Barracuda

NetatWork

Comprehensive Email Protection

White Paper

Executive Summary

Email continues to be the single biggest source of cyber-attacks globally. A recent survey* estimated that in 2017, 74% of threats initially entered organizations via email.

** 2017 Threat Landscape Survey: Users on the Front Line, conducted by the SANS Analyst Program.*

74% of threats enter organizations through email.

The traditional approach to email security blocks spam and malware at the gateway before it enters an organization and enforces policy controls at this point. This approach is still necessary but is not able to secure against advanced email threats such as spear phishing attacks, account takeover, business fraud and data loss.

Barracuda Email Protection provides a comprehensive solution that secures your entire email infrastructure. The multi-layered approach covers all threat vectors by securing the email gateway, protecting your stored email data, inoculating mailboxes against targeted threats, and training users on how to identify and defend against cyber-attacks.

The Evolving Landscape of Email Threats

Email attacks started as simple volume campaigns delivering spam and malware, and we still see these today, but threats have evolved rapidly since then to employ an increasingly sophisticated range of techniques.

Today's more damaging attacks may involve highly targeted campaigns which leverage social engineering, account takeover, spoofing and other techniques to steal user credentials, and to defraud organizations of large sums of money.

In addition, we are now seeing email attacks entering organizations via personal email accounts and unified inboxes, as well as widespread use of advanced threats such as ransomware.

Spear Phishing and Targeted Threats

Over half a million phishing attacks were estimated in the first six months of 2017.

- Anti-Phishing Working Group, 2017

The most damaging email attacks today are often delivered as spear phishing emails with zero payload. These are customized to target specific individuals within an organization, appear to come from a reputable source, and usually include an urgent call to action that can range from providing credentials to transferring money.

These emails don't display any obvious characteristics (such as infected attachments or suspicious URLs) that would flag their malicious intent to gateway security controls.

Other targeted phishing emails impersonate commonly used services such as Outlook, DocuSign, Dropbox and others, and ask employees to click on a zero-day link. These emails typically originate from compromised accounts that have a high reputation and are not intercepted by traditional security gateways.

Account Takeover and Business Fraud

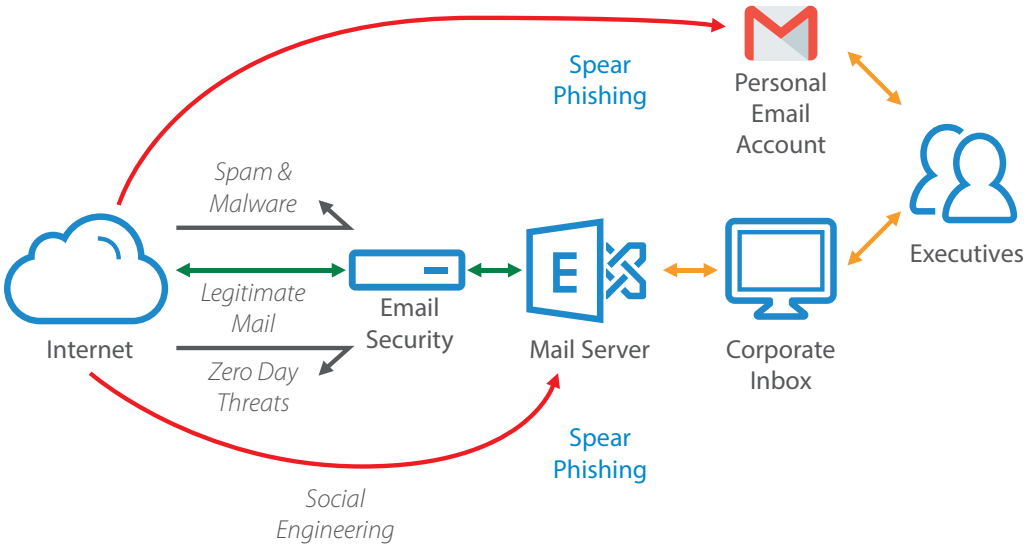
In these attacks, social engineering or other intrusion techniques are first used to obtain the credentials of email accounts for targeted individuals. Attackers then use these compromised credentials to send emails to other internal employees, or use the accounts to launch additional external phishing campaigns. These attacks are very hard to stop with traditional gateways because they emanate from internal mailboxes.

Similarly, attackers are increasingly spoofing domains of corporations and public institutions, and using their high reputation to launch phishing and spam campaigns, as well as tricking the employees of these organizations to commit fraudulent wire transfers.

Advanced Malware

This is designed to circumvent security controls and then exploit platform and system level vulnerabilities, allowing it to infiltrate networks, exfiltrate sensitive information, and in some cases encrypt business critical data.

The polymorphic nature of zero-hour malware makes it difficult to detect using traditional signature-based anti-virus techniques.



Spear phishing attacks evade traditional gateway defences.

