

mimecast[®]

EMAIL SECURITY RISK ASSESSMENT

Quarterly Report | March 2019

This is an aggregate report of Email Security Risk Assessment tests showing the number and type of unwanted and dangerous emails missed by incumbent email security systems.*

EMAIL SECURITY RISK ASSESSMENT

Quarterly Report | March 2019

Many organizations think their current email security systems are up to the task of protecting them from phishing. Unfortunately many email security systems fall short and do not keep their organizations safe. The reality is the entire industry needs to work toward a higher standard of email security. The proof is in the numbers. Mimecast is establishing a standard of transparency for organizations and raising the bar for all security vendors.

In working with our more than 30,000 customers, Mimecast has observed firsthand that not all email security systems perform equally well. But, until we started conducting these tests we lacked the comparative data to prove our perceptions. In order to address this head-on, Mimecast has been continually executing Email Security Risk Assessments (ESRAs) for the past two years.

The Mimecast ESRA has three goals:

1. To test the Mimecast Secure Email Gateway service against an individual organization's incumbent email security system. We do this to help the organization understand the relative efficacy of the security systems and to see the number, type and severity of email-borne threats that are currently getting into their organization.
2. To inform the security industry with hard data on the effectiveness of various commonly-deployed email security systems.
3. To inform the security industry regarding the number, type and severity of email-borne threats that are being actively used in attacks.

What is a Mimecast ESRA?

Mimecast uses our cloud-based Secure Email Gateway service to assess the effectiveness of legacy email security systems. An ESRA test passively inspects emails that have been passed by the incumbent email security system and received by the organization's email management system. In an ESRA the Mimecast service re-inspects the emails deemed safe by the incumbent email security system and looks for false negatives, such as spam, malicious attachments and URLs, as well as impersonation attempts.

What We Found to Date

The results we've uncovered are concerning. Email attacks ranging from opportunistic spam to highly targeted impersonation attacks are getting through incumbent email security systems both in large number and variety. Let's evaluate the scope of the problem by digging into the aggregated test data that is presented in Figure 1.

