Spear Phishing: Top Threats and Trends

Vol. 2 August 2019

Email account takeover: Defending against lateral phishing

Lateral phishing is emerging as an effective way for attackers to leverage legitimate accounts compromised through email account takeover. This report takes an in-depth look at the latest tactics used by scammers and how to protect your business.»

Barracuda
Your journey, secured.

Table of contents

Email account takeover

Defend against this widespread and increasingly sophisticated attack.»

Over the past year, Barracuda researchers teamed up with leading researchers at UC Berkeley and UC San Diego to study a growing threat to enterprise organizations: email account takeover. In email account takeover, the attackers use legitimate enterprise accounts they've recently compromised to send lateral phishing emails to an array of recipients, ranging from close contacts within the company to partners at other organizations.

Because attackers send these lateral phishing emails from legitimate accounts, they can effectively fool many existing email protection systems and unsuspecting users. In this study, spanning nearly 100 organizations, we take a detailed look at the widespread and dangerous nature of this attack, analyze the different strategies that attackers use for selecting their potential victims and the content they use in their attack messages, and highlight a few forms of sophistication and stealth exhibited by this evolving attack.

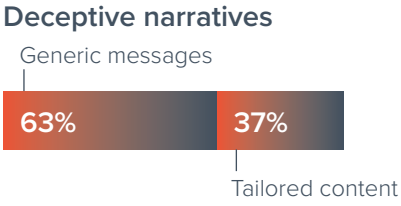
Key findings

1 in 7 - Organizations attacked

Email account takeover and lateral phishing present a growing threat to enterprise organizations. 1 in 7 organizations experienced lateral phishing attacks within a seven-month timespan, based on a random sample of enterprise organizations. Of the organizations who suffered from this attack, over **60 percent experienced** multiple incidents.

Because email account takeover takes advantage of compromised, but nonetheless legitimate, enterprise accounts, these attacks are effective and particularly insidious. Over **11 percent of attacks** successfully compromised additional employee accounts, and over **42 percent of the lateral phishing incidents** do not appear to have been reported by a recipient to the organization's IT or security team.

The attackers conducting lateral phishing attacks follow four primary strategies for selecting target recipients. Over **55 percent of the attacks** in our study target recipients with some personal or work relationship to the hijacked account.



Lateral phishing attacks rely on two popular narratives to trick their victims into falling for the attack: "account error" and "shared document" lures. While **63 percent** of the lateral phishing incidents used generic and commonplace messages, **37 percent tailored** their content to be more enterprise-oriented or highly specific to the victim organization.

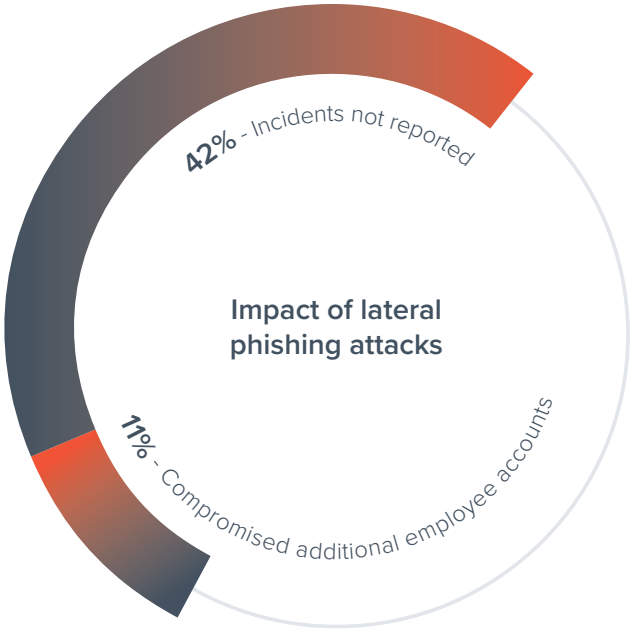
Nearly all the lateral phishing attacks occurred during the regular workweek and during the victims' regular working hours. The attackers perpetrating the email account takeover might be remote or foreign actors.

Roughly one-third of email account takeover attacks in our study engaged in additional behavior designed to make their lateral phishing emails stealthier or more convincing, such as actively responding to recipients' questions or actively deleting all traces of the phishing email from the hijacked account.

