# Spear Phishing: Top Threats and Trends

Vol. 4 July 2020

## Insights into attacker activity in compromised email accounts

A specialized economy is emerging around email account takeover as cybercriminals find new ways to attack and exploit email accounts. This report takes an in-depth look at the threats organizations face from account takeover and the types of defense strategies you need to have in place to protect against these types of attacks.»

Barracuda
Your journey, secured.

# Table of Contents

# Lifecycle of account takeover

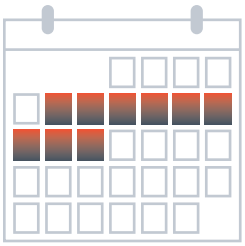
## Build a better defense based on attacker behavior in hijacked accounts.»

Over the past year, Barracuda researchers teamed up with leading researchers at UC Berkeley to study the end-to-end lifecycle of a compromised account. Examining **159 compromised accounts that span 111 organizations**, they looked at how the account takeover happens, how long attackers have access to the compromised account, and how attackers use and extract information from these accounts.

The findings show clearly that account takeover incidents often last for weeks or even months. Many times, multiple accounts—and even multiple cybercriminals—are involved. The researchers also found that a significant source of these compromises came from employees reusing passwords that had been stolen in a separate breach rather than through phishing attacks.

This report takes a detailed look at the widespread and dangerous nature of these attacks, analyzing how cybercriminals behave in compromised accounts and how that should inform your organization's defense strategies.

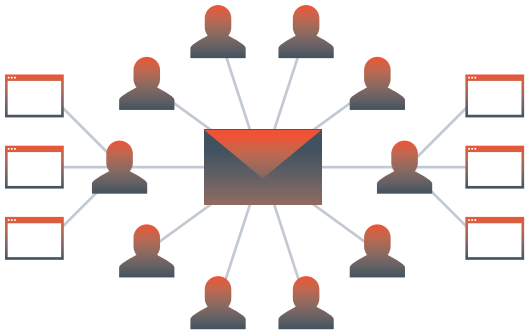
# Key findings



Over 33% had attackers dwelling in the account for **more than one week**.

**More than one-third of the hijacked accounts analyzed** by researchers **had attackers dwelling in the account for more than one week**. This suggests that beyond initial detection, post-compromise tools, such as forensics, automated incident response, and post-delivery threat removal, are crucial for preventing the compromise of additional accounts.

**20 percent of compromised accounts appear in at least one online password data breach**, which suggests that cybercriminals are exploiting credential reuse across employees' personal and organization accounts.

**31 percent of these compromises reflect an increasingly specialized criminal market** for account compromise, where one set of attackers focuses on compromising accounts and then sells account access to another set of cybercriminals who focus on monetizing the hijacked accounts.

**78 percent of attackers did not access any applications outside of email**, which suggests that either many organizations' cloud accounts do not have access to interesting data and functionality outside of email, or that attackers have yet to adapt and exploit these additional sources of information.

