PHISHLABS
by HelpSystems

Ransomware Playbook

DEFENSE IN DEPTH STRATEGIES TO MINIMIZE IMPACT

A Digital Risk Protection Playbook

www.phishlabs.com

Ransomware operators are strategically targeting enterprises, disabling critical systems, and publishing stolen data. The average ransom demand has increased 144%[1] and victims are experiencing pressure to pay up or risk the fallout of confidential information being made public.

Businesses that fall prey to ransomware often feel helpless determining a solution post incident because the threat itself is in a constant state of evolution. Determining what action your organization should take in the wake of an attack is more than a binary decision, and must be approached in a comprehensive manner that adds layers of depth to existing security measures.

In this playbook, we address the trends driving the increase in ransomware attacks, best practices for protecting your organization, and the additional security strategies that should be applied, pre and post incident, to strengthen traditional security architectures.

To successfully minimize the impact of an attack, organizations should put into place a defense in depth approach that includes:

1. Identifying and mitigating attacks before they occur
2. Maintaining broad visibility into data leaks and threat actor activity
3. Preparing a plan of action in the event data is further compromised

Breaking Down the Consequences

Organizations that are affected by ransomware believe they are left with one of two choices: Refuse to meet ransom demands and risk the loss or the broadcasting of sensitive data or, pay the ransom and hazard it being released anyway. Other concerns that influence this decision include:

- Inability to operate
- Complete loss of data
- Reputational damage

Ultimately, enterprises experience the most pain when they are faced with compromise and lack options or a clear path of action. If unprepared, enterprises can find themselves in a situation in which the only viable option is to pay the ransom and hope the threat actor honors the agreement. Multiple ransomware actors and complex campaigns make this choice problematic however, as compromised data is likely to be leaked or sold regardless of whether the ransom is paid.

[1] Palo Alto

Visibility into the dark web, open web, and social media channels is essential to knowing whether stolen data has been leaked, where it is published, what the threat actor's intentions are with the data, and the extent of the disclosure. Improving and upgrading your organization's security posture will provide you this additional visibility and is best achieved by adding layers of protection that will minimize the risk of a ransomware attack ahead of time. If a breach does occur however, these layers will also provide an active defense, as well as options other than simply paying the ransom.

Factors Driving Increase

Ransomware attacks in North America Increased more than 104%[2] last year. Demands are significantly higher, and the pressure to pay is evident with payments met more than half the time. Industries of all types are being targeted, with critical services and infrastructure no longer immune to attack.

Trends that continue to drive these increases include:

- Double and Triple Extortion: As of Q4 2021, 84%[3] of ransomware attacks incorporate the threat to publish data, in addition to encrypting it. This tactic was first seen in 2019 with Maze operators, and has since exploded in popularity throughout the ransomware community as this move acts as an additional and strong incentive for victims to meet demands. Triple Extortion takes this tactic a step further by launching a Distributed Denial of Service (DDoS) if demands aren't met by the set deadline.

- Ransomware-as-a-Service (RaaS): A business model where ransomware groups sell access to specialized malware, empowering a broader set of threat actors the opportunity to engage in attack campaigns. This provides a low barrier to entry where inexperienced threat actors can participate in enterprise-wide infections leveraging enhanced and proven ransomware variants. RaaS models often allow affiliates access to how-to videos, 24/7 support, and dedicated dashboards.

- Initial Access Brokers (IABs): Facilitate Ransomware-as-a-Service by selling access to vulnerable networks. IABS compromise corporate systems by exploiting network vulnerabilities and deploying phishing attacks. IABs are opportunistic, and will sell various levels of network access to affiliates indiscriminately on dark marketplaces and forums.

[2] SonicWall
[3] Coveware

Taking a Modern, Defense-in-Depth Approach

The key to improving and upgrading your security posture from passive to active defense is to take a layered, defense-in-depth approach to combat the varying and complex ransomware threats that your business will face.