Modern Email Infrastructures Need Layered Security

Traditional email security solutions are good at preventing spam and emails containing malicious software and attachments from reaching the email server, but they fail to provide sufficient protection against socially-engineered and internal attacks. Organizations now require a layered approach that goes beyond simply blocking spam and viruses, and provides these additional capabilities:

Inbound protection from advanced threats

Incoming attacks with zero-hour malware should be blocked and prevented from entering the organization, and users should be protected from malicious URLs embedded within messages and attachments.

Outbound protection to prevent data leakage

Outbound email should be monitored to prevent the leakage of sensitive content, and messages encrypted if needed to secure sensitive communications.

Secure archiving for compliance and e-discovery

Archiving is a key aspect of securing the email infrastructure. An accurate record of all email communications must be captured and retained securely to ensure compliance with regulatory requirements, and to facilitate a quick and easy response to e-discovery requests on historical data.

Business and Email Continuity

Organizations should be able to restore production email data quickly and accurately in the event of accidental deletion or data loss. In addition, users should be able continue email communications if their primary email server becomes temporarily unavailable.

Spear Phishing and Business Fraud protection

Zero-payload spear phishing emails should be proactively detected, and quarantined from email inboxes, and attempts to compromise user email accounts should be prevented. Organizations should also be able to identify and protect against domain spoofing and business fraud activities.

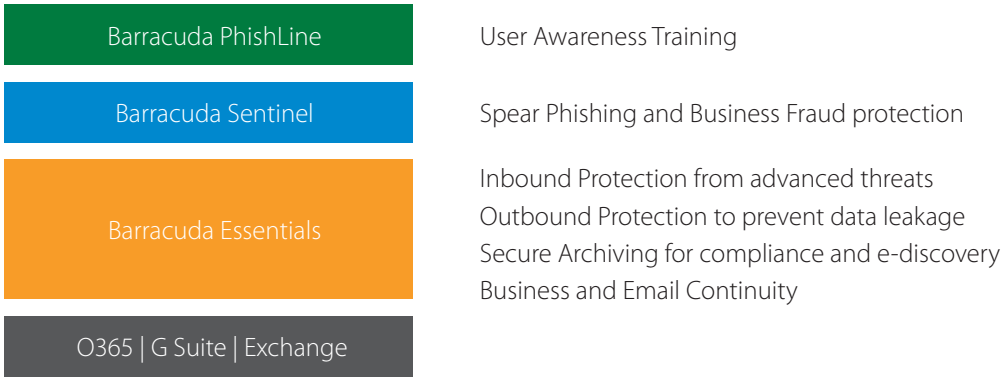
User Awareness Training

End users should be enabled as the last line of defense against spear phishing and other targeted attacks, by providing them with tools and training to proactively identify and avoid these threats.

Barracuda Email Protection

Barracuda provides the most comprehensive, cloud-based, multi-layered solution to secure your entire email infrastructure.

Modern Email Infrastructures need layered protection.



Barracuda Essentials

Inbound and outbound email protection, secure archiving, and business and email continuity.

- Inbound email filtering protects against spam, viruses and phishing attacks, and enforces policy controls.
- Advanced Threat Protection leverages Barracuda's global threat intelligence network to block incoming zero-hour email attacks.
- Link protection sanitizes malicious URLS embedded in emails and attachments.
- Email Continuity Service ensures users can continue working through email server and service disruptions.
- Outbound email filtering prevents data leakage and automatically encrypts sensitive data.
- Cloud Archiving Service provides comprehensive email archiving, with granular retention policies ensuring compliance, e-discovery searches and mobile access for end users.
- Cloud-to-Cloud Backup maintains business continuity by protecting email as well as OneDrive and SharePoint data against accidental or malicious deletion and ransomware attacks.

Barracuda Sentinel

Spear Phishing and Business Fraud Protection.

- AI-based real time identification and protection against targeted spear phishing attacks.
- Detection, prevention and remediation of email account takeover.
- DMARC Reporting and Management guards against domain spoofing and business fraud activities.
- API-level integration with Office 365 provides complete automation of setup and operation.

Barracuda PhishLine

Security Awareness Assessment, Training and Simulation.

- Multi-Vector and Multi-Variable attack simulations to train users and turn them into a strong last line of defense against email threats.
- Customizable simulation scenarios including pre-built email templates and landing pages.
- Rich, elegant and engaging training content including quizzes and risk assessment surveys, in easy to use online catalogs.
- Granular visibility and measurement tools to manage risk levels based on performance and feedback.

Conclusion

Providing a comprehensive solution to defend against the full range of email threats that organizations are now facing is a complex and rapidly evolving multi-dimensional challenge.

Barracuda's suite of purpose-built security solutions builds on years of experience and leverages a global network to provide an easy, economical, scalable, and powerful way for organizations to address this challenge.

"We found Barracuda Essentials to be the perfect solution for our customers using Exchange or Office 365. Being able to prevent problems before they happen saves our customers and us more time to focus on what really matters."

- David Rolleri, Systems Engineer, INTERDEV Managed Security

Barracuda Email Protection:

- Barracuda Essentials

- Barracuda Sentinel

- Barracuda PhishLine

NetatWork
t: 800.719.3307
e: info@netatwork.com
w: netatwork.com