Comprehensive Security in The Age of Evolving Email-Borne Threats

White Paper

Introduction

Email is the most commonly exploited vector for cyber attacks. If that sounds familiar, it should. It's been true for years, and likely will be true for years to come.

But just because that bare fact hasn't changed, doesn't mean that the nature of the threat has remained static. In fact, methods and payloads used in email-borne attacks have been evolving rapidly—and this means that your defenses against such attacks need to evolve as well.

Modern email threats include targeted attacks that entice an unsuspecting user to click on a malicious link, download an infected attachment, provide credentials, or leak other forms of confidential data that can be used to propagate the attack chain.

These types of attacks range in sophistication, severity, and impact. From spam campaigns that deliver malicious payloads to large number of users, to domain-spoofing, phishing, and highly customized spear phishing and business fraud, the range of methods used to bypass traditional security is increasing rapidly.

Depending on the nature of the attack, victims incur increasingly significant financial losses and business damage. Protecting against these types of attacks requires a comprehensive strategy that goes beyond traditional signature-matching.

Payloads

The payloads that malicious emails can deliver include:

- Malware of all kinds, including the advanced, evasive ransomware variants that have been much in the news lately
- Falsified URLs or messages that lead users to enter their credentials, which attackers can later use to access sensitive data or gather further intelligence on target organizations
- Purely social, non-technical payloads, such as an impersonated CEO urgently requesting a large wire transfer

As a general rule, the less technical and more social payloads are delivered primarily by the most targeted types of email attacks. Less targeted, spam-type attacks are best suited to malware payloads, either as attachments or through links to compromised or fraudulent websites. However, malware may also be propagated by more targeted email attack types.

Volumetric Spam

Volumetric spam campaigns are a very common way for ransomware to be propagated. These attacks generate email that appears to come from legitimate, broad-based sources like financial institutions, government organizations, or service/utility providers. They can deliver harmful payloads through these messages to many users at once, enticing them to unknowingly install devastating malware. Recent ransomware attacks including Petya/NotPetya, Cerber, and others were delivered through this mechanism.

Phishing

Unlike volumetric spam, phishing emails are constructed to deceive a specific class of users and may rely on data that be gathered about these users through social media and other channels. They are designed to trick users into clicking on a link or attachment, which may then take them to a fake website that asks them to enter confidential information, or it may simply install malware such as ransomware or other advanced threats.

The deception mechanisms used in phishing attacks include sender impersonation, domain impersonation, typo-squatting, and more. Common phishing emails usually hide malicious links in the message body, contain seemingly legitimate attachments, etc. These attacks rely on users being distracted, or unaware that such emails can harbor threats.

Spear Phishing, Business Email Compromise, and Fraud

Spear phishing uses the same basic strategy as phishing, but takes it to a new level. Attackers perform extensive, in-depth research about specific target organizations and individuals, using social media, publicly available information, and even on-site surveillance. They then use the intelligence they've collected to craft a highly convincing message that is very unlikely to raise the suspicions of even the most security-aware user. The attackers may impersonate or steal credentials of highly visible employees (CEO, CFO, HR, Finance) and craft personalized emails to specific individuals they interact with.

These emails often contain no apparent distinguishing characteristics (like links or attachments) or obviously suspicious meta-data (like IP reputation, domain reputation), which means that they may be immune to traditional gateway-based detection techniques or complex whitelist/blacklist rules. Organizations and individuals have lost large sums of money because of these types of attacks.

Domain Spoofing

Domain spoofing is a technique that is often used to support phishing and spear phishing attacks. It uses technical means to send an email from a particular company's domain (such as barracuda.com), without using a company sanctioned mail system (such as Outlook). Domain spoofing is typically used to confuse the recipient into believing they got an email from the company's domain, to conduct a spear phishing attack or steal personal information. In addition to impacting the recipient, domain spoofing can also damage the reputation of the company that is being spoofed.

Even if corporate email is secure, users can still fall victim to threats like malicious links and harmful downloads that are transmitted over personal email, social media, messaging platforms, and more.

Effective Protection Against Evolved Email Attacks

Comprehensive protection against these types of attacks requires a layered security strategy that can stop spam, phishing emails, malicious links, and malicious attachments before they are delivered. It must detect and eliminate advanced spear-phishing emails, prevent domain spoofing, and protect users from malicious internet content. It should also actively train users to identify potentially malicious emails and respond appropriately.

Many solutions only address a subset of these requirements. This leads to organizations compromising on their security posture or dealing with the cost and complexity of piecing together multiple solutions.

Barracuda Security Solutions

Barracuda offers the industry's most comprehensive security suite, to elegantly and simply protect your network, data, and users against fast-evolving email-borne attacks.

Barracuda Essentials

Barracuda Essentials provides email security at the gateway and prevents malicious emails from entering your mail server, whether you host email on-premises or in the cloud. It blocks spam, viruses, and both known and unknown (zero-day) malware.

- Combines anti-phishing technologies including IP Reputation Analysis, Sender Authentication, Domain Verification, Intent Analysis, and Anti-Fraud Intelligence, along with granular policy controls
- Scans and rewrites URLs in email messages to redirect malformed, suspicious, or typo-squatted domains to a sandbox at time of click
- Provides DMARC, DKIM, and SPF authentication to detect domain-spoofing attempts
- Leverages Barracuda Advanced Threat Protection—a multi-layer, cloud-based filtering system to detect and filter malware, including a CPU-emulation sandbox environment to spot zero-day threats

Barracuda Sentinel

Barracuda Sentinel employs advanced artificial intelligence and big-data analytics to spot and block spear phishing and cyber fraud attacks in real time. Delivered as a cloud service, Barracuda Sentinel combines a powerful artificial intelligence engine, domain fraud visibility using DMARC, and anti-fraud training into a comprehensive solution that protects people, businesses, and brands from spear phishing, impersonation attempts, business email compromise (BEC), cyber fraud, and domain spoofing.

Barracuda Network Security

Barracuda NextGen Firewalls and Barracuda Web Security Gateways include URL filtering and Barracuda Advanced Threat Protection to ensure that users are always protected from malicious internet content including harmful links, advanced malware, phone-home spyware, and other intrusions. This provides an additional layer of security, ensuring that users are always safe even if they are exposed to these attacks outside of corporate email channels.

Conclusion

Cyber criminals never rest in their quest to design innovative techniques to bypass security and steal or extort your money. Fortunately, the capabilities of security offerings continue to evolve as well. Today's email security must extend seamless, comprehensive protection across cloud, hybrid, and on-premises environments. It must efficiently implement advanced technical strategies without introducing lag or adding administrative overhead. And it must provide effective security-awareness training that helps transform your userbase into a powerful security layer in its own right

Barracuda Essentials, with Barracuda Advanced Threat Protection and Barracuda Sentinel together meet these requirements and effectively defend your organization, your data, your users, and your brand against the potentially devastating consequences of today's advanced, highly targeted threats.

About Barracuda Networks

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com