Dealing With the Problem of Targeted Email Attacks

An Osterman Research White Paper

Published January 2015

SPONSORED BY

TREND MICRO™
EXECUTIVE SUMMARY

Targeted email attacks are a serious issue for organizations of all sizes and across every industry. Trend Micro’s and other industry research have shown that these focused emails are by far the number one initial attack vector for targeted attacks on enterprise data. In fact, they account for more than 95% of initial intrusions that lead to important data breaches. Moreover, Osterman Research found in a survey conducted during September 2014 that 47% of organizations considered targeted email attacks to be a very high priority to address and prevent, while only one in six organizations considers them to be a low priority.

While virtually all organizations have deployed security solutions that will block spam and known malware, most have not implemented solutions that will deal with the much more serious problem of targeted email attacks.

Targeted email attacks are not run-of-the-mill malware incursions. These attacks use sophisticated delivery techniques and advanced malware that will normally not be recognized by standard email and endpoint security solutions. Additionally, these attacks provide an entry point into the larger organization and its sensitive data, wreaking havoc on an organization’s finances, its intellectual property and its other sensitive or confidential data. Organizations of all sizes are the victims of these attacks and those that are successfully breached will experience critical business impacts, inclusive of damage to reputation, unexpected legal, regulatory and response costs and more.

KEY TAKEAWAYS

There are five key points made in this paper:

• Targeted attacks and advanced threats that result in data breaches are most often initiated by targeted email attacks. While a great deal of press attention focuses on attacks directed against large retailers and other high-profile companies, all types of organizations regardless of size and industry vertical are being subjected to attack.

• A single employee can be an entry point for a full-blown attack on the corporate network, sensitive data assets or financial accounts. Senior staff members like CFOs or CEOs are sometimes targeted in highly specific attacks, but the much larger attack surface is comprised of every employee in an organization.

• Users must be the first line of defense in thwarting targeted attacks; they require thorough and ongoing training to detect the social engineering techniques that these attempted attacks are employing.

• However, because targeted email attacks employ advanced malware, employee training is simply not enough – sophisticated technology to detect these threats is essential to prevent these attacks from achieving the loss of financial or other data for which they are designed. Further, while employees should serve as an important line of defense against threats, in many cases it is unrealistic to expect employees to keep abreast of every changing social engineering tactic.

• Ninety-one percent of organizational decision makers do not wholeheartedly agree that their current email security solution is sufficient to protect them from targeted email attacks. This, despite the fact that security professionals understand the problem.

ABOUT THIS WHITE PAPER

This white paper discusses the growing problem of targeted email attacks, their essential role in targeted attacks and advanced threats, how they occur, and what organizations can do to prevent them. The paper also provides a brief overview of Trend Micro, the sponsor of this paper, and the company’s relevant solutions designed to deal with these threats.
THE GROWING PROBLEM OF TARGETED EMAIL ATTACKS

WHAT ARE WE TALKING ABOUT?
The focus of this white paper – and a growing concern for security managers – is targeted email attacks. These threats are email-based attacks directed against a specific target, typically a company or a government agency. Because of the way that these attacks are constructed, using social engineering techniques and advanced malware, they quite often can penetrate an organization’s security defenses and create significant harm. Because most traditional, email-focused security defenses are not designed to deal with this sophisticated/never-been-seen-before type of threat, cybercriminals using custom designed targeted attacks can penetrate corporate systems with relative ease.

What we are not focused on in this paper are:

- **Spearphishing attempts**
  Targeted phishing attacks that are directed at a small subset of typically senior or high-ranking individuals within a company or other organization. Targeted email attacks are normally much broader in scope, intended to penetrate an organization’s security system through any employee.

- **Advanced Persistent Threats**
  Stealthy, long term and continued attacks against a specific company or organization.

- **Hacking**
  A form of specialized attack in which cybercriminals use a variety of techniques in an attempt to breach corporate defenses, such as the recent incursion against Sony Pictures.