Enterprises should ensure they have the ability to:

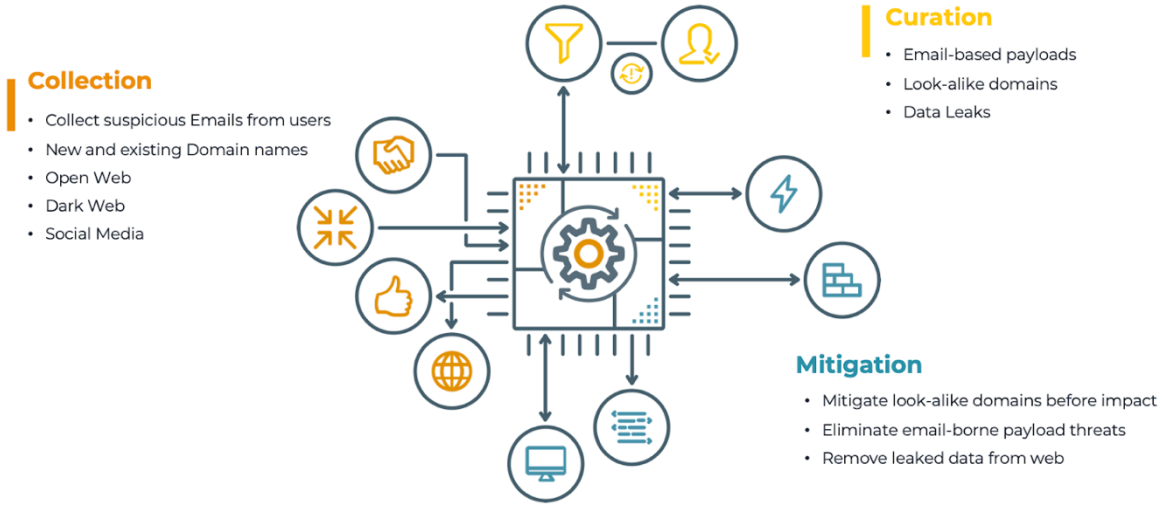
- Take action before hearing of stolen data from other sources
- Understand what data is online, the data's sensitivity, and mitigation options
- Assess existing security posture to determine if gaps exists and to ensure similar attacks do not occur

An organization will also better understand the impact of an attack by knowing what was compromised, how the attacker maintained access to the environment, and what actions were conducted inside the system.

Post incident, organizations should have visibility into what is happening with the stolen data, where it is located, and real-time updates on any new activity. With this information, the victim may prepare a plan of action, respond effectively to threatening behavior, monitor for additional leaks, and react quickly if necessary to minimize risk and further exposure. This will empower the organization to leverage resources and proactively plan rather than be caught off guard if data is published. It will also enable security teams to take action quickly to mitigate data and ensure further damage isn't done.

Best Practices

To effectively protect your business against ransomware, you need enhanced visibility across multiple channels to collect as much relevant data as possible, and be able to quickly sift through the noise and add critical context to that data to determine the true risks to your business. You should also have a mitigation strategy in place for on-going monitoring of the data in question, as well as action plans to enact takedown if possible.



Collection

Organizations should cast a wide net and pull data from as many targeted sources as possible including reported suspicious emails, new and existing domain names, and social media. Security teams should also monitor the open and dark web. These sources will provide the critical visibility needed to respond quickly and mitigate if necessary.

Email is the primary attack vector for ransomware. They compromise systems through business email compromise scams and phishing lures, impersonating trusted brands with look-alike and spoofed domains. Users can act as a valuable resource for enterprises and should undergo training that enhances their ability to identify suspicious emails and learn what to report.

Security teams should also collect data from Zone files, SSL certificate logs, and passive DNS to monitor new and existing domain registrations. Broad visibility across the domain landscape increases the speed of detection of domain data and enables the rapid identification of threats.

Finally, security teams should conduct continuous monitoring for leaked data across the Open Web, Dark Web, and Social Media. Visibility into these channels gives critical insight

into where leaked data is located, actor intentions, and what is currently being done with the data. This clarity allows teams to better respond to criminal actions and, if possible, have the content removed.

Curation

As data is collected, in-depth analysis must take place to add context. Cleaning the data will allow security teams to sift through the noise and determine whether they are interacting with threatening email-based payloads, look-alike domains, or leaked information.

Properly curating data is a multi-step process that leverages automated logic and machine-analyzed results that are then closely examined by specialists. Data curation should always be done through a combination of automated technical and expert human review and if possible, having dedicated experts that examine specific subsets of search results. This will greatly enhance curation speed and the ability to catch and mitigate threats.

Mitigation

Security teams can mitigate a ransomware attack through technical blockers, or through takedown.

Technical mitigation involves blocking indicators from employee-reported emails and preventing threat exposure within the organization. It also involves stopping user traffic to and from look-alike domains.

Takedown involves the complete removal of data or domains stood up to promote stolen information. This action can be taken by mitigating look-alike domains before impact (in the form of suspending domains or adding domains to security controls as threat indicators), eliminating email-borne payload threats, and removing leaked data from web and social sites.

