Why Email Security Is So Valuable for Protecting Against Ransomware

Table of Contents

Executive Summary

It's easy to admit that email security is essential to protecting against ransomware when it's one of the three primary ways ransomware gets into an organization. Email is the one vector used to prey on human behavior to initiate an attack through the click of an attachment or link. However, it's important to appreciate how email plays a pivotal role in stopping ransomware attacks in their very earliest stages, which in turn prevents the rapid escalation of disruption and costs associated with a successful ransomware attack.

The following conceptual diagram shows how email security tools prevent, detect, and even facilitate response to phishing and other attacks that involve ransomware early on before the threats reach an employee's inbox.

Today's email security solutions prevent many ransomware attacks from occurring across organizations large and small.

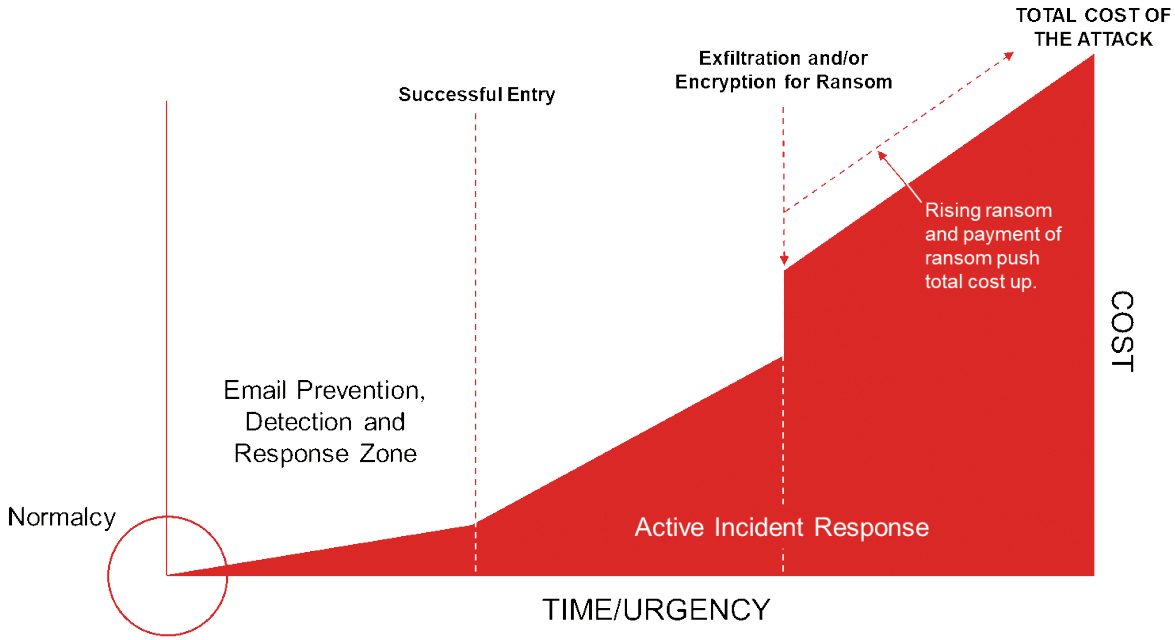


Figure 1: The cost of a ransomware attack over time.

Recommendations for Enhancing Email Security Against Ransomware

This section provides guidance and practical recommendations. But first, we look under the hood to better understand how email security solutions typically work and outline key capabilities and best practices to apply to the business environment.

Putting ransomware in the proper context of email security

Email security controls play their most important role in working to stop malicious inbound emails. At this stage, it's important to recognize that ransomware, in many respects, is the underlying payload (delivered in the form of an attachment or a link to a malicious download) while using the guise of phishing or spear phishing through email. For this reason, identifying incoming ransomware is as much about identifying phishing and impersonation characteristics as it is about inspecting file attachments and URLs embedded in emails. The following graphic shows the types of email threats and the building blocks of those threats.

Figure 2: Types of threats and their building blocks.

General guidance for enhancing email security

It's essential that everyone in the organization follows email safety best practices. Because stolen credentials can give threat actors (including ransomware gangs or individuals) access to send emails internally or externally, it makes complete sense that organizations adopt multi-factor authentication (MFA) for accessing the overall environment, networks, systems, and applications, including email.

Also, because no single security solution is 100% effective for email, it is important to enable logging for purposes of analysis and forensics.