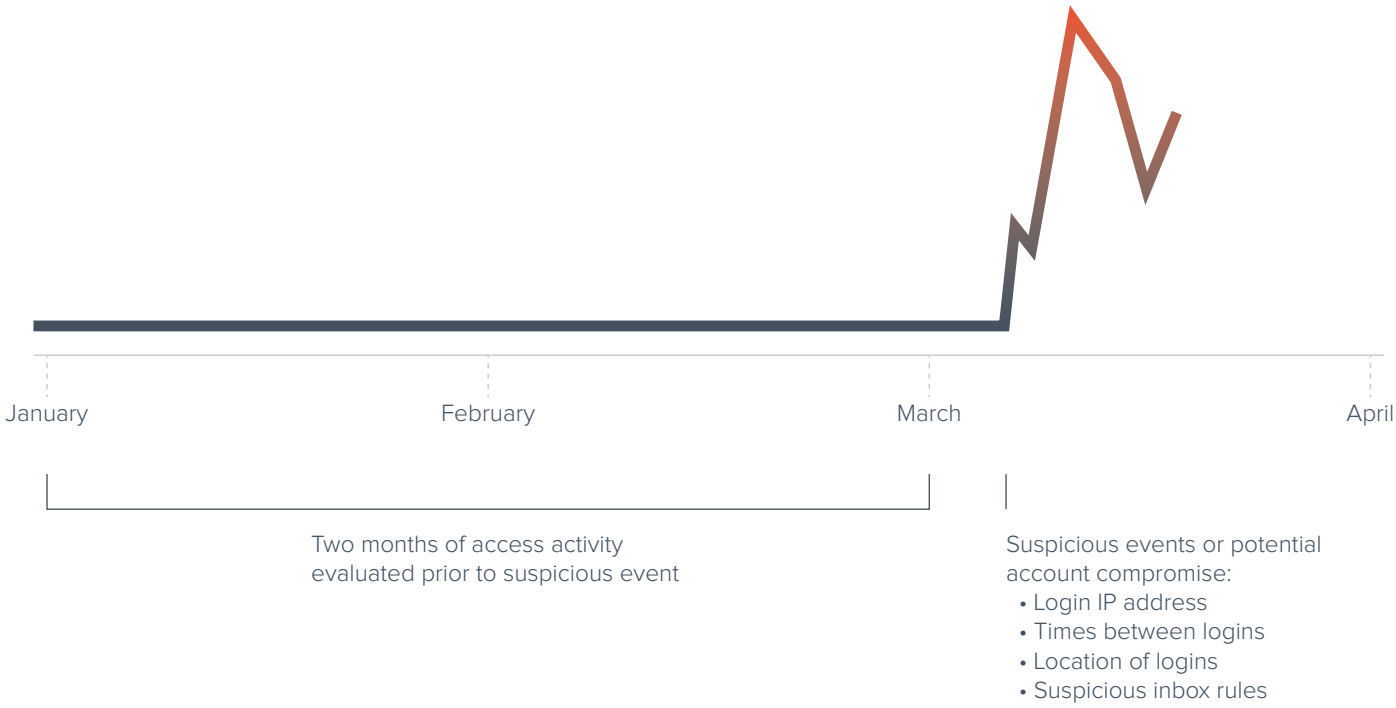
# What is email account takeover?

In email account takeover, cybercriminals use brand impersonation, social engineering, and phishing to steal login credentials and access an email account. Once the account is compromised, hackers monitor and track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled, so they can launch subsequent phishing attacks, including harvesting financial information and additional login credentials for other accounts.

Cybercriminals can launch subsequent phishing attacks, including harvesting financial information and additional login credentials.»

# Signs of attack

To identify attacker activity, researchers looked for suspicious events around the time the user's organization confirmed the account was compromised. This activity was compared to typical behavior for the account from a two-month period before the compromise.

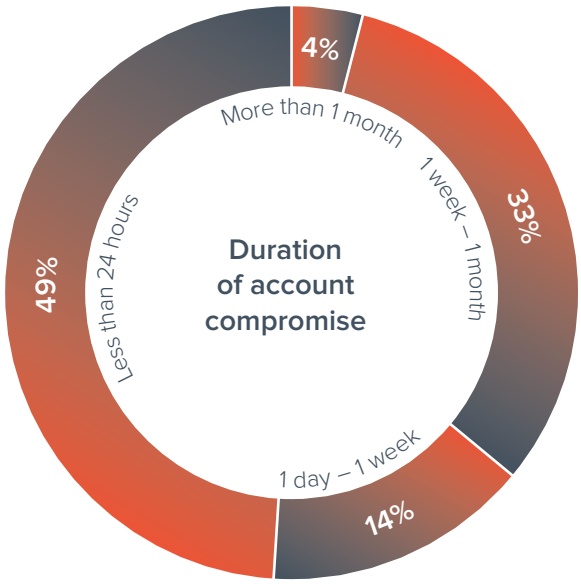



Suspicious activity included logins from IP addresses mapped to countries, states, or provinces that were never used before for the user's account. Researchers also compared the elapsed time between logins from different locations to the time it would take to travel between locations. For example, if there was a login from Japan that showed up 46 minutes after a login from Illinois (where that user is based), but the expected travel time between Illinois and Japan is about 13 hours, then researchers would reason that the login from Japan was suspicious.