While the removal of stolen data from the dark web poses a completely different set of challenges, continuous monitoring of the activity associated with the data provides businesses the ability to mitigate the threats if transactions occur and if the data is transferred to open web or social media repositories where legal mitigation can take place. This constant monitoring of activity also helps businesses maintain a plan of action to minimize risk associated with the threat.

A Fluid Process

Collection, curation, and mitigation can occur both pre and post incident.

Pre-incident

Ransomware delivery is a multi-step process, and the ransomware itself does not come from the email, but rather from droppers and former banking trojans that have enhanced functionality. If security teams prevent droppers from entering their network via email, they will thus prevent ransomware delivery. Security teams can monitor and block look-alike domains that are responsible for producing malicious emails through continuous monitoring of SSL certificate logs, DNS data, TLDs, and more. Implementing DMARC email authentication will also reduce the odds that your domain is spoofed, and prevent users from interacting with malicious messages in the first place.

Employees are a significant resource in preventing the delivery of these malicious emails, both by recognizing and reporting suspicious messages, links, and attachments to security teams. SOAR functionality can then provide an even broader layer of mitigation, by quarantining threats related to the threat indicators identified in the reported emails.

Post Incident

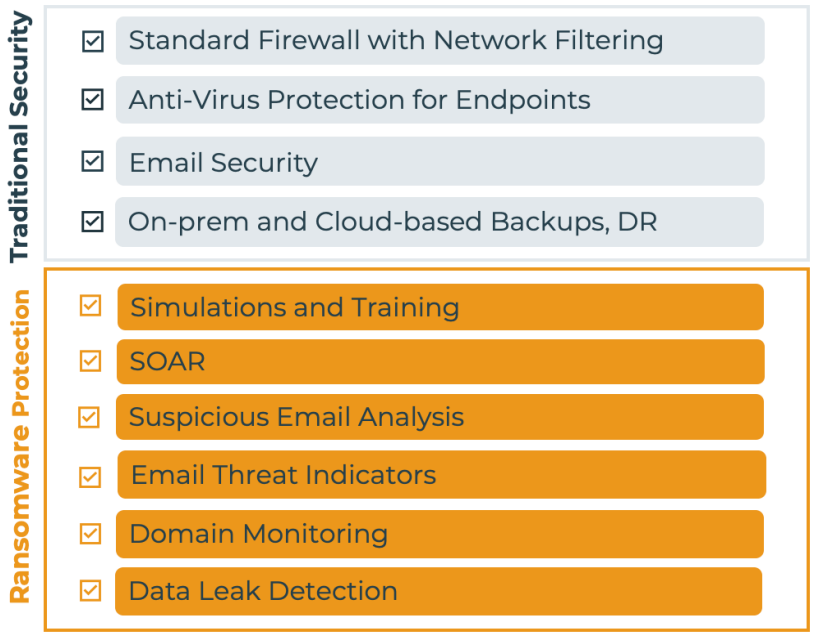
Security teams should constantly monitor new and existing domain registrations for notable changes such as content creation and mail exchanger records (MX records). A MX record specifies the mail server is responsible for accepting messages on behalf of a domain name and is a good indicator that the threat actor is, or plans to, distribute email.

Security teams should also continuously monitor for data leaks and mentions of their brand on the open web, dark web, and social media pre and post attack. The discovery of any additional leaks should be matched with threat actor personas for improved visibility and tracking. Forensics on the attack should be conducted as well to determine what the damage entailed, where the threat remains, and what weakness was compromised.

Conclusion

Today, organizations traditionally rely on a number of security solutions that have been based on years of industry best practices to defend against cyberattacks. This usually includes a firewall with network filtering, anti-virus for endpoints, an email security stack, and some form of traditional or cloud-based backup solution.

While these methods provide adequate security, threat actors still find ways around defenses to infect organizations with malicious malware, because traditional security methods provide no proactive visibility into external threats.



Taking a defense in depth approach to ransomware provides the additional and necessary protective overlays to traditional security solutions and helps businesses take a layered approach to combating ransomware. This includes monitoring for external threats before they can target your business, training employees to identify threatening emails that bypass security filters, and proactive data collection and analysis.

By following this playbook, security teams will have added layers of protection that will minimize the impact of a ransomware attack before it occurs. In the case that a breach does take place however, these actions should provide organizations with options that allow them to react and respond on their own terms, rather than simply paying the ransom.