RAPID7

SOLUTION GUIDE

Ransomware Playbook

Actions you can take to lower the risk and impact of this kind of attack.

TABLE OF CONTENTS

Introduction

The threat of a ransomware attack is the thing that keeps IT, security, and executive teams up at night. Not only can the impact be significant, but every ransomware story seems to make headline news.

Victims of ransomware attacks suffer the impact of productivity and revenue loss due to work stoppage. Those businesses are also likely to have to manage communications with the press, customers, prospects, and vendors as well.

Ransomware is a unique security threat where most of the security team's effort is spent on prevention and response because once ransomware is detected, it's too late. However, there are many actions you can take to lower the risk and impact of this kind of attack.

What is ransomware?

First, let's define ransomware. Ransomware is malicious software that covertly encrypts your files—preventing you from accessing them—and then demands payment for their safe recovery. Like most tactics employed in cyber-attacks, ransomware attacks can occur after clicking on a phishing link or visiting a compromised website.

How do ransomware attacks happen?

Ransomware attacks happen similarly to other malware-based attacks. Here's an example of a typical Ransomware attack from an incident response engagement Rapid7 conducted where the customer's environment was encrypted using the popular Ryuk ransomware.

> The threat actors conducted targeted spear phishing attacks against multiple users at the customer account, sending the emails from a compromised third party that the users already had an established relationship with.
>
> The user clicked on a link in the phishing email that instructed the user to install software to view a PDF. Once executed, TrickBot malware was installed on the system.
>
> Leveraging this initial foothold, the threat actors leveraged TrickBot modules to harvest credentials using Mimikatz, and moved laterally in the environment using PowerShell Empire. Within a few days, the threat actors gained access to an account with elevated

privileges, and deployed Ryuk ransomware to hundreds of systems in the environment using the Windows system administration tool PsExec. Rapid7 identified "hands-on" keyboard activity within minutes of TrickBot entering the environment.

Typical delivery methods

As the example above shows, the first step of any ransomware attack is to get the malware installed on the host system. This typically occurs using specific techniques for initial access:

- Spear phishing - where the victim receives an attachment or link that they click
- Drive-by - where an attacker is able to exploit a vulnerability in the web browser or related applications
- Exploitation - where an attacker is able to exploit a vulnerability and gain access to a remote system or allow the ransomware to propagate automatically
- Replication through removable media - this also includes networked media that ransomware encrypts at the same time as it infects the victim
- Valid accounts - where an attacker has valid credentials to the target system and can authenticate to it

From there, attackers will use common techniques for execution, typically through:

- Command-Line Interface / Graphical-User Interface
- PowerShell
- Scripting
- User execution

How have attackers changed?

For many ransomware attacks in the past, threat actors employed mass spam campaigns to socially engineer users into clicking links or attachments. Once clicked, ransomware encrypted the system and, in an automated fashion, potentially encrypted other systems where access was established or allowed, such as a mapped file share.

Increasingly over the past few years, there has been a shift to "big-game hunting" threat actors leveraging access established by taking advantage of poor security controls in an environment like an unpatched externally facing server, unsecured remote access solutions, or an undetected banking trojan (such as TrickBot, Emotet, or Dridex).

When access is gained, the threat actors go "hands on" using post-exploitation frameworks to recon the environment and gain elevated privileges. If a threat actor gains unfettered access to the environment, they can encrypt the network en mass (deploying Ryuk or BitPaymer), leading to complete disruption of business services. Many times this leads to ransomware taking down large healthcare centers and hospitals, manufacturing facilities, educational institutions, municipalities, and other corporations.

These big-game hunting threat actors have continued to increase their ransom demands, which are now regularly in excess of seven figures. In addition to rendering the network unusable, some of these threat actors exfiltrate sensitive data and extort their victims by threatening to release the data.

Your best defense is a full incident response plan

To say that ransomware causes technical difficulties is an understatement. Without the proper preparation, an attack can bring your business to a grinding halt and put your critical information at risk. Fortunately, ransomware attacks are both avoidable and containable by following fundamental security and disaster recovery best practices.

Because security teams primarily try to prevent ransomware from getting through the perimeter, teams should focus on updating policy, controls, and technology to best prepare:

1. **Preparation** - Are you ready if a ransomware attack happens? Do you have a playbook? Does your team know what to do and who is responsible?