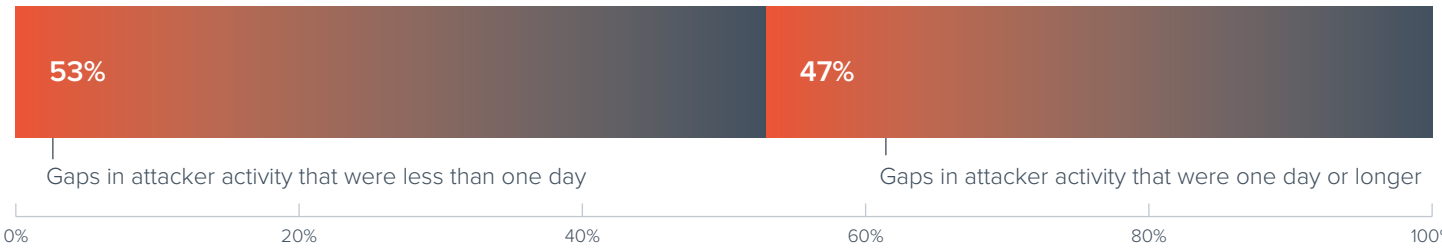
Another red flag that researchers looked for was suspicious rules being created in a user's account, such as emails being forwarded to the trash or to an external account.

# Duration of compromise

Based on analysis of attacker behavior in 159 compromised user accounts across 111 organizations, researchers found that **roughly half of accounts (49 percent) are compromised for less than 24 hours, and 37 percent of accounts are compromised for at least one week.**

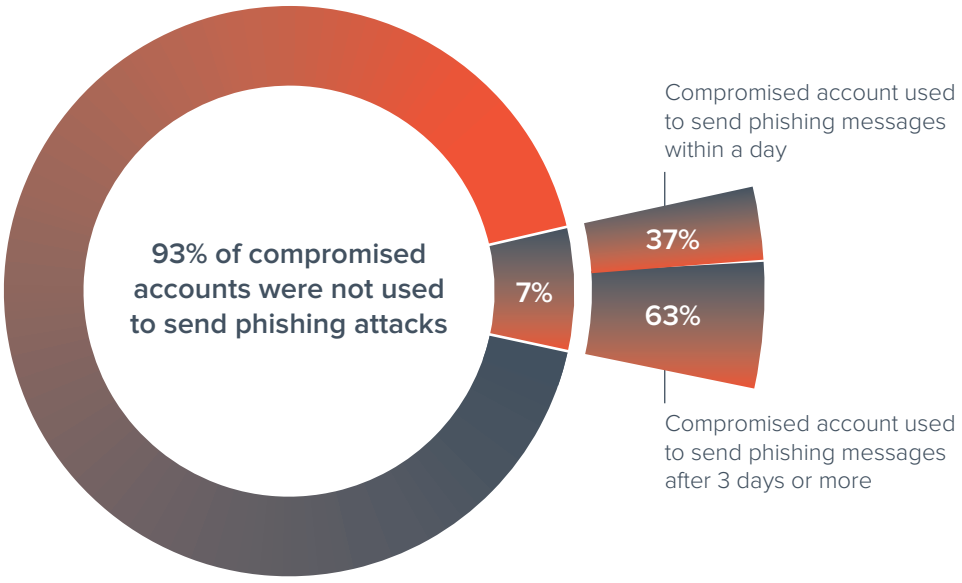



For each of 159 compromised accounts, researchers also analyzed the time between attacker events and calculated the longest gap in attacker activity for each account. **In 53 percent of compromised accounts, the largest gap in attacker activity is less than one day, while the remaining 47 percent of compromised accounts (74 out of 159) contain gaps in attacker activity that were one day or longer.** Hackers sometimes sell login credentials to other cybercriminals after compromise, so a different set of attackers will end up using the compromised account. Large time gaps in an attacker's activity could be the time needed to conclude the transaction and hand over login credentials.



# Accounts used in phishing attacks

Of the 159 compromised accounts analyzed, **7 percent (11 accounts) sent phishing emails** flagged by Barracuda. **Four of the 11 accounts** (37 percent) had less than one day between the attacker's first login and the first phishing email being sent. The remaining seven accounts (63 percent) had three days or more between the attacker's first login and the first phishing email being sent. Although it's a small sample size, this suggests that attackers who aim to send phishing emails vary their approach upon first accessing a compromised account. Some send phishing emails almost immediately, while others wait for some time to pass.



For the seven accounts that had more than three days between the first attacker login and the first phishing email sent, researchers found that in six of these accounts, the first phishing email was part of a large burst of emails, each with the same subject, sent in **25 minutes or less**. Four of these accounts sent **400 or more emails** as part of the burst, while the remaining two accounts sent fewer than 100 emails as part of the burst. The six accounts with bursts sent emails to a variety of accounts within and outside the compromised organizations, and three of these accounts had at least one email where BCC was used to send a phishing email.