Scale of email account takeover attacks

Email account takeover attacks are a widespread and effective attack that enterprises need to defend against. As highlighted in an earlier Threat Spotlight, based on a random sample of dozens of Barracuda customers, our researchers found that **1 in 7 organizations** experienced email account takeover and lateral phishing within a seven-month timespan. To make matters worse, most organizations that experienced email account takeover suffered from multiple lateral phishing incidents: Over **60 percent of these organizations** had multiple compromised employee accounts that attacker used to send lateral phishing attacks.

These attacks prove particularly insidious because they come from a compromised, but legitimate account. As a result, many users and existing email protection systems assume these lateral phishing emails are legitimate, because phishing emails have historically come from spoofed or external accounts. Across the **180 lateral phishing incidents** examined in this study, our researchers estimate that over **11 percent of attacks** successfully compromised other employees at the victim organization. Moreover, for over **42 percent of the lateral phishing incidents**, none of attack's recipients appear to have reported the phishing attack to the organization's IT or security team.



Recipient targeting strategies

Across the study's dataset, attackers used a total of **154 hijacked enterprise accounts** (ATOs) to launch lateral phishing attacks. Examining the recipient sets who received these lateral phishing emails, our researchers identified four primary strategies that attackers used to select the potential victims.

1. Account-agnostic (45%)

Across **45 percent of the hijacked accounts**, attackers did not appear to draw heavily on the hijacked account's relationships when selecting their victims. These attackers appeared more interested in opportunistically phishing as many accounts as possible, rather than compromising victims with some tie to the hijacked account.

2. Targeted-recipient

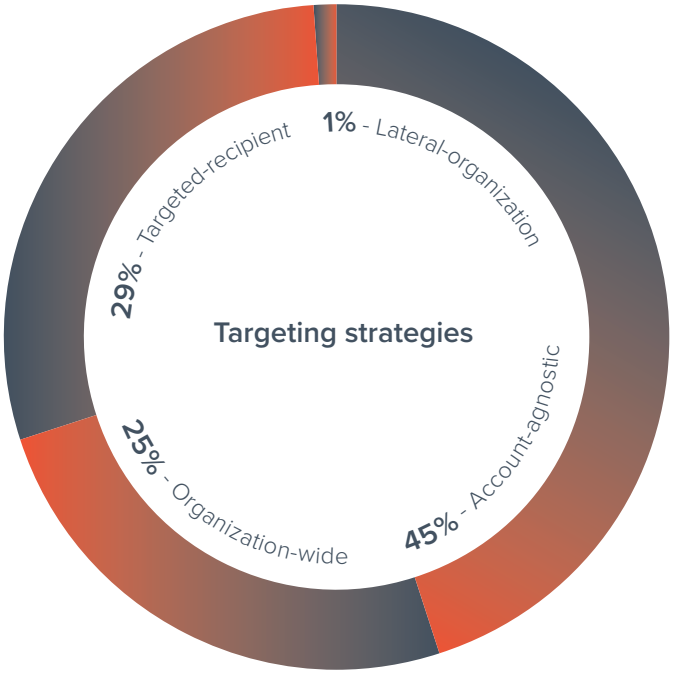
Attackers selected their victims by mining the hijacked account's recent or close contacts; **29 percent of attacks** followed this strategy.

3. Organization-wide

Attackers leveraged the hijacked account to send phishing emails to dozens to hundreds of fellow employees at the same company; **25 percent of attacks** used this strategy.

4. Lateral-organization

Attackers used the hijacked account to send phishing emails to recipients at other organizations within the same industry, e.g., business partners of the hijacked account's organization. Only **1 percent of attacks** adopted this strategy.



Content in lateral phishing attacks

Because attackers control a legitimate account in an email account takeover attack, they could mine the hijacked account's emails to craft custom and highly personalized messages. Across the incidents studied, our researchers found that the majority of lateral phishing attacks rely on two deceptive narratives:

1. Messages that falsely alert the user of a problem with their email account
2. Messages that provides a link to a fake "shared" document

In both cases, the attacker provides a link for the victim to click on, which often leads to a phishing website designed to look like a legitimate login page but that ultimately steals the victim's username and password.

Among the incidents studied, **63 percent of the attacks** used commonplace variants of the "shared document" and "account problem" messages (e.g., "You have a new shared document"). However, **30 percent of the incidents** used more refined messages, modifying the language to target enterprise organizations (e.g., "Updated work schedule. Please distribute to your teams").

