Most organizations will be legally required to comply with state and federal laws surrounding protection of data as well as the disclosure of an incident. It is the legal and communications teams responsibility to coordinate disclosures and reports to the proper authorities in a timely manner. The GDPR, for example, provides businesses with a 72-hour window to disclose a data breach involving customers' personal information. Depending on where you do business, you may have to comply with requirements of one of the following:
  - Gramm-Leach-Bliley Act
  - HIPAA
  - SOX
  - State breach requirements. (i.e., Virginia's CAN SPAM law)
  - PCI-DSS
  - GDPR
- One category everyone should be aware of are the disclosure requirements that are contractually required from vendors, customers, and partners. Have your legal team review all contracts thoroughly for disclosure requirements.
- One restriction as of 2020 is detailed in an advisory from the U.S. Treasury Department on the payment of ransomware to the threat actors. They have placed sanctions on certain potentially state-sponsored ransomware groups that, if breached, would bring legal action against the company that paid the ransom. If you are notified that you are under a ransomware attack, contact your cybersecurity insurance company, your managed security servicesprovider if you have one, and the FBI. Do not attempt to broker the ransom on your own, as certain situations may have legal requirements for negotiation.

Know Your Environment

The better your team knows the details of your network environment, including devices, assets, and applications, the quicker they will be able to assess the scope of the attack, and begin remediation and recovery. For more on how to set up comprehensive network monitoring, see Deepwatch's Network Security Best Practices.

PHASE 2

Ransomware **Identification and Verification**

When a ransomware attack occurs, it usually starts with either an alert for the security team, or another department reporting an issue. Before incident response begins, one important step must be taken: the incident has to be confirmed as a true positive. This is not a technical task, but rather, a Risk Management task.

STRENGTHEN THREAT DETECTION AND RESPONSE CAPABILITIES

- Larry Greenblat, CISSP mentor extraordinaire, explains that when a practitioner has the option of shutting down the network, taking an axe to the network cable, or verifying the incident, they should first verify the incident.
- Many network events and even other malicious attacks can present similarly to ransomware. There are even malicious web pages that will say the target machine has ransomware, in an attempt to trick the victim, but doesn't actually infect the host device. The critical step of incident verification allows the team to investigate first whether an attacker has actually performed the intended actions on the network before declaring a formal incident and kicking off the incident response process.
- Once an incident has been declared, the containment and remediation actions of the team need to be defined and focused by the scope of the attack. The scope of the initial attack vector(s) used, as well as the initial identification and triaged investigation of affected devices, would happen in this phase.

Your MSSP or MDR provider is there to help you detect ransomware threats that may already be in your network. With Deepwatch MDR, the detection processes we have in place are mapped to the MITRE ATT&CK Framework, and engineered to identify and respond to threats fast. Proactive threat hunters look for anomalous activity, while the Squad monitors customer networks and manages security alert investigation.

PHASE 3

Containment of an Active Ransomware Attack

This is the action phase where to start remediation efforts. This is the time for the security team to follow defined incident response plans to the letter, as deviation from them could have legal consequences.

Notification

- The first step is to communicate with the management chain using the defined RACI matrix in the IR documentation. This usually starts with management closely followed by legal. Next, as above, all required notifications need to be performed per the regulatory compliance and contractual obligations. Lastly, leadership should coordinate with marketing/public relations. Ransomware has a high degree of social impact, and must be handled properly to minimize both disclosure as well as reputational damage to the organization. If there is an MSSP or MDR partner, they should be notified of the official incident. They 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. It can help prevent further spread as well as triaging remediation, if the affected subnets could be isolated from each other. This will provide system administrators the ability to segment and remediate a group of devices at one time.

Collection

Incident Responders / Forensic Analysts
Device forensic data: memory dumps, hard drive images, etc. With the legal requirements of ransomware incidents and the involvement of law enforcement, there may be extra chain-of-custody requirements that the team must follow. Consultation with the legal department should be taken for 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 can assist with the investigation by looking at the timeline of the ransomware attack and look for any indicators of initial compromise, as well as persistence actions. If an MSSP has been hired for security monitoring, they should be informed that incident response is underway, and enlisted to help where relevant and required.

