Countering Impersonation, Spearphishing and Other Email-Borne Threats: A Review of Mimecast Targeted Threat Protection

Jerry Shenk
Any digital device or application can be a vector for a cyberattack, but email is an especially acute problem for many organizations. As individuals or members of organizations, most people rely on email to communicate with colleagues, whether in the next cubicle or across the globe. For many in the business world, 24/7 access to email is routine, and often required. Instant, ubiquitous and inexpensive communication gives us quick access to others in our business and personal lives, but gives criminals easy and direct access to us as well.

We’re all targets, but some people are more high-value targets than others. Attacks against high-value targets, sometimes called “whales,” have cost organizations millions of dollars, with devastating impact on the reputation of their organizations, their personal lives and even the political landscape in countries around the world. For example, the breach of Hillary Clinton’s personal email server almost certainly began with a phishing attack against campaign manager John Podesta.1 The risk is high enough that in April 2016, the FBI issued a warning that was specifically focused on one type of email-based attack, namely business email compromise (BEC), reporting a 270 percent increase since January of 2015.2

Phishing—like fishing—depends on luring a victim to bite, while hiding a sharp hook. Phishers can often lure the uninitiated with no more bait than a coupon or a tidbit of juicy gossip. Landing a whale, though, usually takes more sophistication. Criminals want whales—people who have access to a lot of money or data—to transfer funds to them or to turn over confidential information. Wary organizations are doing more to make their users aware of these dangers; they are also doing more to automatically intercept phishing emails that contain things such as malware or malicious URLs. To make defending against them even more challenging, authors of targeted whaling or impersonation attacks generally avoid including the indicators that traditional email security systems look for, namely attached malware or poisoned URLs. This means that without updated defenses, attackers can get through and have a better chance to land a whale, with the money and data rewards that come along with that.

---


Mimecast’s Targeted Threat Protection (TTP) service attempts to defend against impersonation and other targeted attacks by inspecting inbound emails for malicious URLs and attachments, impersonation attacks and message content that could indicate a request or response for targeted information. TTP’s features can be tuned for specific users and groups, and most organizations will want to focus at least initially on their high-value users because the likelihood of false positives could make the screening of quarantined emails time-consuming when used immediately for the general population. Although users in general and whales in particular need to understand the dangers of phishing and how to recognize them, Mimecast TTP can help by blocking malicious email traffic or at least warning the user of questionable email messages that aren’t blocked.

In testing by SANS, Mimecast’s TTP services worked well. The management interface can be a bit cumbersome for the administrator, but Mimecast officials said a more streamlined interface is in the works. TTP was effective in stopping inbound impersonation emails without extensive configuration, but best results required tuning filters to help define which messages qualified as threatening among the specific mix of email coming in to the test system. TTP did very well in recognizing links in email messages and rewriting them so that they would be checked when clicked. Those URL checks worked regardless of whether the user was on the local network or checking in from a remote connection such as a smartphone, home computer or hotel PC. HTML, images and other active content were held for review, rewritten or otherwise “defanged” before being delivered to the end user, if they were allowed through at all.
The Mimecast Email Security Gateway, which includes Targeted Threat Protection (TTP) services, is in most basic terms a cloud-based email-filtering solution for both inbound and outbound emails. It offers antispam and antivirus capabilities based on signatures, antspoofing rules, the reputation of IP and domain addresses, and other factors. TTP, which is the focus of this review, is a more recent set of security capabilities in the solution. In addition to scanning inbound email, the Mimecast email security service can also be configured to inspect outbound email messages as part of a broader data loss prevention (DLP) program, sometimes called data leak prevention.

TTP is designed to detect targeted attacks against those high-value employees (and members of their staffs) who handle confidential information or large amounts of money—and therefore are valuable targets of criminals. TTP’s primary objectives are to detect and stop 1) malicious URLs, 2) malicious attachments and 3) impersonation attacks.
Mimecast TTP operates by processing incoming email before it gets to an organization's email server, whether that server is on-premises or in the cloud. To accomplish this, the organization's DNS record needs to point all incoming mail to the Mimecast gateway instead of directly to the organization's production mail server. This mail flow enables Mimecast to analyze all incoming email before it presents any risk to the organization. Mimecast can also monitor outbound email by configuring the mail server to forward all outbound email to the Mimecast cloud service for inspection and delivery to the recipient’s mail server.