In the most sophisticated approach, **7 percent of the attacks** involved highly targeted content that was specific to the hijacked account's organization. For example, in one email account takeover incident, the attacker compromised an account at an organization that was about to celebrate its 25th anniversary. Using the hijacked account, the attacker sent dozens of spear-phishing emails to fellow employees advertising a 25th year anniversary celebration event (e.g., "Please see the attached announcement about FooCorp's 25th year anniversary").

Top 10 most common words used in lateral phishing emails:

Document (89 incidents)

View (76 incidents)

Attach (56 incidents)

Click (55 incidents)

Sign (50 incidents)

Sent (44 incidents)

Review (43 incidents)

Share (37 incidents)

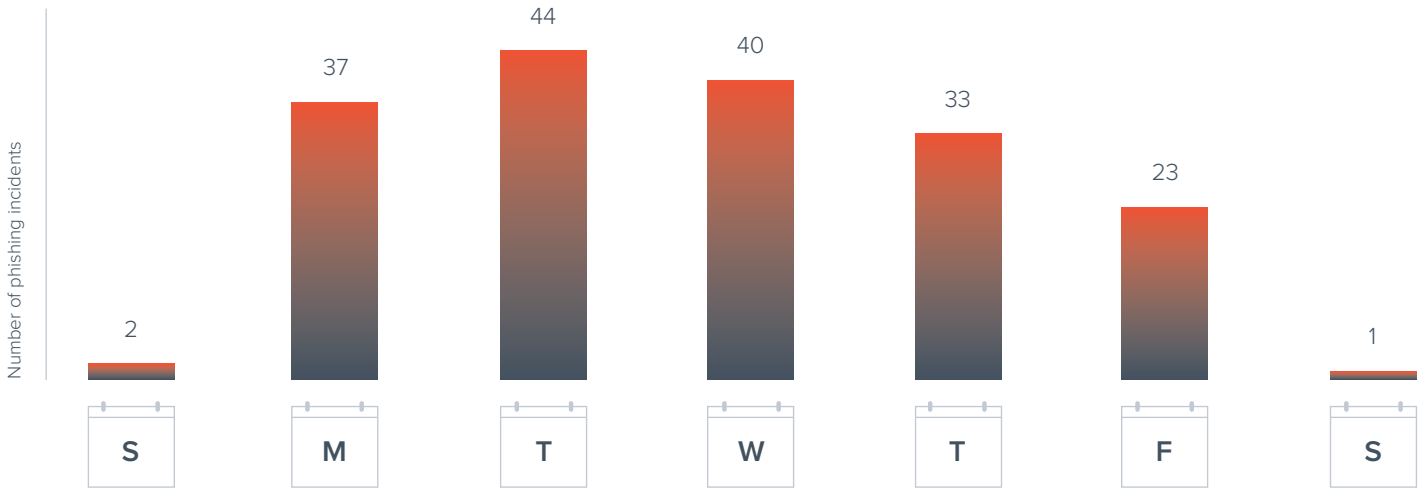
Account (36 incidents)

Access (34 incidents)

Timing of attacks

Several studies have hypothesized that attacks such as phishing might be detectable by looking for suspicious emails that are sent at unusual times. However, based on the attacks in this study, it appears that attackers send lateral phishing emails from compromised accounts during the typical working hours of the affected organizations.

A full **98 percent of the lateral phishing incidents** occurred during a weekday. The study also looked at whether lateral phishing emails occurred at unusual hours by comparing the times when the lateral phishing emails were sent versus the historical times when the hijacked accounts usually sent benign, work emails. From this analysis, our researchers found that **82 percent of lateral phishing attacks** were sent by an attacker during the compromised account's typical working hours.