Recommendations

1 Access

Ensure employees, including administrators, are using MFA. MFA helps mitigate the exploitation of stolen credentials and prevent account takeover—common objectives of email-based attacks.

2 Authentication

Disable legacy protocol authentication (e.g., POP3, IMAP, SMTP).

3 Logging for Analysis and Forensics

Turn on mailbox auditing, including access logging.

4 Integration With SIEM and SOAR Technologies

Email security solutions should be integrated with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities to allow for further analysis and correlation of data with other telemetry sources and automate response actions. This is where integrated platforms become very important—To counter multivector, multistage ransomware attacks, organizations need platform capabilities that tie together the security infrastructure while automating critical workflows across the various security capabilities.

Threat intelligence matters

The importance of threat intelligence in email security cannot be overstated or oversold. Ultimately, threat intelligence is what guides both the development of effective email security solutions and feeds the day-to-day ability of those solutions to prevent, detect, and respond to the latest email-based threats.

Recommendation

When evaluating email security solutions, organizations should keep the following in mind:

1. Does the vendor have a formal threat research team?
2. How many full-time researchers are part of that threat research team?
3. Has the research team deployed any sensor networks for data collection?
4. Does the vendor's research team have visibility into:
    - Email-based threats
    - The full life cycle of threats beyond email
    - Threats using other vectors and security domains outside of email
5. Ask the vendor to describe how research and analysis generated by this team leads to enhancements within their email security solutions.
6. How does the threat research team identify zero-day threats?
7. What is the feedback loop that exists for newly detected email-based attacks?

How email security solutions work to prevent, detect, and respond to attacks, including ransomware

At a high level, email security works to process incoming emails as efficiently as possible to determine at the earliest opportunity if an email is safe or malicious.