2. **Identification** - What are your measures to identify ransomware before machines are encrypted and a message asks you to pay? How can you identify that an attack is taking place before ransomware is executed?

3. **Containment** - Do you have proper methods (or have automation workflows) in place to contain threats early in the attack chain? The earlier you're able to contain the threat, the more likely you are to restrict the ability of an attacker to execute the ransomware.

4. Eradication - Can you eradicate the threat on your own or do you have an Incident Response retainer set up in the event of a breach? Cleaning things up is one of the last things to do in a ransomware attack. Are you able to scope the incident thoroughly to understand what happened and prevent it from happening again? Do you have the expertise on staff to eradicate the threat completely, ensuring you're not going to get encrypted in a week?

5. Recovery - Do you have proper measures in place to recover from an attack and get things back to normal as soon as possible?

6. Review Lessons Learned - What is your post-mortem process? How can you use this as a lesson to improve your security posture?

Ransomware threat prevention and response

To prevent ransomware threats, there are two distinct phases of the attack lifecycle where we can act. In MITRE ATT&CK parlance, those are the initial access phase and execution phase; the ransomware needs to get past the perimeter and run.

Avoiding ransomware and reducing risk

To reduce risk, organizations should focus on reducing the attack surface by looking at the specific techniques attackers are using to deploy ransomware. From there, security teams can apply layers of preventative measures and reduce risk.

User education training

User education is the first line of defense in our preventative arsenal -- people should not be clicking suspicious links or visiting websites that are known carriers of malvertising networks. Organizations should look to add technology and content that reminds the user to be cautious when the user needs to be cautious. It sounds complicated, but notices on emails originating from outside sources including a reminder to be vigilant are effective. Education programs should address the following:

- All users must use caution when opening links or attachments. Users should ask:
    - Do I know the sender?
    - Does this look suspicious?
    - Is this something that I should open or a link I should follow?
- Users should receive instruction on how to use a Virtual Private Network (VPN) while accessing public WiFi.
- Users should be reminded not to provide personal details when answering emails, phone calls, texts, or other messages, and should contact the IT department as soon as possible if there is a suspicious communication.
- Users should know how to validate IT resources and communications to ensure a communication from a new contact is not an attempt at social engineering.
- Users should alert the IT department before traveling.

Reduce the attack surface

One of the best ways to lower the possibility of a successful ransomware attack, or any other cyber attack, is to reduce your attack surface. Segmenting your network can ensure that critical

machines are isolated to prevent the spread of malware. This is an important step in lowering the potential, and impact, of a ransomware attack.

Ensure account permissions are managed appropriately

Creating granular controls on user rights, specifically restricting administrative rights on endpoints, can reduce the attack surface and capabilities for malware to spread across the network. These include:

- Restricting write permissions for servers
- Restricting admin users and privileged accounts
- Granting users the lowest-level system permissions that still allows them to do their job
- Removing abilities for users to install and run unapproved software applications on the endpoint

Blocking indicators of the ransomware

Blocking indicators of malicious executables will prevent the ransomware from executing and communicating with the command-and-control server. Doing so may prevent subsequent infections from fully encrypting the target data. For example, proper mail scanning should have the ability to filter files by extension, specifically ".exe" files.

Mitigate spear phishing

Spear-phishing mitigation technology can be deployed to inspect links and attachments at the mail server. The amount of risk organizations reduce is directly proportional to the layers of technology and controls applied.

An optimal layered approach would include technology that looks for known threats in attachments and links, technology to run and perform analysis on suspicious attachments and links, and technology that would enforce the reputation of the sender (though this might impact the ability for the business to fully operate).

Mitigate drive-by attacks

Drive-by web proxy technology can be deployed to inspect web browsing activity for ransomware threats. The amount of risk reduction here is directly proportional to the layers of technology and controls applied.

An optimal layered approach would include domain name resolution sinkholing to prevent users from accessing malicious domains, content inspection technology to identify and evaluate applications being transferred across the network, and network threat prevention technology to block access to known bad IP addresses.

Mitigate exploitation

Exploitation mitigation is achieved by patch management; routine scanning for vulnerabilities, prioritizing them based on active threats, and quickly deploying patches are the keys to success. Ensuring operating systems and any software running on the machines on your network are patched with the latest updates reduces the number of exploitable entry points for an attack. One common area attackers are exploiting is via third-party software such as Java, Flash, and Adobe. Many common attacks can be prevented by ensuring often-targeted software is patched.