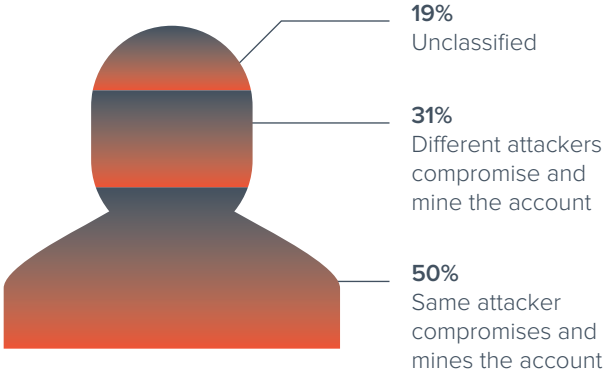
For the remaining 93 percent of the accounts, attackers don't seem to be using the accounts to send phishing attacks, at least not during the time period researchers analyzed, but there are a number of ways they could still use those accounts. For example, attackers could use information from the compromised accounts, set up impersonating domains, and launch conversation hijacking attacks that way. The low number of accounts flagged for sending phishing emails suggests that the attackers don't want to send emails from compromised accounts because that will increase their chances of being caught, and they want to keep access to these accounts. A second possibility is that some attackers have no interest in using the accounts; rather, they are interested in just selling the access, and they haven't found a buyer yet.

These findings illustrate the need to react as soon as possible to any sign of attacker activity, even if the initial compromise was not detected. For instance, due to the fact most attackers wait for some time before sending their first phishing email, organizations have a small window of time to intervene and react to potential attacker activity before more damage is done.

> Attackers could use information from the compromised accounts, set up impersonating domains, and launch coversation hijacking attacks.»

# Two types of attackers

Our researchers estimate that in **50 percent of the accounts analyzed**, a single attacker conducts both the compromise and utilization of the account. However, **31 percent of accounts** are compromised by one attacker and then used by a different attacker that mines for information and extracts value from the account. As a result, a more mature and specialized criminal economy around compromised accounts is emerging, where some attackers specialize in compromising accounts, while others specialize in extracting value and information.




Researchers made these classifications by analyzing attackers' activities within compromised accounts by looking at:

- **ISPs data**
- **Devices used to perform activities**
- **Geo-location of access**
- **Duration of an attack**
- **The length of time gaps in attacker activity**

Accounts with compromise lasting less than a day and with small gaps in attacker activity were likely compromised by single attackers. Accounts with a long duration of compromise and large gaps in attacker activity, along with strong signs of different types of activity before and after these large gaps, likely involved multiple attackers. Accounts with the larger time gaps in activity and longer duration of compromise are likely to be sold among attackers, with time gaps representing the transaction window.

In most cases, the second set of attackers who gain access to the account inflict more damage than the first set of attackers who perform the compromise. This makes early detection and mitigation even more important.

# Compromise through credential reuse

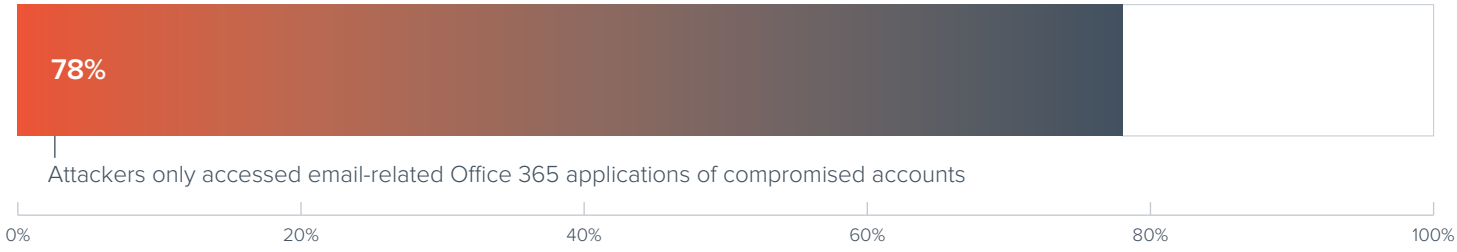
In trying to understand how accounts are compromised, our researchers discovered that **20 percent of the accounts were found in data breaches** of online company databases. For these accounts, email addresses were likely used to create personal accounts on websites and when the databases were breached, the users' account credentials were leaked. As a result, if these users reused credentials across their personal and organization accounts, their corresponding organization account would also likely have been compromised through the same data breach.