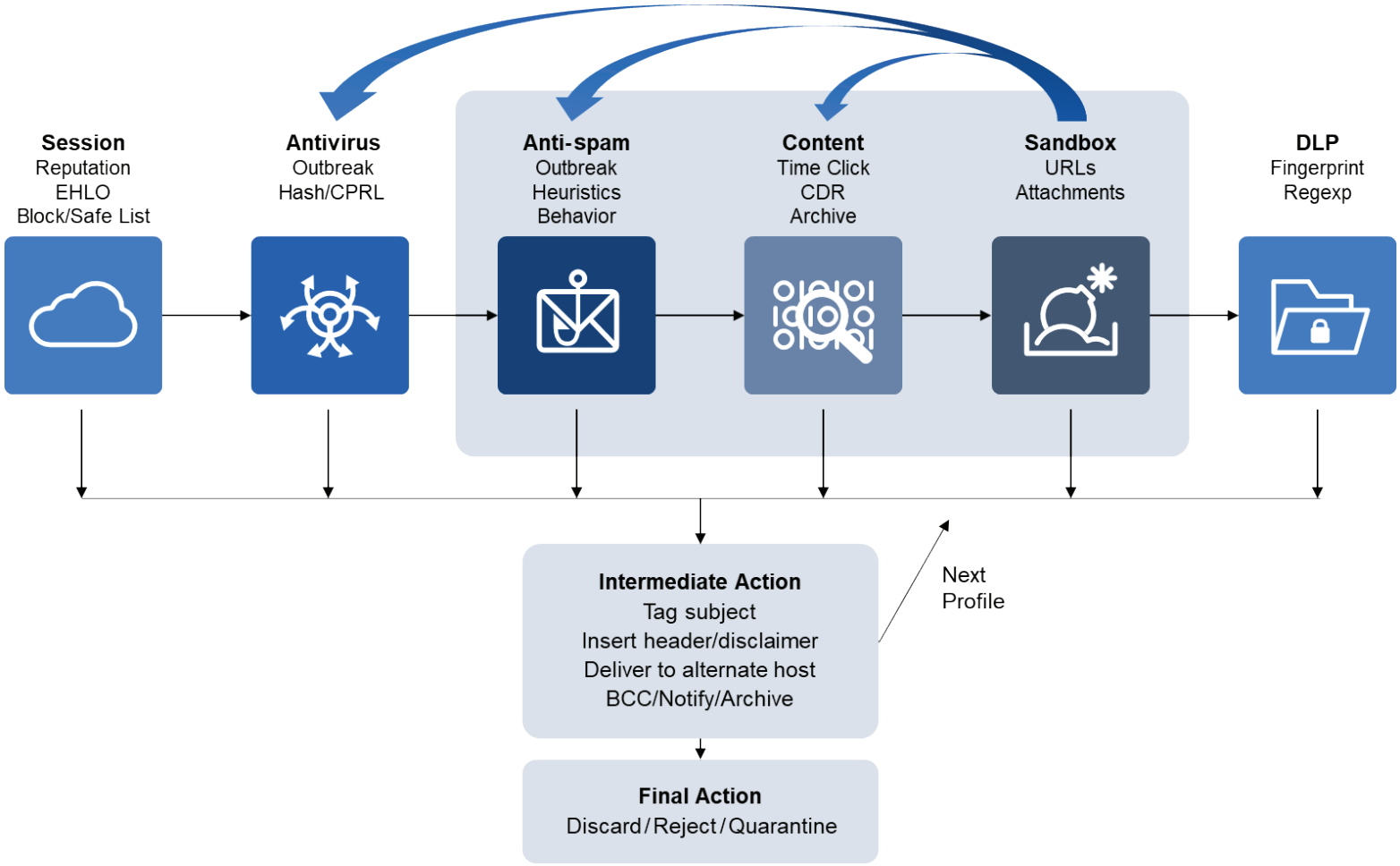


Figure 3: High-level view of how today's email security works.

Inbound Email Security Recommendations

When we go deeper, we see numerous verifications and checks, inspections, analyses, filtering, and actions associated with detecting malicious emails. We've highlighted a number of areas that organizations should consider.