An optimal approach would involve weekly scanning for vulnerabilities, dynamic prioritization of vulnerabilities based on how they are being used by attackers, and a less than 24 hour patching timeline for critical remediations. It's best to use automated patching when possible.

Mitigate replication through removable media

Replication mitigation can be summarized by undoing all that Windows does to make networked computing easy:

- Do not use persistent mapped network shares.
- Do not allow removable media to be automatically mounted.
- Prohibit writing to removable media.
- Apply a layered network architecture and prohibit discovery of Windows operating systems across network zones.

Mitigate invalid accounts

Valid account mitigation can be achieved by enforcing multi-factor authentication to valuable data assets in your environment. Further, enforcing a stricter authorization model instead of the traditional default allow will reduce the impact of credential theft.

Mitigate execution

Execution mitigation technology like next-generation antivirus (AV), endpoint detection and response, firewalls, behavioral-based detections, application whitelisting, and sandboxing can be deployed to add layered defenses to prevent the threat of ransomware on the endpoint. In the

case of AV or anti-malware solutions, this is typically one of the first lines of defense for your business, blocking payloads from launching. It's imperative to keep AV solutions up to date to ensure the most recent signatures of new malware variants are being assessed. Sandbox technology gets the honor of mitigating both risk and impact as the sandbox will typically not let the ransomware permanently encrypt resources. There are also many controls that can be deployed including limiting user permissions, restricting scripting capabilities, and limiting administrative tools on workstations.

Monitor your environment for process-related triggers

Developing policies for disabling macro scripts unless approved by security is one way to prevent exploits delivered by common documents. However, it should be standard to disable executables, such as macros, from running from any email attachment. Users who open attachments and enable macros often execute the payload which installs malware on the machine. One way to spot this type of malicious execution is to monitor the process start/stop on the machine and to correlate the opening of a document, for example, Powershell invocation spawned from a Word document. This is rarely an action taken by a user, so this type of action would most likely be correlated to an attack.

Implement early detection mechanisms

The last lever to pull in avoiding ransomware is to detect an infection before it spreads. Of course, if you detect ransomware, it's already too late, but there is often a period of time to respond to indicators of threats before ransomware hits, or to limit the spread of the encryption and impacted data in the event that ransomware is present on systems.

Detecting ransomware can be done with traditional detection methods like simple indicator matching, user behavior analytics, or attacker behavior analytics (including process spawning). Ransomware carries similar traits to traditional malware. Once detected, quickly implementing remediation steps is paramount. You should consider some automation solutions with the following capabilities:

- User account actions, such as locking or deleting an account and/or forcing a reset
- Firewall IP address blocking
- Domain blocking
- Process termination
- Physical network port blocking

Limiting the impact of an attack

To limit the impact of a ransomware attack, security teams need to limit its access to mission-critical data and be able to quickly recover data encrypted by the ransomware. Mapped to the MITRE ATT&CK framework, the specific technique that attackers use is “Data encrypted for impact.”

Security teams should ensure that all techniques for limiting access to mission critical data are listed in the above 'Ransomware threat prevention and response' section. Further actions to ease the speed with which your organization recovers from a ransomware breach include:

Removing infected systems from the environment

This may be a technological solution like disabling a physical network port or a manual process like physically removing the network cable from the port. Removing infected assets can help limit the replication of the ransomware to adjacent assets.

Restore data with no loss

The first step to ensuring business continuity in the event of a ransomware attack is to employ a comprehensive data backup and recovery plan for all high value data. The good news is, backing up your systems (and testing the restore) should be a high-priority investment, anyway.

The healthiest way to think about your ransomware-locked systems is the way you'd think about laptops your employees dropped on business trips. Sure, you might recover the data on them if you keep at it, but it would save everyone a lot of time and effort if you just restore the backup images from last night to the impacted systems (or replacement laptops). Great backup hygiene is somewhat like your insurance policy. And it’s most likely something your IT team is doing anyway to prepare in the case of natural disasters (like floods) or building disasters (like broken water pipes).

But just backing up files is not enough; important files and backups should be isolated on external storage devices or in the cloud, disconnected and inaccessible from any potentially infected computer once the backup is completed. It’s important to perform backups and test these in a real-world environment to limit the impact of data loss and ensure the backups are able to recover quickly should a ransomware attack occur.