Moreover, we are not focused on “traditional” spam – i.e., indiscriminate, unfocused email attacks across a wide spectrum of users that is the domain of standard email security solutions.

Instead, this white paper is focused on the broader threat problem that can exploit any user within a company, from clerical staff to senior executives. We are focused on email-based attacks only insofar as they serve as the beachhead for a deeper attack into an organization.

THE PROBLEM IS ALL TOO REAL
Targeted email attacks are by no means a theoretical problem: our research found that these attacks frequently disrupt company operations and steal data, as shown in Figure 1. While targeted attacks are often the entry point to a broader breach, they can cause significant damage in and of themselves. Importantly, our research also found that the problem of targeted email attacks is either not improving or is actually getting worse for 77% of the organizations surveyed.

THE GOAL OF TARGETED EMAIL ATTACKS
The goal of a targeted email attack is a fairly simple one: to bypass ALL security defenses using sophisticated malware for a variety of malicious purposes given that email is perceived to be the path of least resistance. Their goals include stealing login credentials for corporate financial accounts so that funds can be stolen; stealing intellectual property like proprietary designs or corporate planning documents; achieving ingress to sensitive systems like military databases, defense contractor files or other highly valuable content; or simply for gaining access to various backend systems to search for content that might be sensitive or confidential. The underlying motivation being to locate, extricate and monetize your data and intellectual property without you finding out.
Dealing With the Growing Problem of Targeted Email Attacks

Figure 1
Security Incidents Attributable to Malicious Emails
% of Organizations that Have Experienced These Problems

<table>
<thead>
<tr>
<th>% of Organizations</th>
<th>Security Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>74%</td>
<td>Disruption of company operations</td>
</tr>
<tr>
<td>41%</td>
<td>Loss of sensitive data on an employee’s computer</td>
</tr>
<tr>
<td>24%</td>
<td>Loss of sensitive corporate data from the network</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

WHO ARE THE TARGETS?
The object of a targeted email attack can be anyone in an organization that has an email account or who uses any other email account on the corporate network, such as personal Webmail. That employee might be a member of the clerical staff, a contractor, the CEO, or anyone in between who a cybercriminal can exploit to gain access to the corporate network and sensitive data resources. In many cases attackers select targets based on online social profiles and their ability to identify topics that will resonate with the intended target.

THE NEXT STEPS
Once a foothold is established, organizations face the next phase of attack. For example, a “watering hole” attack is one in which cybercriminals will determine which internal Web sites or resources are frequented by members of a target group and then infect them with malware. The goal of this type of attack is to infect additional employee computers and thereby further infiltrate an organization, looking for the access rights is the ultimate goal.

WHY ARE TARGETED EMAIL ATTACKS SUCCESSFUL?
The social engineering techniques used to create authentic-looking emails are quite sophisticated and exploit most users' lack of formal and ongoing training in recognizing these threats, as well as sloppy user practices. Exacerbating the problem is the typical corporate email user’s information overload that contributes to the mindset that all emails can safely be treated with equal caution or acceptance.

Osterman Research has identified six primary reasons why targeted email attacks are successful in penetrating conventional email security defenses and wreaking havoc among the organizations that experience them.

• **Lack of user attention to sound email practices**
  Many email users simply do not follow sound practices when reviewing email in their inbox or in a spam quarantine. For example, many email clients support “tooltips”, the pale yellow box that displays the actual URL of a hyperlink included in the body of an email when the mouse cursor hovers over the link for more than one second. However, instead of taking this preliminary step in evaluating whether or not a link is valid, many users will simply click on a link without questioning its authenticity. While many organizations instruct users not to click on links from unknown sources, this advice is often not heeded. Moreover, even when spam is properly identified as such and placed into quarantine, some users will mistakenly believe that the message was incorrectly flagged as spam and reclassify the message as valid, thereby introducing spam or malware back into their inboxes.