**Initial Setup**

Because the Mimecast Email Security Gateway is a completely cloud-based solution, setup for our review was minimal. A Mimecast technician handled the initial setup configurations over a WebEx session, adding the SANS test domain and the IP address of the lab’s mail server to Mimecast’s service. SANS initially configured Mimecast to allow email coming in to all users. Adjustments were made to the lab firewall to allow SMTP (port 25) traffic in from Mimecast. After initial setup, we ensured that mail was flowing correctly before redirecting the DNS zone’s mail exchange (MX) record to point to the Mimecast servers. Once the mail flow through Mimecast was verified, the MX records for the SANS test DNS zone were pointed to two of Mimecast’s SMTP IP addresses. From that point forward, any email addressed to the lab’s email server would first pass through Mimecast to be inspected for threat and spam.

**Dashboard**

All client-accessible administration for the Mimecast Email Security Gateway is done from the administrative dashboard, which provides system administrators with a quick overview of their email services (see Figure 1).
This view of the dashboard shows the inbound and outbound email queues, some notifications and an overview of recent activity. Each of the numbers in the “Activity over 24 hours” section is a link that will open a tab with details. This example shows that in the previous 24 hours, the Mimecast service took several actions, including blocking one attachment and rejecting seven messages. This particular report is for December 4. During the testing period, rejection counts peaked shortly after Black Friday (peak shopping day after Thanksgiving in the United States). Similar reports are available that show this information and more under the Services drop-down to help administrators track ebbs and flows in accepted and rejected email. The reports make it simple to research baselines and deviations from normal trends, and customized reports can be delivered on a weekly or monthly schedule.

Testing revealed some quirks with the dashboard. In particular, switching between setup options is somewhat difficult, especially at the outset. Mimecast is aware of the issue and is implementing “bread crumbs” in future versions to make it easier to work through the many configuration options offered. Another slight frustration was that sessions would sometimes close out seconds after activity, and a fresh login was generally required if the interface was idle for an hour, even though the threshold was set at four hours. These were fairly minor inconveniences that may even be resolved by the time this paper is published.
Spam and Known Malware Detection

Like many email security solutions, the Mimecast Email Security Gateway provides for the detection of spam and known malware. Because the testing lab’s domain is about 15 years old and has regular users as well as test and notification accounts, it receives a moderate amount of unwanted mail. Mimecast did reasonably well at blocking traffic based on IP address reputation and email with attachments that were malicious or violated stated policy. The system did allow a certain amount of “graymail”—email not malicious or exploitive enough to justify being blocked automatically on a large scale, but too commercial or irrelevant for a place on the priority list of most email administrators or business users.

Because individual criteria for blockable spam vary, it is almost impossible to create automatic filters that will catch every unwanted message. That was the case here. The Mimecast service did allow some graymail to get through even carefully configured filters, but it has additional policy configuration options for those who want to address all graymail. One is the ability to tag specific messages for additional action; they can be held for human review or placed into automated quarantine processes, or users can configure rules on their desktop email applications to route graymail into secondary folders for review later.

For safety’s sake, however, even graymail that penetrated the inner email sanctum had its attachments stripped out or modified into a safe format and its URLs rewritten so that users who did choose to click were rerouted through the Mimecast web proxy rather than directly to whatever web fate may have awaited them. Redirecting the connection at the time of viewing rather than when the message comes in means the user is protected from rapidly changing malicious links—links that are at first good and then later bad.
Targeted Threat Protection

One set of services that sets Mimecast apart is TTP, which consists of three primary modules: URL monitoring/checking/rewriting, attachment analysis, and inspection for impersonation attacks. TTP is designed to help email users, especially high-value users, avoid being targeted by email-based attacks. Many organizations concentrate greater resources to protect high-value targets, or whales, because the large sums of money or confidential information they control makes the attacker’s focused effort easier to justify. Smaller fish whose email has been compromised can serve as conduits to the big fish, however, so it is risky to focus excessively on a small number of users. Mimecast offers several levels of service to accommodate varying levels of risk but is able to deliver the highest level to everyone in the organization as well.

URL Protect

The Mimecast web proxy that is built into the service retests email-based links every time they are clicked, regardless of where users are when they connect. This “on-click” inspection is a necessary precaution because DNS-based URLs can be changed in an attempt by criminals to stay ahead of attempts to block them. What was good on one click might be bad on the next click.