Sophistication and stealth

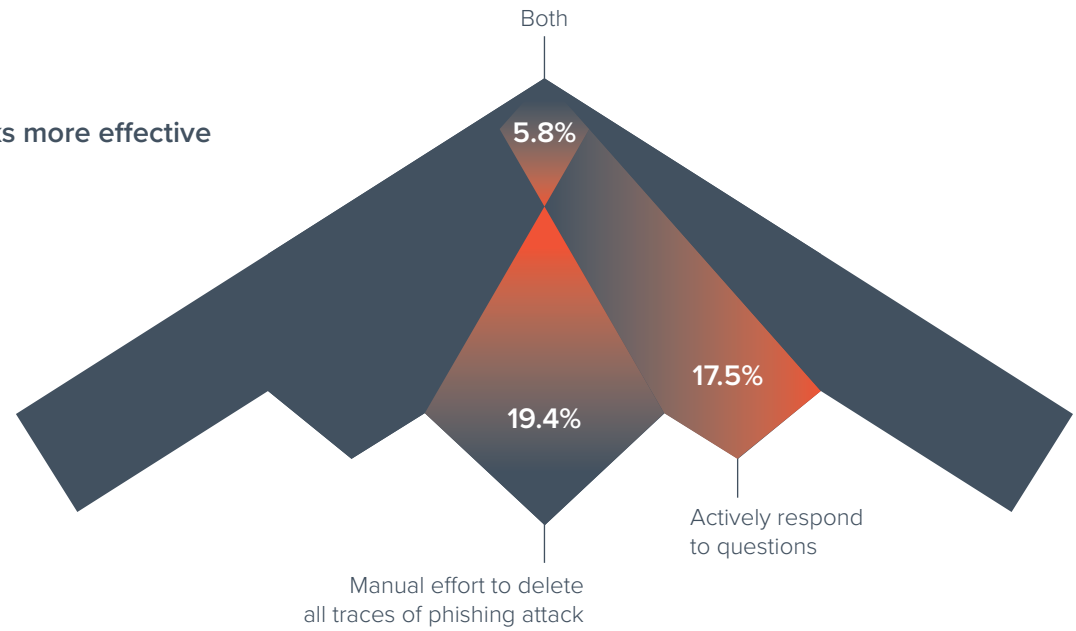
Over the course of the study, our researchers observed that nearly **one-third (31%) of the attackers** perpetrating these lateral phishing attacks used sophisticated tactics to increase the effectiveness of their phishing emails or hide evidence of their attacks.

Often, recipients of the lateral phishing emails replied to the hijacked account to ask whether the email was legitimate or intended for them. Across **17.5 percent of the hijacked accounts** we studied, attackers actively responded to their recipients' inquiries to assure the victim that the email was legitimate and safe to open (e.g., "Hi [Bob], it's a document about [X]. It's safe to open. You can view it by logging in with your email address and password.")

Separate from interacting and assuring their victims, **19.4 percent of hijacked accounts** engaged in a manual effort to delete all traces of their phishing attack from the account they've hijacked. These attackers not only deleted the phishing emails they sent, but also deleted replies from inquiring recipients.

A total of **5.8 percent of the hijacked accounts** engaged in both of these sophisticated behaviors.

Tactics used to make attacks more effective



How to defend against lateral phishing

There are three critical precautions you can take to help protect your organization against lateral phishing attacks: security awareness training, advanced detection techniques, and two-factor authentication.

1. Security awareness training

Improving security awareness training and making sure users are educated about this new class of attacks will help make lateral phishing less successful. Unlike traditional phishing attacks, which often use a fake or forged email address to send the attack email, lateral phishing attacks are sent from a legitimate—but compromised—account. As a result, telling users to check the sender properties or email headers to identify a fake or spoofed sender, no longer applies.

Users can often still carefully check the URL of any link before they click it to help them identify a lateral phishing attack. It is important that they check the actual destination of a link in any email, and not just the URL text that is displayed in the email.

2. Advanced detection techniques

Lateral phishing represents a sophisticated evolution in the space of email-based attacks. Because these phishing emails now come from a legitimate email account, these attacks are becoming increasingly difficult for even trained and knowledgeable users to detect. Organizations should invest in advanced detection techniques and services that use artificial intelligence and machine learning to automatically identify phishing emails without relying on users to identify them on their own.

3. Two-factor authentication

Finally, one of the most important things that organizations can do to help mitigate the risk of lateral phishing is to use strong two-factor authentication (2FA), such as a two-factor authentication app or a hardware-based token if available. While non-hardware based 2FA solutions remain susceptible to phishing, they can help limit and curtail an attacker's access to compromised accounts.

A longer form version of this study will be presented at the Usenix Security Symposium, one of the top academic conferences for security research.

Barracuda
Your journey, secured.