RAPID7

SOLUTION GUIDE

Ransomware Playbook

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

©RAPID7 2021

TABLE OF CONTENTS

Introduction

Failing to plan is planning to fail. The old adage holds true now more than ever as companies, governments, and institutions around the world grapple with the ever-changing threat of ransomware.

The Institute for Security and Technology's Ransomware Task Force Report notes that "in 2020, thousands of businesses, hospitals, school districts, city governments, and other institutions in the U.S. and around the world were paralyzed as their digital networks were held hostage by malicious actors seeking payouts."

Victims of ransomware attacks suffer both the impact of productivity and revenue loss due to work stoppage, and potentially may also incur a loss of confidence or reputational hit, which can also impact revenue. Those businesses are also likely to have to manage communications with the press, customers, prospects, and vendors as well.

But it doesn't have to be this way.

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. This playbook aims to provide exactly that. It will give security professionals and business leaders the knowledge and tools to not only prevent ransomware attacks to the best they can be prevented, but to create a remediation plan that can save critical information from the worst types of exploitation.

With ransomware, plan to prevent, plan to protect.

What is ransomware?

First, let's define ransomware. Ransomware is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. CISA defines ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

How do ransomware attacks happen?

Ransomware attacks happen similarly to other malware-based attacks. Here's an example of a typical phishing-based 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.

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 can exploit a vulnerability in the web browser or related applications
- **Exploitation** - where an attacker can 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. Those controls can often be 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 masse (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 exceeding 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. In this scenario, criminal groups are increasingly demanding two ransom payments: one for decrypting all the systems on the network and one for keeping the exfiltrated from attacker data sharing platforms. These types of attacks are known as "double extortion ransomware."

There is another emerging scenario of "triple extortion ransomware" whereby attackers infiltrate an organization, steal data, encrypt systems and then demand the traditional payment for decryption keys. If a victim organization refuses to pay, the attackers threaten to publicly release records either all at once, or piecemeal, until payment is made. With the release of data, the attackers then use customer, partner, and/or vendor information stolen from the victim to conduct denial of service attacks on those third-parties or contact those third-parties (to put payment pressure on the original victim organization), and demand smaller payments from these secondary victims to prevent their data from being included in any public release.

Recent years have also seen the rise of the "ransomware as a service" (RaaS) business model, which provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop malware on their own. This "as a service" model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from "software as a service" and "infrastructure as a service" business models.

The importance of having a full incident response plan

Ideally organizations want to avoid becoming the victim of ransomware attacks, and there are a number of steps that can be taken to reduce the risk and make the job harder for attackers, detailed below. These measures take time to implement though, and while they should make an organization harder to compromise and more able to recover from attack, no organization can be completely invulnerable. As such, it is critical to have a comprehensive incident response plan in place so that if the worst does happen, you are able to react quickly and efficiently to weather the storm.

It may seem counterintuitive to work on response before the incident, and even before deploying preventative measures, but we strongly recommend you do just that — develop and practice your incident response plan now. You need this in place while you work on your preventative measures so you will be prepared if you have an incident before you can fully implement your defenses. Without the proper preparation, an attack can bring your business to a grinding halt and put your critical information at risk.

A comprehensive incident response program will incorporate the following:

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 postmortem 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 you 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.

Before the attack: Avoiding ransomware and reducing risk

To reduce risk, organizations should focus on minimizing 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.

Workforce education training

Workforce education is the first line of defense in your preventative arsenal; people should not be clicking suspicious links or visiting websites that are known carriers of malvertising networks. Hopefully these sites are blocked by your organization's firewall settings, but educating employees about the risks and reinforcing the guidance in the Acceptable Use Policy will also help reduce risk.