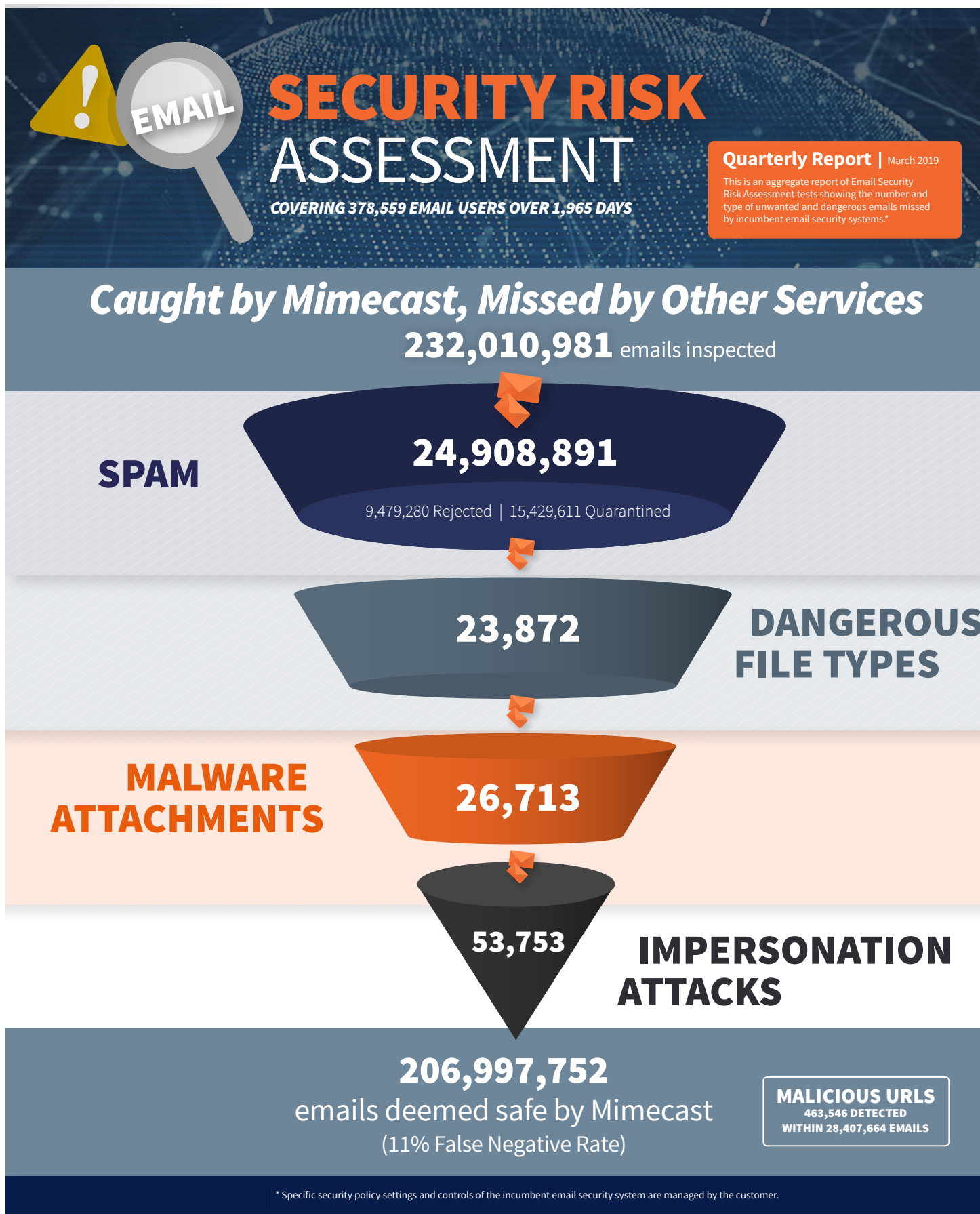


Figure 1 – Aggregated Funnel of ESRA Test Results Completed to Date

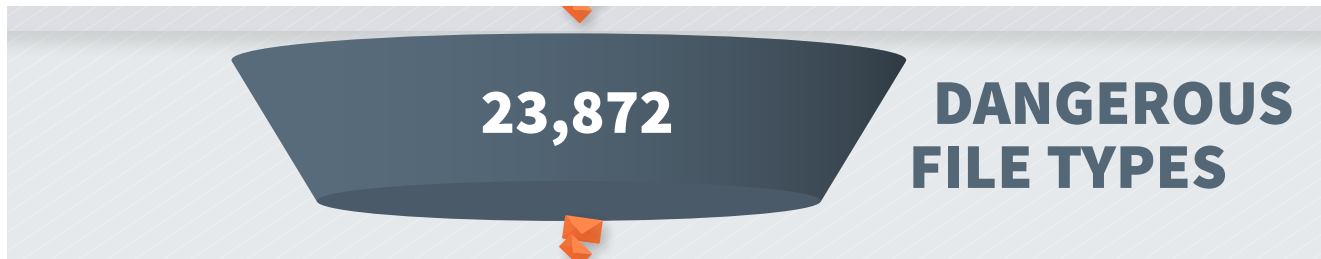
Analysis by Inspection Slice



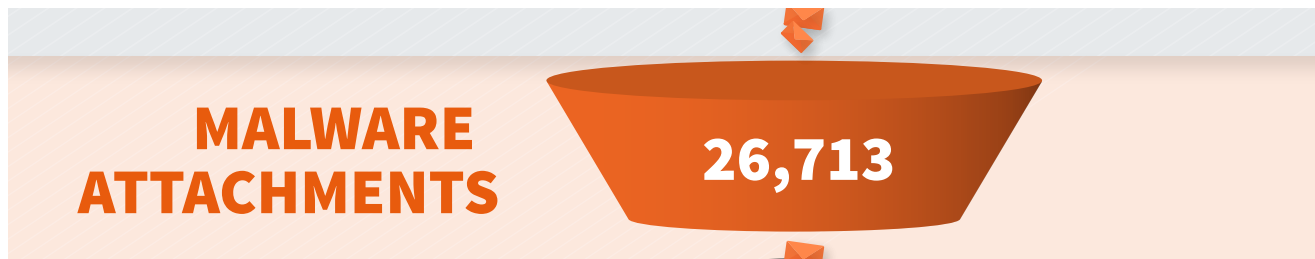
The ESRA testing to date has covered **378,559 email users** over a cumulative **1,965 days** of inbound email received into the organizations participating in the testing. In this time period more than **232 million emails** have been inspected by Mimecast. It is critical to understand that these emails were all passed by the incumbent email security system in use by the particular organization. The Mimecast security inspections occurred passively after the incumbent email security system executed all of its security filters. Overall, the Mimecast security service determined that more than **25 million** of the more than **232 million emails**, or **11%, were in fact “bad” or “likely bad.”** In other words, the overall false negative rate in aggregate for the incumbent security systems that have been tested were **11%** of all emails inspected by Mimecast.

Not surprisingly, the vast majority, or **99.6%**, of the false negatives that were passed by the incumbent email security systems and caught by Mimecast were spam email messages. In general spam email messages are annoying and time wasting, but not lethal. However, as you move down the inspection funnel the negative impact of the false negatives generally increase.





In the next inspection step down **23,872 emails with dangerous file types as attachments** were detected by the Mimecast service, and thus missed by the incumbent email security service. Dangerous file types cover approximately 1,900 file types that are rarely sent via email for legitimate purposes. Examples of these dangerous file types are .jsp (Java Server Pages), .exe (executables), and .src (source) files.



Next, **26,713 emails were determined to contain malware.** Malware of course can take many forms. Some malware is quite common and thus easy to detect with anti-virus engines and file signatures, whereas other, more targeted malware can be much trickier to find. The Mimecast malware detection analytics apply a combination of commercially available AV engines, static file analysis, and behavioral sandboxing to maximize the service's ability to detect even the newest and most evasive types of malware. It is important to understand that missing more targeted and evasive malware when it is attached to an email is a particularly troubling false negative as the next and generally final layer of defense at the endpoint may also be unable to detect and block it. And at this point the malware has landed.