Mimecast also includes a user-awareness feature. If a user clicks on a suspect link, the feature will display the URL and the title of the page and ask for confirmation before proceeding. The URL Protect policy that determines the percentage of URLs that get this treatment can be set individually for each user. Such reminders help users get in the habit of thinking before they click and also reinforces that they bear some responsibility for avoiding malicious links.
During testing, the URL rewriting sometimes caused problems in accessing a site. This didn’t happen often, but it can be annoying for end users. For example, a Kohl’s password reset email was blocked because the rewritten URL broke the site’s verification, which was dependent on the original URL in the email. In the test lab, a group was created named “HighValue.” At first, URLs were rewritten in all incoming email, but after initial testing, only the HighValue users were subjected to URL rewriting. Figure 2 shows how this setting can be applied. The path to this “Targeted Threat Protection – URL Protect” option is Services, Gateway, Policies.

![Figure 2. Setting Up Targeted Threat Protection in Mimecast Email Security](image-url)
Attachment Protection and Content Monitoring

Nearly all email users are likely to be targeted by malicious attachments at some point. While claiming to offer something the user wants or needs, such attachments are in fact designed to steal information, destroy or encrypt data for ransom, give attackers remote access, or compromise the security of the organization’s network and computing resources. Mimecast’s TTP inspects email for attachments that put the organization at risk.

TTP should be configured to block or create a safe copy of attachments for all users. Executable extensions that can be blocked by default include script files and batch files, but many organizations also block compressed files because they can contain malicious executable files. All files that are permitted based on policy are scanned for both known and unknown malware, and those that contain active content, such as a Word document that includes a macro or a PDF file with active content, are “defanged” prior to delivery. Policies can be enacted that let email recipients obtain a copy of an original attachment themselves after it is run through TTP’s sandbox, or that can be defined so that users must contact an administrator to get access to the original.

Figure 3 shows the options that can be configured for blocking attachment types.
As with most of the policy settings in Mimecast, policy violations can be handled with extensive flexibility, with options of Allow, Link, Hold and Block that can be handled by a user, a moderator or an administrator. In addition, notifications can be sent to the sender and/or the recipient, with notifications handled differently for internal and external parties. If an attachment is blocked, the documentation indicates that a notice can also be sent to a “content overseers group” for further processing.

**Impersonation Attacks**

In an impersonation attack, an attacker pretends to be a trusted, often internal, person to gain the trust and immediate interest of the target—and ultimately to get the target to do something he shouldn’t. According to a recent article by Brian Krebs, these types of attacks have become increasingly widespread and have allowed criminals to steal billions of dollars annually.

One common tactic is for an attacker to claim to be someone in the target’s organization. The CFO, for example, might receive an email asking for a transfer of funds that purportedly comes from the CEO. Such ruses, by instilling a sense of urgency, can be a surprisingly effective means of stealing large sums. By default, Mimecast leverages its directory integration to block mail coming into the domain from someone who claims to be from the same domain but is in fact from an external one. To avoid other attack techniques, Mimecast also lets the administrator configure allowed IP addresses so that organizations with multiple Internet connections can send email within the organization without triggering this part of the impersonation filter.

Mimecast’s impersonation-protect feature uses five criteria to determine whether an email message is attempting an attack using impersonation: Similar Domain, Newly Observed Domain, Internal User Name, Reply-to Address Mismatch, and Targeted Threat Dictionary. The email recipient typically does not see all these criteria. Figure 4 shows a Mimecast “suspicious message” notification for an email sent to the CEO of Mimecast.

![Image of a notification](image-url)
One of the tests used for the impersonation filter detects similar domain names. If the company’s domain is company.com, then an email from company.org should raise a suspicion that it might be malicious. In our testing, we set the number of hits to two; this means that two of the criteria need to match before an email will be determined to be suspicious. We also set the Similarity Distance for Internet domains to four. At a similarity of three, company.org would be detected as similar but company.info would not. At the similarity of four, company.info is also detected as being similar (see Figure 5). We also tested smaller differences such as company.com when the Similar Domain criteria was set to “true.”

Mimecast also looks at the words used in emails to determine whether they should be flagged as possible impersonation attacks. For example, it is not unusual for impersonation attack emails to include phrases such as “wire transfer,” “payment immediately” or “transfer funds ASAP.” A Targeted Threat Dictionary is maintained by Mimecast and updated as new threats are discovered. A threshold score must be reached before an email will be blocked, in an effort to avoid false positives. For testing, the threshold was set to two—if any two items tested true, the message would be held.

