New Report Finds Emails Containing Dangerous Attachments Up More Than 25 Percent

December 12, 2018

Latest ESRA Detected Incumbent Email Security Systems are Leaving Organizations Vulnerable to Dangerous Attachments, Malware, Impersonation Attacks and Malicious URLs

LEXINGTON, Mass., Dec. 12, 2018 (GLOBE NEWSWIRE) -- **Mimecast Limited** (NASDAQ: MIME), a leading email and data security company, today announced the availability of its latest quarterly Email Security Risk Assessment (ESRA), an aggregated report of tests that measure the efficacy of widely used email security systems.* This quarter's assessment found that these email security systems are missing more than 25 percent of emails containing dangerous attachments in comparison to last quarter's findings.

Typically dangerous file types are rarely sent via email for legitimate purposes, such as: .jsp, .exe, .dll and .src, and can be used to facilitate an attack. Detailed Mimecast ESRAs help organizations better understand what types of email-borne threats are getting through their current security system. Every quarter Mimecast aggregates the results of individual ESRA tests and reports to the industry its findings. To date Mimecast has inspected more than 180 million emails that were deemed "safe" from these incumbent systems. Within these emails, the tests found 16,581 emails that contained dangerous file types.

The report also found 21,183,014 spam emails, 17,403 malware attachments, 42,350 impersonation attacks and 205,363 malicious URLS, all missed by these incumbent providers and delivered to users' inboxes. This latest report concludes that an aggregate 12% of all secured and filtered email were unwanted emails and thus were false negatives.

"Mimecast has seen an increase in security efficacy versus legacy vendors along with detailed information on the proliferation of threats of all types. The ESRA provides deep insights for our customers on the types of attacks threatening their business," says Lindsay Jack, security service director at Mimecast. "Attacks we are seeing include key executives being targeted with cloud storage services exploits, impersonation attacks targeting legal, finance and administrative assistance as well as social engineering attacks against the C-suite. Mimecast helps organizations understand how they compare with other organizations in their geography or industry vertical. Additionally, these reports provide insights on the rise of new types of malware and key trends in malicious email campaigns."

"Cybercriminals are constantly adapting their email-based attacks, looking for new ways to bypass security solutions that rely too heavily on reputation-based detection or file signature matches. This quarter we saw a particularly large jump in emails containing dangerous file types.," said Matthew Gardiner, cybersecurity strategist at Mimecast. "Mimecast uses multiple layers and types of detection engines, combined with high performance analytics, a diverse set of threat intelligence sources, and computer aided human analysis to identify and stop unsafe emails from getting into our customers' inboxes."

Additional Resources:

- Take a look at the Email Security Risk Assessment infographic
- Read latest blog

About Mimecast
Mimecast (NASDAQ: MIME) is a cloud cybersecurity and resilience provider for IT service organizations and thousands of customers worldwide. Well known for innovating security solutions that make email profoundly safer for business, Mimecast's expanded suite enables a comprehensive cyber resilience strategy delivered via an integrated, easy to implement, cloud platform built on Mime|OS. www.mimecast.com

Mimecast Social Media Resources
LinkedIn: **Mimecast**
Facebook: **Mimecast**
Twitter: **@Mimecast**
Blog: **Cyber Resilience Insights**

Press Contact
Alison Raymond Walsh | Press@Mimecast.com | 617-393-7126

Investor Contact
Robert Sanders | Investors@Mimecast.com | 617-393-7074

Source: Mimecast Limited