Issuing new assets

Part of reducing the impact of ransomware is ensuring employees are able to do their job as quickly as possible. It's important that the Security and IT teams audit and practice these business continuity plans. Teams don't want to be in a position where they find out there are no more assets in the IT closet and data backups haven't run in 7 days when trying to recover from a breach.

Should you pay the ransom?

The ultimate question when it comes to ransomware is: to pay or not to pay?

Hopefully by following the above recommendations to proactively prevent ransomware attacks and limit their impact if the attack is successful allows your business to reduce the need to consider the question in the first place. But if your files *are* encrypted, what do you do?

Most stances, including the US FBI, recommend not paying the ransom demanded by cybercriminals. Similar to other criminal actions, it's recommended not to negotiate since there is no guarantee the criminals will send you the decryption keys and you'll regain access to your files. Paying the ransom will encourage criminals to continue carrying out these attacks by funding their activity.

Warnings for ransomware prevention

Ransomware as attacker cover

Is the ransomware attack really the end goal of the attacker?

Over the last couple years, we've started to see an increase of ransomware being used to cover up for other attacks. Initially, it was thought the attackers' motivation was to distract responders, but it could be possible that attackers are realizing how numb we're becoming to these types of attacks; to the point where we're not even investigating them anymore. It’s best practice to investigate the rest of your detection telemetry for anomalies in addition to the ransomware attack. It’s very possible that there may be something more nefarious going on.

Don’t get caught by recency or news bias

For those with a tested disaster recovery plan and desire to still do more, beware the common mistake the human mind makes called the “focusing illusion,” or convincing oneself that a current event or problem in focus is the most important one. This frequently leads to losing sight of the bigger picture and improperly planning for the future. If you are going to focus your defensive efforts solely on ransomware, it will make you more susceptible to the many other security threats to your business.

Ransomware response actions

When facing a ransomware attack, it's best to have a playbook of what to do. The majority of ransomware attacks are initially spawned by malicious documents or malware. We recommend ensuring your team takes the below prescribed actions to stop ransomware attackers early:

Remediation steps

Rebuild the system(s) from a known-good baseline image
Rapid7 recommends rebuilding the system from a known-good baseline image to counter undetected threats.

Scan the system(s) with an up-to-date anti-virus solution
Rapid7 recommends scanning the system with an up-to-date anti-virus solution to remove malware and related artifacts.

Block malicious domain(s) identified
Rapid7 recommends blocking the malicious domain(s). This should be performed at all appropriate network filtering and domain name server devices such as firewalls, web proxies, and DNS servers.

Terminate the malicious processes
Rapid7 recommends immediately terminating the malicious processes on the compromised endpoint(s) identified.

Quarantine network traffic from the affected endpoint(s)
Rapid7 recommends immediately quarantining the affected endpoints from the network.

Lock the affected account(s)
Rapid7 recommends locking the affected compromised account(s) until the credentials can be rotated.

Change password(s) for affected account(s)
Change the affected account(s) password(s) as soon as possible to prevent an attacker from leveraging the credentials to access services.

Block malicious IP address(es) identified (if applicable)

Rapid7 recommends blocking the malicious IP address(es) identified in this report. This should be performed at all appropriate network filtering devices such as firewalls, web proxies, routers, and switches.

Identify and remove malicious email from other inboxes (if applicable)

Rapid7 recommends determining whether or not other users received the email and removing the email from all mailboxes.

Block the sender's email address (if applicable)

Rapid7 recommends blocking the sender's email address.

Mitigation steps

Remove local administrator rights from a user's account

Rapid7 recommends removing a user's domain account from the local administrator group. User accounts with administrator rights allow for automated and targeted attacks to interact with system-level privileges, including dumping credentials, modifying firewall rules, disabling security controls, and deploying malware. If you need some direction, Microsoft's LAPS is a great tool to manage local administrator passwords.

User awareness training

Users identified as opening unknown attachments or clicking unknown links should take phishing-based training and know how to forward suspicious links to the IT security group for analysis.

Prevent execution of Office macros via Group Policy

Rapid7 recommends disabling execution of macros in the Microsoft Office suite from untrusted locations. Office macros account for approximately 98% of Office malware; disabling macros significantly decreases the attack surface of user workstations.