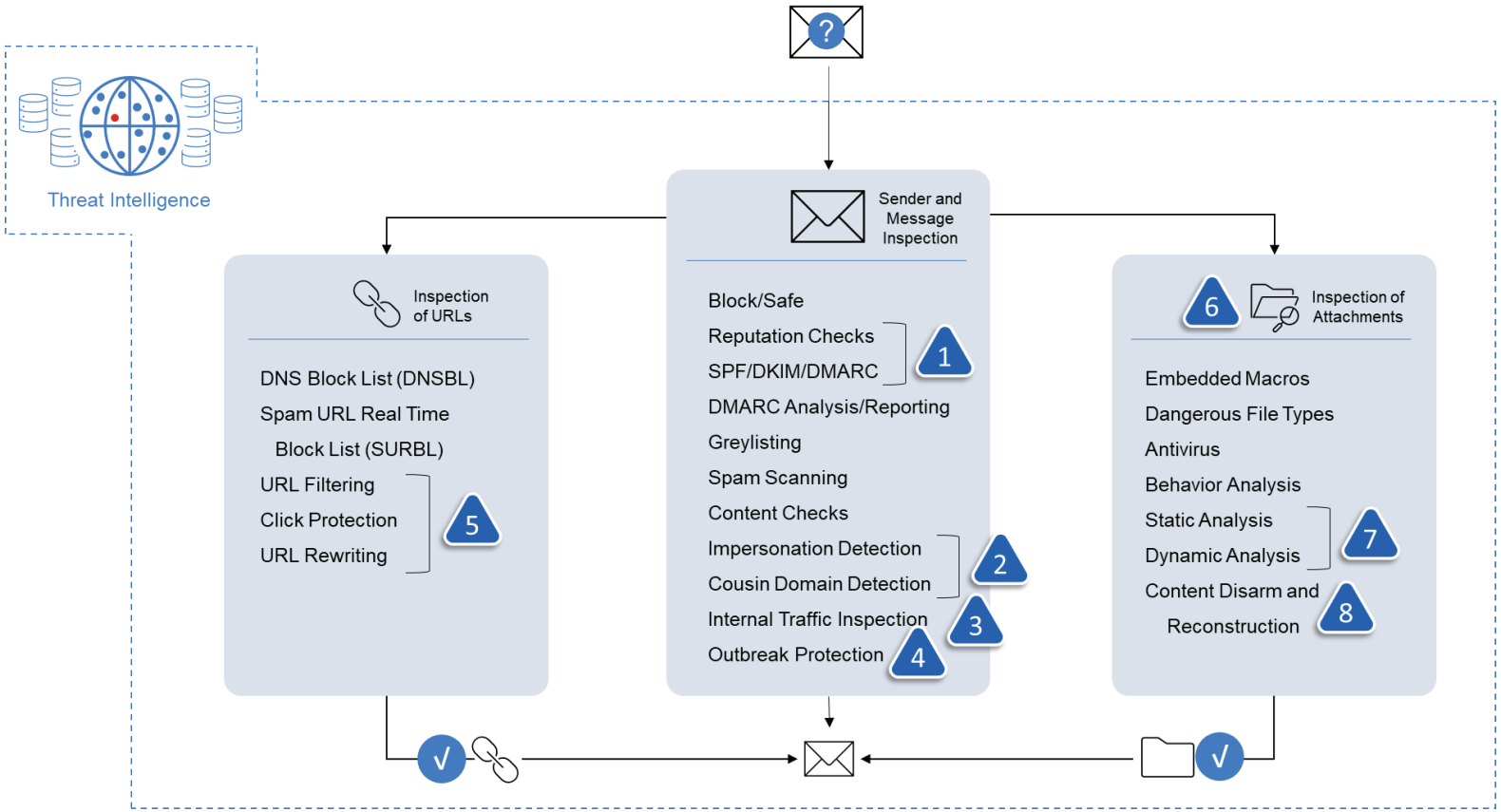


Figure 4: A deeper view of email security inspections and analyses.

Recommendations

1 Sender Reputation Checks and SPF/DKIM/DMARC

Review the various session, sender reputation, and threat detection checks that are performed on incoming emails.

It's important to understand what specific checks and inspections are performed on incoming emails to ensure the sender is legitimate. Be sure to enable Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) to counter spoofing by validating the authenticity of the sender.

2 Impersonation Detection and Cousin Domain Detection

According to Verizon's Data Breach Investigations Report 2021, "misrepresentation" increased 15x in the latest period under review.[1] This suggests that threat actors are spending more time and effort in crafting emails that have a higher likelihood of being opened and a link or file being clicked on. A smaller but very successful category of impersonation attacks is business email compromise (BEC) attacks, which resulted in $1.8 billion in losses to American businesses and government organizations in 2020.[2]

We recommend that all organizations should ensure that they have enabled capabilities for the detection of impersonation. These capabilities should include domain spoofing detection (through homoglyph and homograph detection), as domain spoofing could be tied to a spear-phishing (tied to ransomware) or BEC attack.

3 Internal Traffic Inspection

Organizations should adopt similar email security controls for internal-only traffic as they do for incoming emails from the internet. Organizations can no longer trust that internal email traffic is somehow immune to the spreading of threats, including ransomware and associated risk.

4 Outbreak Protection

Outbreak protection works to prevent broader outbreaks when an email has been identified as potentially suspicious. This enables broader, automated protection in minutes to prevent any spread from messages deemed the same or similar. Outbreak protection just makes sense for organizations to have a proactive safeguard against malicious emails that may have been sent to numerous recipients. IT and IT security practitioners should look for this feature within their email security solution and ensure it's enabled.

5 Click Protection, URL Rewriting, and URL Filtering

Threat actors increasingly rely on URLs embedded in emails to lead unsuspecting victims to a malicious site or trigger an unexpected download.

Investigate and enable link analysis capabilities like click protection (analyzes the reputation of the URL at the time of click) and URL rewriting (rewrites a URL to subsequently detect when a URL has been altered later after the first scan). URL filtering allows one to choose which URL categories in the email body to check, rewrite, or block, which can then be used in antispam/threat profiles.

Additionally, for organizations particularly susceptible to risk that may be introduced through employees browsing the internet, IT and IT security teams should investigate browser isolation solutions for potential adoption.

6 Advanced Sandbox Inspection of Attachments

Today, our guidance is that all organizations should utilize advanced capabilities such as sandboxing to further analyze file attachments (and links within files) for indications that a given file is malicious. These tools are especially well-suited for attachments that have not been encountered before. Today, leveraged models allow organizations to utilize these analysis tools integrated with their email security solutions at relatively low additional cost.

7 Static and Dynamic Analysis

Related to item 6 above, IT and security teams should ask about the specific capabilities of the underlying sandbox technology offered by vendors. This includes the types of analysis performed, such as static and dynamic analysis, code analysis, analysis of links within files, and links embedded in email content. This also includes understanding whether this technology is homegrown or is OEMed from a separate vendor.

8 Content Disarm and Reconstruction (CDR)

Utilize CDR. CDR allows the email security solution to remove any active content in email files, such as hyperlinks, embedded media, JavaScript, and macros, without affecting the integrity of its textual content. It allows network administrators to protect their users from malicious document files. The original copies can also be obtained in the event of a false positive.