Organizations should look to add technology and content that reminds workers to be cautious when they need 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:

- Use caution when opening links or attachments by considering:
    - Do I know the sender?
    - Does this look suspicious?
    - Is this something that I should open or a link I should follow?
- Use a Virtual Private Network (VPN) when performing any work task to gain the benefits of all implemented security controls.
- Do not provide personal details when answering emails, phone calls, texts, or other messages, and contact the IT department as soon as possible if you receive suspicious communication.
- Validate IT resources and communications to ensure communications from new contacts are not an attempt at social engineering.
- Alert the IT department before traveling internationally.

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. While the discipline of attack surface reduction could fill several playbooks and guides on its own there are some basic tenants that all organizations should be following:

- **Detect and monitor for what you AREN'T scanning** - Your vulnerability management (VM) program should include a periodic coverage check, this can certainly be automated if accurate source data is available. Remember cloud and ephemeral assets are part of your attack surface too.

- **Make friends with the application development team** - Application weaknesses — be it from misconfigurations, logic flaws or poor coding hygiene — can all contribute to an organization's attackable surface. So aside from bureaucracy, organizational structure, incentives and time, what is stopping application security management from being a fully ascribed member of the illustrious VM team? Start with a conversation. Reporting and managing risk across the full stack will aid in securing investment and support for refactoring efforts and overdue architectural changes.

- **Vulns come in all shapes and sizes** - Pick up a recent copy of your favorite cyber security trends report and you'll be reminded that a substantial portion of recent (reported) breaches and attacks are due in some way to misconfigurations in cloud-based and traditional infrastructure. Days of ignoring good 'ole configuration management have passed. Hardening baselines must be implemented and maintained under the umbrella of an effective VM program. If you're just starting out, pick an operating system with a smaller footprint or maybe the workstation environment. Slow and steady wins the race, here.

- **Walk a mile in operation's shoes** - The men and women with the much more challenging role in the VM lifecycle are the patching and administration teams. They are tired of getting lists of unverified vulns that number in the 1000's. Simply taking the time to fully understand their workflow, stakeholders and approval gates will go a long way in giving the VM team valuable insights to rejigger their reporting and vulnerability dissemination process. Meet operations where they live — it'll make your work life more satisfying.

Far from an exhaustive list, these themes have a history of recurring across organizations, industries and entire sectors and are areas Rapid 7 can help support, educate and deliver. Defense in depth applies here and causes an echo that attack surface management is an organizational level responsibility.

Purposeful network segmentation can ensure that critical machines are isolated to prevent the spread of malware. Start with the really important stuff. There is value in getting started, if only for certain segments and CIDR ranges. 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 allow 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 efficient 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. It is also important that you have a way to scan and patch remote endpoints such as the laptops of remote employees.

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 (MFA) 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

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 if 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

Important prevention considerations

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

Over the last few years, we've started to see an increase in 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. This means ensuring you have visibility into environments where intellectual property, employee, and partner/customer records are held, accessed, and processed.

Don't get caught out 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. As you work to build up your ransomware prevention capabilities, see how these control enhancements fit into the bigger threat, vulnerability, and risk management picture.

During the attack: Response priorities; Containment; Payment considerations

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.

Additional actions to ease the speed with which your organization recovers from a ransomware breach include the following:

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.

Restoring 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 that 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).

Simply backing up files is not enough, however; 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 can recover quickly should a ransomware attack occur.

Issuing new assets

Part of reducing the impact of ransomware is ensuring employees can do their job as quickly as possible. It’s important that the Security and IT teams audit and practice these business continuity plans. Teams prefer not 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.

Avoiding duplicate attacks

It is not uncommon for organizations who have suffered through a ransomware attack to be attacked repeatedly by the same attacker group or other attacker groups. To avoid becoming a repeat victim, you must quickly identify and remediate the initial access and execution vectors in the first attack, then ensure the original attackers have been eradicated from all networks and assets.

Should you pay the ransom?

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

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

Before you consider paying a ransom, we strongly recommend you investigate alternatives. For example, the No More Ransom project is a collaboration between Europol, various government agencies, and the private sector to gather and share decryption keys. Many governments and law enforcement agencies also offer guidance on recovery and response, so it is worth checking their websites and consulting law enforcement.