Technical Leadership and the IR Team Lead
It's critical to collect the data as well as provide the status of progress made by the team and keep all other stakeholders informed. Ransomware will have stress levels high and leadership will be asking for updates constantly. The IT and IR teams can collect the necessary information and relay it, as well as act onrecommendations and develop the on-going roadmap for risk mitigation activities.

PHASE 4

Eradication and Recovery from the Ransomware Attack

The last step before remediation is to determine the root cause of what caused the infection and fix it. This will prevent 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 check out the most popular attack vectors for ransomware for remediation actions. These will typically be Phishing, open RDP ports, or high profile vulnerabilities. By identifying the ransomware strain and any previously identified vectors, responders can get investigation documentation sourced from other security analysts who have documented IR plans online.

Back-up data storage and testing is part of overall security governance. After a ransomware attack, while managing backup restoration and remediation, the Deepwatch MDR service and Squad will monitor your environment, and continue to identify any transient issues while your backup recovery is on-going.

For remediation, re-imaging and restoring data from backups is a great option. This step is time-consuming and there will be some data loss. On the other hand, if the network has been penetrated so far that devices are completely locked up, and a real attack is occuring, it's safe to assume that most data is lost on that device and should not be recovered. The good news: this step combines both the eradication and most of the recovery actions.

***Note on Backups:** Off-line backups are critical here. While they will feel extremely "old school," tapes/drives in a vault somewhere 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 back-up 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. For enduser workstations, the desktop administrator and incident responder can work together to restore from a known good, "Golden Image", then pull any safe data that needs to be restored. Also, responders should be aware that restoring any files from personal removable media or cloud storage could also be compromised, as ransomware will try to hide anywhere it can for reinfection.

PHASE 5

Ransomware IR
Lessons Learned

Ransomware IR Lessons Learned

Failure to learn from the past will ensure its repetition in the future. Once cyber criminals have found a way into the network and initiated a ransomware attack, no matter what phase of the lifecycle it was found, a full digital forensics investigation should 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 another attack.

The IR team will reveal the security gaps in a post-mortem investigation of a ransomware attack. Considering the high probability that cyber criminals will attack again, security leadership can take this opportunity to fill the gaps and set new standards to maintain the security requirements in the future. By following these four steps, the security team can help the business stay ahead of what's coming:

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. **Work with an MSSP or MDR team to address "lessons learned"**

1 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.

3 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.

Getting the business back to normal operations after a ransomware attack takes time and money. In addition to any postbreach remediation, companies should make additional investments to ensure all security gaps are fixed, because now the likelihood of another attack has just increased. A recent study found that repeat ransomware attacks hit 80% of victims who paid ransoms. 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.

2 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 violationsof these restrictions.
- Establish strong firewall rules and increase device hardening standards to mitigate risks.

4 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

To learn more about Deepwatch MDR and how we provide improved detection and reduced risk for our customers, **visit www.deepwatch.com or reach out to us at sales@deepwatch.com.**

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

SOURCES

SP 800-61 Rev. 2: Computer Security Incident Handling Guide, NIST: https://csrc.nist.gov/publications/detail/ sp/800-61/rev-2/final

2. Incident Handler's Handbook, SANS Institute: https://www.sans.org/white-papers/33901/

3. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, the U.S. Department of the Treasury's Office of Foreign Assets Control: https://home.treasury.gov/system/files/126/ofac_ransomware_ advisory_10012020_1.pdf

4. Blue Team Handbook: Incident Response Edition, Don Murdoch: https://www.blueteamhandbook.com/

5. Larry Greenblatt CISSP 2020 Exam Tips video: https://www.youtube.com/watch?v=HWg2geVJuvs

6. https://home.treasury.gov/system/files/126/ofac_ransomware_ advisory_10012020_1.pdf

7. Ransomware and The True Cost to Business: A 2021 Global Study on Ransomware Business Impact: https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

8. S0cm0nkey's Security Reference Guide, Tom Harrison (@s0cm0nkeysec), Lead Analyst at deepwatch: https://s0cm0nkey/gitbook.io/s0cm0nkeys-security-reference-guide/