• **Lack of initial user training in spotting attacks**
  Many organizations do not adequately train their users with regard to email best practices, such as not clicking on links from unknown sources, not removing questionable email from spam quarantines, or viewing the full header information for potentially questionable email senders. While many organizations have acceptable use policies that focus on these issues, user training is often inadequate, if it occurs at all.

• **User gullibility**
  Simply put, many users are gullible: they will assume without question or verification that the spreadsheet attached to an email is actually from their company’s HR department, they will believe that the link in an email really does go to their company’s benefits administrator, or that they need to click on a link to re-enter their login credentials. It is essential to stress that this is not because employees are foolhardy or ignorant, but many do not view email content with a sufficient degree of skepticism, quite often because they have not been trained to do so.

• **Hacked social media and other accounts**
  Another problem that can lead to targeted email attacks is social media and other types of accounts that can become hacked or otherwise compromised. For example, if a colleague’s LinkedIn account gets hacked, a cybercriminal can use that account to send messages and links to the compromised individual’s contacts. Because social media systems are almost exclusively opt-in, recipients of these bogus messages will, in most cases, assume that the messages are valid and will respond accordingly because of the previous trust relationship that had been established. This type of incursion can reveal valid information to a cybercriminal or, worse, can provide an easy ingress point for malware.

• **Oversharing information**
  An increasingly serious problem is the tendency for users to share too much information in social media and in other venues. Users of social media who provide information on their personal preferences, recent purchases, travel plans, family members’ names, company information or real-time location (often provided automatically by various mobile applications), can provide a cybercriminal with enough information to dramatically increase the efficacy of targeted email attacks. For example, corporate users who regularly share their travel plans are more likely to fall prey to targeted email attacks that have subject lines relevant to those plans.

• **Chance**
  Another reason that targeted email attacks are successful is simply because of the law of averages. If a cybercriminal sends a targeted email with a malicious attachment to a company using a subject line that makes it appear that a FedEx or postal service package could not be delivered, for example, it’s likely that the message will be received by someone who is expecting a package at about that time, making it likely that the victim will click on the link. Cybercriminals need
only one such incursion to be successful, putting victims at a significant
disadvantage even if they are equipped with solid, albeit conventional, email
defense solutions.

**WHAT ARE THE CONSEQUENCES?**

There are three primary consequences that can arise from targeted email attacks:
direct financial losses, loss of intellectual property like trade secrets or proprietary
plans, and infiltration of systems that house sensitive or confidential data.

**FINANCIAL THEFT**

There have been numerous instances in which a targeted email attack was
responsible for significant financial losses:

- On May 9, 2012, a law firm in Charlotte, NC transferred nearly $387,000 to a
  bank in Virginia Beach, VA after closing a real estate deal. Later that day,
cybercriminals initiated a wire transfer for exactly $50,000 less with the law
  firm's bank in Charlotte, which sent the funds to a bank in New York and then on
to a bank in Moscow. The law firm believes it had been infected with keystroke
  logging software from a phishing email that captured all of the critical
  information necessary to initiate the wire transfer\ref{footnote1}.

- A targeted email attack on Fazio Mechanical, an HVAC contractor in Sharpsburg,
  VA, was able to successfully penetrate the organization’s email defenses and
  reportedly infect at least one computer with Citadel, a variant of the ZeuS
  banking Trojan. Approximately two months later, that infiltration was used in the
  attack on Target Corporation that resulted in the breach of information for
  approximately 110 million Target customers\ref{footnote2}.

- In September 2014, Home Depot detected a major data breach that reportedly
  had started about five months earlier, and that may actually end up exceeding
  the number of breached Target customer records. While Home Depot was
  running anti-virus software on its point-of-sale terminals, it was an older version
  that had not yet been replaced by a newer version of the software that the
  company had purchased\ref{footnote3}.