Figure 5. An Impersonation Report with the “Similarity Distance” Set at Four
In our test scenario, if we sent an email to a user in the company.com domain with a similar domain such as company.info and we included the test “wire transfer” in the message, then two of the criteria would be true and the message would be held for moderator review. The moderator would then review the message and release it if it was determined to be acceptable. Based on the setting for the policy, the message could be delivered without modification, or it could have the subject and/or message body modified to warn the recipient that it might be suspicious.

Data Loss Protection

Mimecast provides DLP services for outbound emails to block users from sending confidential or other sensitive information via email. DLP must be turned on by Mimecast administration to enable the setup options. However, because setup options may not clearly identify whether the feature is turned on or not, administrators should verify with Mimecast that the feature is turned on for their deployment. Once enabled, a DLP policy can be configured with terminology specific to the organization. For this test, some common terms were monitored (see Figure 6).

In this example a message will be rejected if it reaches a score of 10 (Activation Score). The Activation Score can be reached if an email contained a credit card number or a date of birth, but the term “Project X” would not cause a rejection unless it was combined with another sensitive term, such as “personal security code.” In that case, the score would reach 13, and the message would be blocked.

Figure 6. Configuring Keywords in Mimecast DLP
The testing lab set up the DLP service so that any outgoing message that violated the policy would be held for approval by an administrator, but the tool offers other options. Figure 7 shows the status of an email message that had the subject line “DLP test about Project X” and a message body that included the words, “My personal security code is 123.” In this case, the Held Messages queue showed this as a held message.

Figure 7. The Held Messages Queue in Mimecast DLP

Clicking on the held message provides details about why the message was held and gives the administrator the options of releasing the message or rejecting it. Various presets can be used in the email to the sender if it is rejected. These presets include “Message goes Against Email Policies,” “Inappropriate Communication,” etc., and there is also an option to write a more detailed explanation (see Figure 8).

Figure 8. A Held Message Report in Mimecast DLP
Email Security Reports

The Mimecast Email Security Gateway offers a thorough set of reports that can be generated for inbound or outbound mail. For example, reports can detail which users get the most mail, either by quantity of messages or size of the data transferred. Other examples are user pairs, breakdowns by domain and a few options for how to report on rejected email. Figure 9 shows total email volume compared with rejected email. Such reports can be useful for organizations that want to know more about the mail they are processing and what their users are doing with it.

By monitoring email usage, an organization would be able to use the information to help users avoid confidentiality issues and identify problems in mail flow.

Mimecast Email Security can generate and send out reports on a weekly or monthly basis—an automated timesaver that most administrators will appreciate.

Figure 9. Mimecast can issue reports on things such as “email volume vs. rejected mail.”
Email security is a serious and growing problem for email administrators and security professionals. Organizations have seen attacks on their high-profile users increase dramatically in recent years, with annual losses adding up to billions of dollars. Because high-value targets have access to big sums of money and large amounts of confidential information, their vulnerability can put business finances, trade secrets and confidential employee and customer data in jeopardy. Something must be done to help organizations detect and avoid these criminal attacks.

The Mimecast Email Security Gateway with Targeted Threat Protection (TTP) services seeks to detect fraudulent or malicious emails before they get into the organization. For outbound emails, its DLP capability seeks to catch sensitive information before it leaves the organization.

In testing, both the TTP and DLP services did well in their stated goals. Some of the features are new and will gain from additional tuning, both from development at Mimecast and by administrators tuning the gateway to meet the requirements and risk tolerance of their particular organizations. SANS’ conclusion, considering risk, is that the strictest filtering options should be reserved for the email users with the highest value or access to avoid end-user frustration and false positives. All of the features of the Mimecast solution allow for a high level of tuning to fit the needs of the particular organization. In addition, the reporting is quite good; having the system automatically email reports is a feature most administrators will appreciate.
**About the Author**

Jerry Shenk currently serves as a senior analyst for the SANS Institute and is senior security analyst for Windstream Communications, working out of the company’s Ephrata, Pennsylvania, location. Since 1984, he has consulted with companies and financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans networks of all sizes, from small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds six GIAC certifications—all completed with honors—and five with Gold certifications: GCIA, GCIH, GCFW, GSNA, GPEN and GCFA. He also holds the CISSP certification.

**Sponsor**

*SANS would like to thank this paper’s sponsor:*

![Mimecast Logo]
### Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Date</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>