53,753

IMPERSONATION ATTACKS

Now to the next ESRA inspection step, the **53,753 false negative emails which were characterized as impersonation attempts**. Impersonation emails, as the name implies, are impersonations which generally carry neither malware nor malicious URLs, and are thus particularly difficult to detect. Impersonation emails are social engineering heavy emails that attempt to impersonate a trusted party, such as a C-level executive, employee, business partner, or well-known internet brand with the goal of prompting the recipient to do something they shouldn't. Examples of this are sending wire-transfers, tax documents, or other sensitive and valuable data to the fraudster under the guise of some legitimate business process.



MALICIOUS URLs

463,546 DETECTED WITHIN 28,407,664 EMAILS

A recently added part of our ESRA testing is the detection of malicious URLs within delivered email. In aggregate the Mimecast ESRA testing detected **463,546 malicious URLs** that were contained in **28,407,664 delivered emails**. That comes out to an average of 1 malicious URL getting through an organization's email defenses for every 61 delivered emails. Given how many emails a typical organization gets in a day, that is a lot of malicious URLs waiting to be clicked in employees' inboxes!

Benefits of the Mimecast ESRA Program

The Mimecast ESRA program is designed to help participating organizations better understand the email-borne threats that are getting through their current defenses, giving them a sense as to the number and types of attacks to which they are likely vulnerable.

For the security industry in general, the aggregated data that is provided by running a series of ESRA tests across multiple incumbent security technologies provides tangible, quantitative evidence of the strengths and deficiencies of commonly used email security systems. This also helps alert organizations to the types of attacks that might be circumventing their existing security defenses.

Over time as Mimecast executes more ESRA tests, the security industry will receive more tangible evidence of email threats and the effectiveness of security defenses, as well as where organizations need to improve.

How an ESRA test works

Figure 2 below shows the basic setup and email flow for an ESRA test.