**LOSS OF INTELLECTUAL PROPERTY**

- Arguably the most infamous targeted email attack in recent years impacted
  security firm RSA in 2011. The attack originated with emails sent to two groups
  of employees. Although RSA’s security solution successfully quarantined the
  offending emails, one employee pulled the message out of quarantine, opened
  the attached malicious Excel file, and unleashed malware that installed a
  backdoor using a previously unknown flaw in Adobe Flash. Data stolen from RSA
  included information about the company’s SecureID offering\ref{footnote4}.

- The widely publicized CryptoLocker malware encrypts victims’ files and then
demands ransom to decrypt them – those who choose not to pay the ransom will
have their files deleted within a few days. This malware, which typically extorts a
few hundred dollars per incident, is typically delivered via email with a PDF or
.zip file disguised as a shipping invoice or some other business document\ref{footnote5}. As of
early 2014, CryptoLocker had infected roughly 25 million computers worldwide\ref{footnote6}.

- In April 2012, Israel Aerospace Industries (IAI) was the victim of a targeted
  email attack, presumably initiated by the “Comment Crew”, a Chinese
government-sponsored hacking group. In the several months following the initial
incursion, the group installed various Trojans and other malware designed to
steal highly sensitive military data, including data on Israel’s “Iron Dome” missile
defense system. A US-based cyber intelligence firm was able to identify more
than 700 files that were stolen from IAI’s systems, which the company

\ref{footnote1}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.

\ref{footnote2}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.

\ref{footnote3}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.

\ref{footnote4}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.

\ref{footnote5}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.

\ref{footnote6}: A targeted email attack on Fazio Mechanical, an HVAC
contractor…was able to successfully penetrate the organization’s
email defenses. Approximately two months later, that infiltration
was used in the attack on Target Corporation.
Dealing With the Growing Problem of Targeted Email Attacks

acknowledges was just a fraction of the total content stolen in the attack.

ININFILTRATION OF SENSITIVE SYSTEMS

• MiniDuke is a tool used by cybercriminals to infiltrate systems that manage critical infrastructure systems, government computers and other sensitive systems. It is delivered in PDF documents that are sent via email with subject lines like “Membership Plans” and “Human Rights Seminar”, and has infected systems in a number of countries.

• A successful phishing scam, presumably from the Syrian Electronic Army, that mimicked The Washington Post’s email portal was able to deliver malware to various reporters at the paper. The goal of the attack appears to have been simply to gain access to Washington Post reporters who possess Twitter accounts.

WHAT CAN YOU DO ABOUT IT?

Osterman Research recommends a three-pronged approach to dealing with targeted email attacks.

START BY EDUCATING USERS

First and foremost, decision makers should understand that users are the first, but certainly not the only, line of defense in any security model. While the appropriate technology-based defenses, as discussed below, are essential to protect an organization, users are a critical element in preventing targeted email attacks. However, our research has found that only one in eight organizations provides extensive training on targeted email attacks with frequent updates to the training regimen.

Consequently, all organizations should begin by educating users about the problems associated with targeted email attacks in order to ensure that they are ready to recognize and thwart them. This includes initial and ongoing training focused on being skeptical about messages that seem suspicious, not clicking on links in email messages that have the slightest possibility of being malicious, not opening attachments unless one is sure that they come from a bona fide source, and generally being careful about emails unless one is absolutely certain about the source of the message and its content.

CONDUCT ONGOING TESTING

Second, organizations should test their employees, before and after training, to determine their vulnerability to targeted email attacks. Although there are several solutions available to test employees’ vulnerability, one solution for which Osterman Research has conducted research is offered by KnowBe4. Our research found that among organizations that had implemented the solution, the number of organizations that reported an improvement in their phishing problem was nearly three times higher than for customers not using the solution.

The fundamental goal in testing employees is not only to help decision makers evaluate the potential for specific employees to fall victim to targeted email attacks, but also to help employees become more sensitized to these attacks – what they look like, how they differ from valid email, and how better to recognize them.