It is also critical to understand that even if you pay the ransom and the attackers do release your data and systems, that will not be the end of the matter. You will still need to thoroughly inspect your environment to determine the true scale of the incident, and confirm the attackers no longer have a presence in your system and have not stolen data or caused other harm. You will also need to take steps to harden your systems against a similar attack, and in some cases, you may have to take steps to rebuild or recover systems impacted by the attack. Although attackers involved in the ransomware attack against HSE, Ireland's national health authority, released the decryption keys, HSE has reported that it believes recovering from the attack will cost $600 million.

Most stances, including that of the U.S. 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, and once a criminal group knows you are willing to pay, they may look for other ways to victimize you.

In addition, proceeds from ransomware may help finance child exploitation, human trafficking, or the proliferation of weapons of mass destruction. In some cases and jurisdictions, paying a ransom demand may be a criminal or sanctionable offense. In October 2020, The U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) issued an Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments to highlight the risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities. The G7 issued a similar advisory in their October 2020 Ransomware Annex to G7 Statement.

After the attack: 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 still initially spawned by malicious documents or malware. We recommend ensuring your team takes the below prescribed actions to stop ransomware attackers early.

Remediation steps

Rapid7 recommends:

- **rebuilding** systems from known-good baseline images to counter undetected threats.
- **scanning** systems with an up-to-date anti-malware solution to remove malware and related artifacts.
- **blocking** malicious domain(s) and IP addresses. This should be performed at all appropriate network filtering and domain name server devices such as firewalls, web proxies, switches, and DNS servers.
- **terminating** malicious processes on the compromised endpoint(s) identified.
- **quarantining** affected endpoints from the network.
- **locking** affected compromised account(s) until the credentials can be rotated.
- **changing** affected account(s) password(s) as soon as possible to prevent an attacker from leveraging the credentials to access services.
- **determining** whether other users received malicious communications and removing them from all mailboxes.
- **blocking** the sender's email address (if applicable).

Mitigation steps

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.
- **conducting** phishing-based user awareness training and know how to forward suspicious links to the IT security group for analysis.

- **disabling** execution of macros in the Microsoft Office suite from untrusted locations via Group Policy. Office macros account for approximately 98% of Office malware; disabling macros significantly decreases the attack surface of user workstations.

- **ensuring** 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.

- **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.

- **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.

- **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).

- **following** vendor-recommended guidelines for security settings on Windows, Mac, and Linux platforms.

- **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 detection and response solution, 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 several main stages that our solution is designed to circumvent:

Stage	Example InsightIDR / MDR Detection
Initial Access	User behavior analytics and other authentication-based detections to alert on unusual account activity.
Execution	Detection rules for common malware launching techniques used by RansomWare groups.
Privilege Escalation	Many detections for common privilege escalation techniques.
Defense Evasion	Detections for clearing of logs, disabling backups and shadow copies, and more.
Credential Access	Various detections around password spraying and brute force attack, credential dumping and more.
Discovery	Detections for tools used by attackers for network group and account enumeration. Also for discovering network trust relationships.
Lateral Movement	Detections for WMI, Powershell, etc and other common techniques used by attackers to perform remove command execution.
Command and Control	Coverage for common C2 tools like Cobalt Strike.
Impact	Detections for the deletion of backup files and shadow copies.

In addition to what we have listed above, the Rapid7 Threat Intelligence team is continuously coming up with new detections from our 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 Rapid7 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 are both 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

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 reducing the time it takes to contain, block, or reduce privileges to endpoints. As such, it is important to ensure you can access such orchestration platforms from unaffected workstations.

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

Final recommendation

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 all of our 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.

Rapid7 encourages 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 when responding to a ransomware scenario and be prepared to act if a ransomware attack was successful.