

# The Mimecast Email Security Risk Assessment

for Microsoft Office 365

**mimecast**<sup>®</sup>

# The Mimecast Email Security Risk Assessment

*for* **Microsoft Office 365**

Many organizations think their current email security systems are up to the task of protecting them. 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 quality, protection and overall email security. The proof is in the numbers, and Mimecast is establishing a standard of transparency for organizations and raising the bar for all security vendors.

Since the beginning of the program Mimecast has completed many Email Security Risk Assessments against multiple incumbent email security systems. This report provides the details of these test results with a focus on Microsoft Office 365 and an explanation of what the results mean.

## **What is a Mimecast ESRA?**

Mimecast uses its cloud-based Advanced Security service to assess the effectiveness of legacy email security systems. The 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 or malicious attachments.

## **What We Found in This Series of Tests**

The information we've uncovered in this test series is concerning: Email attacks ranging from opportunistic spam to highly targeted impersonation attacks are getting through the Microsoft Office 365 service both in large number and type. Let's evaluate the scope of the problem by digging into the test data that is presented in Figure 1.

# The Mimecast Email Security Risk Assessment

for Microsoft Office 365

40,659 email users over 191 days

36,699,637 emails inspected by Mimecast

9,629,898

3,444,869 Rejected | 6,185,019 Quarantined



CAUGHT TOTAL SPAM

8,270



CAUGHT DANGEROUS FILE TYPES

1,958

1,534 | 424



CAUGHT MALWARE ATTACHMENTS

- 1,534 KNOWN MALWARE ATTACHMENTS
- 424 UNKNOWN MALWARE ATTACHMENTS caught by Sandboxing

9,412



CAUGHT IMPERSONATION ATTACK

27,050,099 emails deemed safe by Mimecast

### Analysis by Inspection Slice



These ESRA tests covered **40,659 email users** over **191 days** of inbound email received by the organization. In this time period, more than **36 million** emails were inspected by Mimecast. It is critical to understand that these emails were all passed by the organization’s implementation of the Microsoft Office 365 service with Exchange Online Protection (EOP) or Advanced Threat Protection (ATP). 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 nearly **10 million of the more than 36 million emails, or 26%, were in fact “bad” or “likely bad.”** In other words, the overall **false negative rate** in aggregate for the Microsoft Office 365 security service series of tests was **26%** of all emails inspected by Mimecast.

Not surprisingly, the vast majority, or **99.8%**, of the false negatives that were passed by the incumbent email security system 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 lethality of the false negatives increase.





In the next inspection step down **8,270 emails with dangerous file types as attachments** were detected by the Mimecast 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, **1,534 emails were determined to contain known malware.**

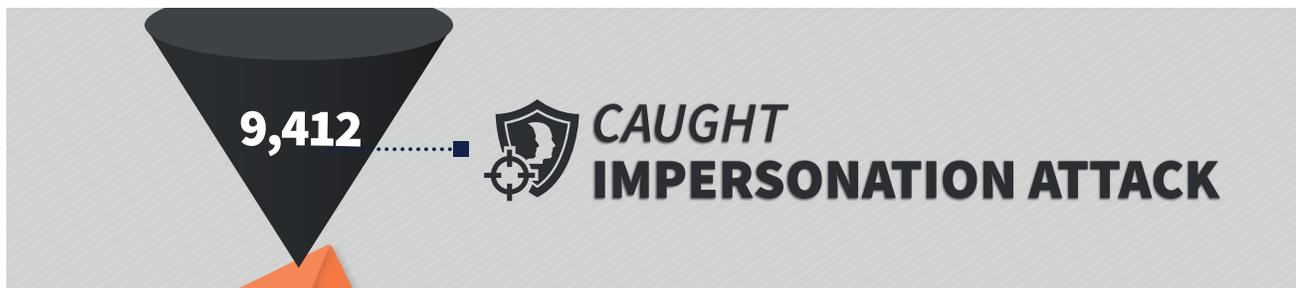
Known malware is a general term for malware which has previously been seen in the wild and is usually, for example, known by malware information sharing services such as Virustotal, and are readily detectable by up-to-date signature-based malware detection engines.

Missing known malware is a sign of a significant weakness in the malware detection capabilities of the security system.





Stepping down another level of lethality, in this series of ESRA tests **424 emails which contained unknown malware** attachments were detected through the use of file behavior monitoring technology, generally known as sandboxing. Unlike missing the **1,534 emails** containing known malware, which can generally be caught in a true belts-and-suspenders approach by commonly deployed endpoint-based anti-virus technologies, **missing emails with unknown malware attachments can be very bad**. This is because unknown malware will generally not be blocked by commonly used endpoint anti-virus technology. These false negatives will likely result in the attacker gaining or extending his foothold in the organization.



Now to the final ESRA inspection step, the **9,412 false negative emails which were characterized as impersonation attempts** that were missed by the Microsoft Office 365 security service. Impersonation emails, as the name implies, are emails which generally carry neither malware nor malicious URLs, and are difficult to detect. Impersonation emails are social engineering heavy emails that attempt to impersonate a trusted party, such as a C-level executive, employee or business partner, with the goal of prompting the recipient to do something they shouldn't. Examples of this are sending wire-transfers, W-2s, or other sensitive and valuable data to the fraudster under the guise of some business process.



### Benefits of the Mimecast ESRA Program

The Mimecast ESRA can 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 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. This data will be reportable by vertical industry, incumbent email security system, and even by the geographic location of the organizations as more tests are completed.

### How an ESRA test works

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

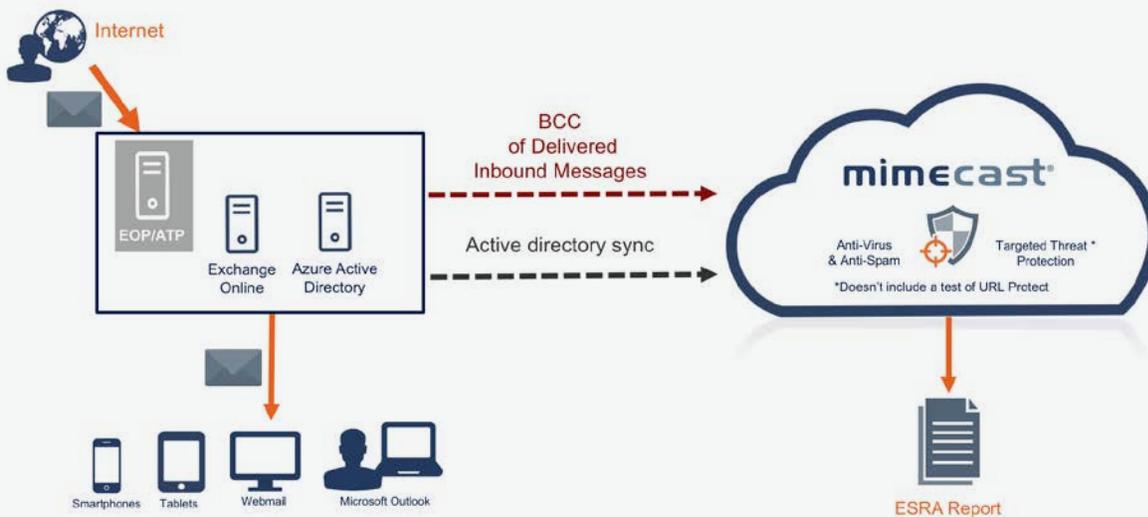


Figure 2 – Architecture and Email Flow of an ESRA Test

- 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, malware attachments and 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.

### Conclusion

While 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 tests. 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.