Implement unique passwords for local administrator accounts (if applicable)

Local administrator account passwords should be unique per system to prevent lateral movement due to local credential compromise.

Implement application whitelisting for critical systems (if applicable)

Rapid7 recommends implementing application whitelisting for critical systems, such as domain controllers and Exchange servers. Application whitelisting reduces the likelihood that attackers

could execute malware or unapproved utilities and is less labor-intensive to implement on systems with static configurations.

Separate privileged domain access from a standard user account (if applicable)
Rapid7 recommends creating separate user accounts for privileged and non-privileged domain activities. Privileged domain accounts should only be used when required to perform maintenance or other system administration activities and non-privileged user accounts should be used for normal daily activities.

Review firewall and proxy policies (if applicable)
Rapid7 recommends reviewing URL and firewall outbound access policies and blocking high-risk categories (adult material, games, gambling, advertisements, peer-to-peer file sharing, Dynamic DNS, as well as categories such as spyware, phishing, keylogging, and malicious mobile code).

Harden systems by following industry guidelines (if applicable)
Follow vendor-recommended guidelines for security settings on Windows, Mac, and Linux platforms.

Prevent activation of OLE packages in Word documents (if applicable)
Rapid7 recommends preventing activation of OLE packages in Microsoft Word to prevent users from launching malicious packages.

How Rapid7 can help

Preventative measures

Since it is commonplace for ransomware to leverage vulnerabilities to propagate itself, maintaining a proper vulnerability risk management program is critical. Solutions like Rapid7's leading Vulnerability Risk Management Solution, InsightVM can help detect and prioritize assets that may be ideal targets for spreading malware.

Incident detection

Rapid7's leading cloud SIEM InsightIDR (the basis for the MDR technology used by our SOC) uses a variety of mechanisms to detect ransomware in your environment utilizing the configured foundational event sources and the endpoint agents.

In addition to the actual encryption of files, ransomware depends on four main stages:

Stage	Example InsightIDR / MDR Detection
Initial Ingress	Malware document detection
Code Execution/Download/Deployment	PowerShell and code injection
Defense Evasion	Clearing Windows event logs, disabling VSS (Volume Shadow Copy), and disabling backup/restore
Spread	EternalBlue-style SMB lateral movement

In addition to what we have listed above, the Rapid7 Threat Intelligence team located in our MDR SOC is continuously coming up with new detections from our own honeypot network (Project Heisenberg), as well as participating in other cyber-threat feeds.

Beyond curated threat signatures, InsightIDR comes with pre-built Attacker Behavior Analytics (ABA) detections built by the Threat Intel team. ABA applies Rapid7's existing experience, research, and practical understanding of attacker behaviors to generate investigative leads based on known attacker tools, tactics, and procedures (TTP).

It's also worth clarifying that InsightIDR and the MDR service is based on detection, not prevention. The detections that Rapid7 have in place for ransomware will identify ransomware

should it occur. However, this will not prevent ransomware from occurring. Rapid7 strongly recommends patching vulnerabilities found in the environment, user education, and robust backup procedures to reduce the likelihood of a successful ransomware attack.

Automated response

Ransomware attacks are especially destructive and with the necessity for visibility and coverage of remote assets, it'll become an increasingly uncertain environment. Leveraging security orchestration, automation, and response (SOAR) solutions like Rapid7's InsightConnect can help lessen the severity of such attacks (or prevent them altogether) by containing, blocking, or reducing privileges to endpoints.

Many of the above playbook recommendations for containment, remediation, and mitigation can be achieved through automation in conjunction with EDR tools you've most likely already deployed. To explore our growing library of prebuilt plugins and workflows, please visit Rapid7 Extensions.

Final recommendations

If this all sounds complicated, that's because it is. Ransomware continues to evolve to evade the technological solutions we have in place; it is time that our entire security programs rise to support the tools.

The best solutions in security always involve people, process, and technology. Yet our security programs consistently favor the technology, leaving the people to struggle with overwhelming data and inconsistent processes.

We encourage all security teams to build a ransomware defense plan with proper security hygiene, defensive tactics, and a continuity plan to better prepare and respond to ransomware attacks.

Finally, a ransomware plan is useless unless it is practiced and kept up to date. All security staff should rehearse what to do in the event of a ransomware scenario and be prepared to act if a ransomware attack was successful.