SONICWALL

EXECUTIVE BRIEF: WHY ADVANCED THREATS DEMAND ADVANCED EMAIL SECURITY

Ransomware and unknown threats make email security more crucial than ever

Abstract

In today's hyper-connected world, email-based communications are not just commonplace – they have become a fundamental cornerstone for effectively conducting business, with the total volume of worldwide emails sent per day projected to increase by at least 5% every year. Given its ubiquitous nature, email is a critical vector that an organization must protect.

Email usage continues to increase

Regardless of the proliferation of text and social media, email communication is still growing strong. According to a recent study by the Radicati Group, the total volume of worldwide emails sent and received reached 205 billion per day, with this volume projected to increase by at least 5% every year.[1] And, this fact is not lost upon hackers, who are constantly seeking opportunities to exploit organizations.

1 The Radicati Group, Inc., Email Statistics Report, 2015-2019

Anatomy of an email attack:

- A CFO gets an email from the CEO authorizing an emergency fund transfer. But the email is actually from a cybercriminal
- An employee with administrative rights to key systems receives an urgent email from IT to update their network password. They actually disclose their password to cybercriminals.
- An employee receives an email to read an important attachment about their benefits provider. When they open the attachment, they unknowingly activate hidden Trojan malware.

E-mail threats organizations face today

Emails offer hackers a vehicle to deliver a variety of vulnerabilities to an organization. Some of the more common email-borne threats include:

- **Ransomware** – one particularly nefarious malware variant is ransomware. Once the email attachment is activated, the code embeds itself on a network and ransomware typically encrypts or locks critical files and systems. The hackers then coerce the organization to pay an extortion fee in order to have the files or systems un-encrypted or unlocked. Email is the preferred vehicle to deliver ransomware either through infected attachments or malicious URLs.
- **Spear Phishing / Whaling** – in this variant of phishing, key IT/networking individuals or company execs are targeted using malware-laced emails appearing to come from a trusted source, in efforts to gain access to internal systems & data. Over 90% of cyber-attacks start with a successful phishing campaign.[1]
- **Business Email Compromise / CEO Fraud / Impostor email** – Over the past few years, Business Email Compromise (BEC) schemes have caused at least $5.3 billion in total losses to approximately 22,000 enterprises around the world, according to the latest figures from the FBI.[2] The FBI defines Business Email Compromise as a sophisticated email scam that targets businesses working with foreign partners that regularly perform wire transfer payments.
- **Phishing** – this common hacker tactic utilizes emails with embedded links to hacker sites. When gullible users visit these sites, they're prompted to enter PII (Personably Identifiable Information) that is in turn used to steal identities, compromise corporate data, or access other critical systems.
- **Malware** – email is one of the top delivery mechanisms to distribute known & unknown malware, which are typically embedded into email attachments in hopes that the attachment will be opened or downloaded onto a computer or network, thereby allowing hackers to gain access to resources, steal data, or crash systems.
- **Spam** – emails are used to deliver spam or unsolicited messages, which can clog inboxes and network resources, diminish businesses productivity, and increase operational costs.
- **Outbound Email Hijacking** – corporations are also subject to corporate policies and government regulations, which hold businesses accountable for their outgoing emails and ensuring they protect their customer's PII. Zombie attacks and IP hi-jacking can disseminate customer PII, ruining the reputation of a business.

Conclusion

Emails communications are essential to organizations today, something hackers are keenly aware of. Given today's sophisticated and targeted attacks, it's paramount that organizations deploy a multi-layered security solution that includes dedicated advanced threat protection for email. To effectively combat today's emerging threats, organizations are well-advised to implement a next-generation email security management solution that provides real-time breach prevention capabilities.

To learn more about ways to protect your organization's emails, read our solutions brief and discover what your next-gen email security needs to stop advanced threats.

1 www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2 www.ic3.gov/media/2016/160614.aspx

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com