Outbound Email Security Recommendations

Email security solutions can also play a role in preventing the successful exfiltration of sensitive data sent via email tied to a ransomware campaign, preventing the inadvertent sending of malware (including ransomware) by an employee, or mitigate the abuse of an email account as a result of a takeover. Typical solutions today integrate data loss prevention (DLP) capabilities.

Recommendations

1 Data Loss Prevention

Spend the time to research the capabilities of an integrated DLP solution thoroughly.

- Perform an internal assessment (data classification) to identify sensitive file and data types stored, processed, and handled across the organization. Be sure to identify file types and data formats unique to your organization.
- Catalog and fingerprint directories and files.
- Enable relevant pre-made dictionaries the vendor has made available.
- Create and customize dictionaries to make them purpose-suited for the organization's needs.
- Perform testing to ensure the DLP capabilities in the email security solution are working properly to detect sensitive file and data types sent in email.

Take the following steps to prevent or reduce the impact of an email account takeover:

2

Enable MFA

As mentioned earlier, MFA can play a key role in preventing threat actors from exploiting stolen credentials to send malicious emails within and outside of your organization.

3

Inspect URLs

We recommend all organizations enable URL inspection capabilities, including click protection, up to and including the use of sandbox analysis for determining whether a URL embedded within an email poses risk to an organization.

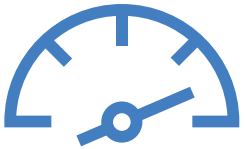
4

File/Attachment Inspection

Utilize antivirus, content inspection, and sandbox analysis for file attachments to guard against the sending of malicious files in outgoing emails.

Validating the Efficacy of Email Security Solutions

Even with all of the various practices cited above, it's essential to rise above the specific controls in place to understand the true efficacy of cloud-native controls or third-party secure email solutions. In cybersecurity, this isn't always easy to find out. There aren't always benchmarks or independent testing to give a clear idea of how one solution works versus another.



Recommendations

1 Validating Email Security Efficacy Through Independent Testing

The good news is that there are a few different resources available to determine the actual efficacy of most email security solutions in the market today.

- SE Labs – Based in the United Kingdom, SE Labs likely performs one of the most exhaustive comparative testing programs for email security solutions, including Microsoft Exchange Online Protection (EOP) and Microsoft 365 Defender and Google Workspace, of any vendor.
- ICSA Labs – ICSA Labs performs testing of advanced threat protection (ATP) solutions generally specific to each vendor.
- Virus Bulletin – Virus Bulletin performs specific spam capture, malicious email detection, and anti-malware protection testing of vendor solutions.

2 When Using Microsoft 365 Exchange or Google Workspace Native Security Tools

In SE Labs testing, they found that Microsoft 365 EOP and Microsoft 365 Defender performed poorly, receiving a Total Accuracy rating of 28% and 29%, respectively, and rated as "C" overall.[3] For comparison, Fortinet FortiMail achieved a 90% Total Accuracy rating and a "AAA" rating in the same testing. Google G-Suite Business posted a Total Accuracy rating of 39%, receiving a "B" rating overall. Google's Enterprise version posted a slightly higher Total Accuracy rating at 42%, earning it an "A."

Because of the risk posed by today's ransomware attacks, organizations need to use alternate or complementary secure email services when using these platforms. Engage a third party to address known gaps in the efficacy of Microsoft 365 and Google Workspace native security controls.

The increase in ransomware attacks over the past 18 months is having a very real impact to organizations across the world with no industry immune. With one in three ransomware attacks originating via email, email security plays a critical role in stopping many ransomware attacks. IT and IT security teams can take a number of steps to enhance the effectiveness of their email security solutions against ransomware, including adopting a robust sender and recipient verification scheme as well as advanced detection capabilities, such as sandboxing, URL click analysis, and impersonation analysis, to name a few. In addition, organizations should do their due diligence by reviewing available independence testing to validate the likely efficacy of solutions.

[1] "2021 Data Breach Investigations Report," Verizon, 2021.

[2] "Internet Crime Report 2020," U.S. Federal Bureau of Investigation IC3," 2021.

[3] "Email Security Services Protection," SE Labs, Spring 2020.

FORTINET®

www.fortinet.com

October 27, 2021 7:53 AM

1292704-0-0-EN