IMPLEMENT THE RIGHT TECHNOLOGY SOLUTIONS

Finally, decision makers should implement the appropriate technology solutions that will prevent targeted email attacks from reaching end users. Such a solution should:

• Scan incoming emails for malicious URLs and attachments that might contain malware.
• Use sandboxing technology that allows potentially suspicious files to run. This allows files from untrusted or unknown sources to run in their entirety without the possibility that malware could enter the corporate network.

• Finally, the solution should allow administrators to implement granular policies for suspicious content. For example, the system should look for malicious URLs and attachments and allow fine-grained treatment of this suspicious content, such as deleting it, sandboxing it, categorizing it, passing it along to an administrator for inspection based on individual user requirements, or adding administrator-defined messages to the content. The solution should use heuristics and sophisticated, continually updated algorithms to ensure that new and zero-day attacks have little or no chance of entering the corporate network. Finally, the solution should employ robust reputation analysis to ensure that as much data about the source of the suspicious content is known before it is passed along to users.

Our research found that for all of the defenses available to organizations to defend against targeted email attacks, two-thirds are focused on technology-based solutions, while only one-third involve user training and awareness. While both are essential elements in dealing with these attacks, technology solutions are clearly the most important defense mechanism.

Osterman Research has found that there is a significant difference between what organizations are currently doing to address targeted email attacks compared to what they would do ideally. For example, as shown in Figure 2, while 27% of organizations do not currently address these attacks with anything other than their standard email gateway, the vast majority would implement additional capabilities to deal with targeted email attacks. Moreover, the figure also demonstrates that in an ideal security environment, 61% of organizations would implement either an on-premises server/appliance or a cloud service in addition to the email security gateway to deal with targeted email attacks compared to the 49% that do so today.

Figure 2
Current and Ideal Approaches to Dealing With Targeted Email Attacks

Source: Osterman Research, Inc.
SUMMARY

There are four primary issues presented in this white paper:

• Targeted email attacks are an incredibly serious problem and are getting worse over time because they are the initial step of an ultimate data breach.

• Because email is the most commonly used application by information workers, and because the typical email user receives approximately 100 emails per day, email systems typically are the past of least resistance into the organization.

• These attacks impact all organizations and can target every employee, not just senior executives.

• Users need to be the initial line of defense against targeted email attacks because they can thwart some of these attacks through good training and continued diligence in being skeptical of what they receive in their inboxes. However, because users make mistakes, they cannot be relied upon as the only defense against targeted email attacks.

• Consequently, robust, technology-based solutions must be implemented to provide as complete a defense against targeted email attacks as possible.

ABOUT TREND MICRO DEEP DISCOVERY EMAIL INSPECTOR

With most targeted attacks arising from a targeted email, or spear-phishing attack, sophisticated social-engineering techniques are used to target specific employees in an organization. Attackers are able to convince users to unknowingly download a malicious file attachment or click through to a malicious site. Once this occurs malware is then installed on their machine and attackers are able to establish a beachhead to penetrate your network; in search of valuable data and intellectual property.

To identify and stop targeted email attacks, The Trend Micro Deep Discovery Email Inspector uses proven algorithms and specialized detection methodologies to detect and block email traffic that contains malicious attachments or URLs. This single-appliance solution seamlessly interoperates with your existing secure email gateways to create an integrated defense against attacks that would otherwise evade your defenses Deep Discovery Email Inspector:

• Protects sensitive data, intellectual property, and privileged communications from theft and spying
• Defends organizations and executives against unwanted exposure and damage to their reputation
• Minimizes the risk of major financial impacts associated with litigation, fines, clean-up, and investigation costs.

Read more about Deep Discovery Email Inspector
ABOUT TREND MICRO
Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on 26 years of experience, our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by over 1,200 threat experts around the globe. For more information, visit TrendMicro.com.
© 2014-2015 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

http://krebsonsecurity.com/category/smallbizvictims/
http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breac-at-target/
http://www.bankinfosecurity.com/analysis-home-depot-breach-details-a-7323/op-1
http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
http://www.newsobserver.com/2014/01/20/3547208/malware-threatens-small-businesses.html