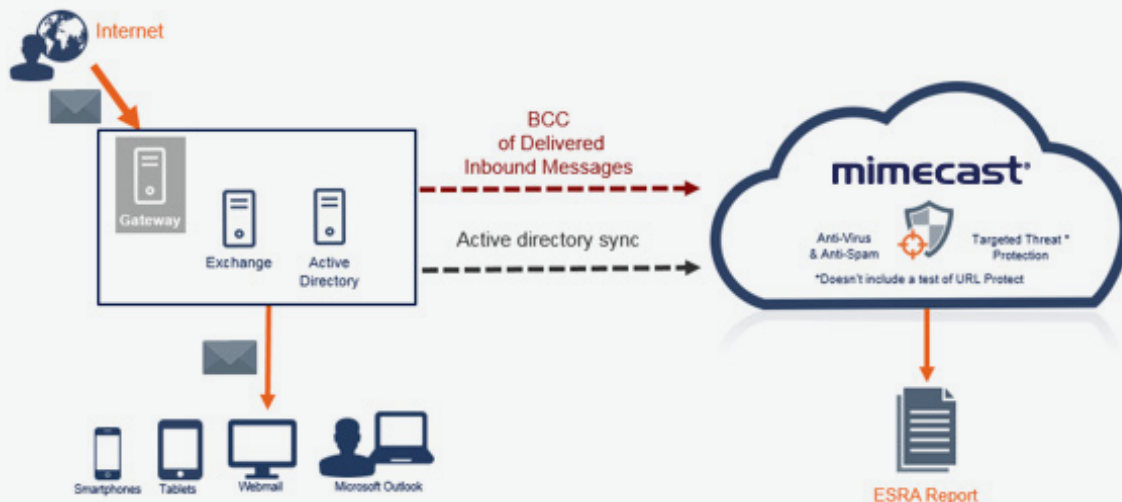


Figure 2 – Architecture and Email Flow of an ESRA Test

- The organization that is taking part in the ESRA test provides access to inbound emails after they have been inspected and filtered by their incumbent email security system. These emails are not manufactured or specially sent for the test, but are the actual emails being received by the organization during the test period. It doesn't matter whether their current security or email management system is deployed on-premises or in the cloud.
- The Mimecast service gets a stream of BCC copies of emails that have been delivered to the organization's email management system and thus passed by their incumbent email security system.
- The Mimecast security service inspects these emails for spam, malicious attachments and URLs as well as impersonation attacks that have been missed by the incumbent email security system.
- The testing period usually runs from 14 to 30 days.
- At the end of the test period a customized ESRA report is provided back to the organization participating in the test.
- The data is collected, anonymized and aggregated for use in reports such as that which is represented in Figure 1 and which is discussed in this paper.

Conclusion

Many organizations erroneously think their current email security systems are up to the task of protecting them, in particular from today's more sophisticated, well-resourced and targeted attackers. The Mimecast ESRA takes an important step to proving this to be wrong. Mimecast, as part of our commitment to improving security in general, and email security in particular, commits to continuing our ESRA testing. As we collect more data from more individual tests, we commit to update the security industry on what we are seeing. Ultimately the email security industry needs to be driven by data and not vague claims and generalizations, to more effectively protect customers and to improve the security industry's overall performance.



Want more details on how Mimecast
delivers Cyber Resilience for Email?

DOWNLOAD OUR TECHNICAL DEEP DIVE

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.

APPENDIX

Email Inspections Broken Down by Incumbent Provider

- Re-inspection totals aggregated from 75 organizations across 25 industries
- Data gathered over 1,965 days & 378,559 Email Users

Emails originally inspected by Microsoft Office 365™:	104,937,968
Emails originally inspected by Proofpoint:	63,495,503
Emails originally inspected by other providers:	63,577,510
Aggregated emails re-inspected by Mimecast:	232,010,981

Email Security Issues Not Identified by:

	Office 365	Proofpoint	Other Providers
Spam	16,437,723	2,981,583	5,489,585
Dangerous files	20,356	1,742	1,774
Malware attachments	12,948	11,734	2,031
Impersonation attacks	33,493	10,137	10,123