This data illustrates that breaches are fairly common among organization accounts, and credential reuse with personal accounts can cause significant damage. As a result, organizations should frequently alert their employees of the dangers of credential reuse among their accounts to avoid additional compromises, and possibly adopt multi-factor authentication or the use of password managers.

If these users reused credentials across their personal and organizational accounts, their corresponding organization account would also likely have been compromised through the same data breach.»

# How attackers use compromised accounts

Attackers compromising accounts primarily use the accounts for accessing email-related Office 365 applications. Our researchers found that in 98 percent of compromised accounts, attackers accessed at least one email-related Office 365 application, such as Microsoft Outlook, providing a quick and convenient way for an attacker to gain access to contact lists and learn about any confidential and financial information tied to the employee and the organization. In fact, in **78 percent of compromised accounts**, attackers only accessed email-related Office 365 applications. This suggests that the type of organization compromised does not influence the ways an attacker uses the account.




Attackers accessed non-email related Office 365 applications in just **22 percent of compromised accounts**. Of these non-email applications, Microsoft SharePoint was the most popular target, accessed by attackers in **17 percent of attacks**. As SharePoint is a document management and storage application, attackers can likely use it to gain easy access to confidential documents about the user and the organization.

Email and inboxes are incredibly valuable today. They contain a lot of information, including sensitive data that is being shared. Many employees will store that data in their inboxes — without archiving. As a result, attackers are able to use and search inboxes in the same way they would a filing system and can obtain everything they need. In fact, it's probably much easier to look for information in the inbox than in other cloud-based applications because everything is date stamped and historical context information on all parties involved exists. That makes it very easy to set up targeted attacks or conversation hijacking using only inbox data.

Given the wide range of cloud applications accessible by attackers, such as Office Delve and Microsoft Forms, and the abundance of documents and files shared among organizations, it's surprising that attackers don't access these applications

more often. But, the more accounts attackers access, the bigger footprint they leave and the greater their chances of being caught. At the end of the day, most attackers want money for their efforts, and phishing attacks can be easier to monetize than stealing data and then finding a buyer for it.

Our researchers also found that attackers rarely change account passwords and never grant authorization to cloud applications to access data within the accounts. **Only two out of 159 compromised accounts (1.3 percent)** had at least one Change Password for User operation performed in close time to attacker activity. Researchers uncovered more attacker activity after the change password operations were performed, indicating that these passwords were changed by the attacker themselves. None of the 159 accounts had a single Add Authorization operation performed during the time period of attacker activity, which grants applications access to data within the account. Taken together, these findings suggest attackers are not interested in changing a user's password or adding authorization to a user's account because these actions might reveal to the user that their account has been compromised and limit the amount of time the attacker can operate in the account.

Only 1.3 percent of compromised accounts had at least one "change password for user" operation performed in close time to attacker activity.»

# How to defend against account takeover

### 1. Automated, AI-based detection of compromised accounts

Due to the fact attackers can compromise accounts in a variety of ways (phishing, password reuse, from another compromised account), it's important to deploy an AI-based detector for compromised accounts that examines a variety of signals, including suspicious links, sender behavior, IP login information, and suspicious inbox-forwarding rules.

### 2. Monitoring and forensics

The research clearly shows that account takeover incidents often last for weeks or even months. Many times, multiple accounts—and even multiple cybercriminals—are involved. This raises the importance of the ability to continuously monitor internal accounts for suspicious activity, as well as the need to use forensics and remediate these attacks even after the initial compromise has occurred.

### 3. Education and training

The sheer amount of privileges granted to accounts can very easily end up in the wrong hands without up-to-date knowledge of attacker patterns and enhanced defense mechanisms. IT security teams should prioritize making email applications more secure and training employees to be more stringent in sharing confidential documents and information in applications such as Microsoft SharePoint.

### 4. Password management

A significant number of these account compromises aren't from classic email attacks like phishing. Rather, they come from a breach affecting another system where passwords were stolen and employees reused those passwords. This strengthens the importance of multi-factor authentication, continuous monitoring of internal accounts, and being able to deploy forensics after the fact. It's also important to train users on best practices in password creation and storage and review password-management policies to see if they need to be strengthened. Password management is not a panacea because once attackers get into an organization, they can compromise additional accounts, but it's still an important part of protecting against account-takeover attacks.

You can read the full academic paper, "A Large-Scale Analysis of Attacker Activity in Compromised Enterprise Accounts" at https://www2.eecs.berkeley.edu/Pubs/TechRpts/2020/EECS-2020-80.pdf

Barracuda
Your journey, secured.