**proofpoint.**

# Cloud Account Compromise and Takeover

## Fast Facts

### DESCRIPTION

Cloud account compromise is the act of maliciously gaining control over a legitimate user's cloud-based email or collaboration service account—giving the attacker wide-ranging access to data, contacts, calendar entries, email and other system tools. Beyond the compromised user's data, the attacker can use the account to impersonate the user in social engineering attacks such as business email compromise (BEC) and more, both inside and outside of the organization. Threat actors can access sensitive data, persuade users or outside business partners to wire money or damage an organization's reputation and finances. They can also install backdoors to maintain access for future attacks.

### TOOLS OF THE TRADE

- Phishing attacks, including OAuth token phishing.
- Brute-force attacks that automate credential guessing, such as Aircrack-ng and Jack the Ripper.
- Credential recycling or stuffing, which uses already stolen username and password pairs.
- Malware, including keyloggers and credential stealers such as PunkeyPOS and Spyrix.

### TYPES

- Credential theft—attackers exploit weak passwords, poor security systems and reused passwords from other sites to hack into systems.
- Malicious OAuth apps—use OAuth token phishing and app impersonation to manipulate account owners into delegating permissions for accessing system resources.
- Insider threats—credential loss created by negligence or malicious intent.
- Malware—malicious software installed in systems can go unnoticed for long periods of time. Such malware can steal credentials and communicate with the attacker.

### RISK FACTORS

- Using shadow IT or cloud applications and services without approval from the IT department.
- Poor email and cloud security monitoring tools.
- Credential sharing among employees or with outside partners.
- Low user awareness of good security practices and common phishing techniques.

As business assets have moved to the cloud, cyber attackers have followed close behind. Starting with hosted email and webmail, cloud productivity apps like Office 365 and Google Workspace, and on to cloud development environments like AWS and Azure, cyber criminals have prized account credentials and made them the target of countless phishing campaigns. And with single sign-on giving lateral access to many different systems within an organization, a single compromised account can cause widespread damage.

## Cloud Account Compromise in the News

### Capital One fined $80 million for 2019 hack of 100 million credit card applications

The U.S. Department of Justice arrested Paige Thompson, a former Amazon software engineer, and charged her with computer fraud and abuse for allegedly accessing Capital One data. Using a server-side request forgery (SSRF) attack, she obtained credentials for a role that had access to sensitive information stored in Amazon's S3 file-storage service. According to prosecutors, Thompson discussed her exploits in detail on her Slack channel and posted instructions on GitHub for duplicating the attack.[1]

### NSA and FBI blame Russia for massive 'brute force' attacks on Microsoft 365

A joint report produced by U.K. intelligence, the U.S. National Security Agency, FBI and U.S. Department of Homeland Security, identified Russian cyber crime group "Fancy Bear" as responsible for a long-term campaign to breach Microsoft 365 accounts. The attacks involved "password spraying," where computers try to access an account multiple times in succession using different password combinations.[2]

1 Devling Barrett (The Washington Post). "Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications." August 2020.
2 Thomas Brewster (Forbes). "NSA and FBI Blame Russia for Massive 'Brute Force' Attacks On Microsoft 365." July 2021.

## Anatomy of a Cloud Account Takeover

Here's how most cloud account takeovers play out.

1. **Credential theft.** The attacker gains access to the user's credentials through credential phishing, brute-force password attacks, credential stuffing/recycling, malicious OAuth apps or credential-stealing malware (see **"Tools of the Trade" on page 1**).

2. **Infiltration.** Once logged into the user's account, the attacker has access to the victim's email, contacts, calendar and files. The attacker can steal this data directly or use it to impersonate the user convincingly.

3. **Persistence and expansion.** Some fraudsters may respond to existing email threads or send draft emails with malware or unsafe URLs to colleagues and outside business partners. Posing as the compromised user, the attacker may then target others inside and outside the company with fake invoices or payment rerouting instructions. The attacker may also upload malware into corporate file shares or sabotage the company in other ways. Often, the attacker sets up auto-forwarding rules that provides access to the user's email even if the user changes the password. Seeing all incoming email and calendar invites gives the attacker key details for future impersonation attacks.

4. **Monetization.** If an attack is not detected in time and allowed to persist, account compromise can result in theft of money or valuable data such as financial records or intellectual property.

## Attacks lead to data loss, wire fraud and system abuse

| 1 | RECONNAISSANCE |
|---|---|
| | **Credential Phishing** |
| | **Leak or Dump** |
| | **Keylogger or Malware** |
| | **Malicious Insider** |
| | **Social Engineering** |

| 2 | INFILTRATE |
|---|---|
| | **Credentials Variance** |
| | **Direct Login** |
| | **Cloud Malware (Third-Party Apps)** |

| 3 | EXPAND, PERSIST AND LEARN |
|---|---|
| | **Maintain Access**<br>• Create email forwarding rules<br>• Change permissions<br>• Create admin accounts<br>• Disable multifactor authentication<br>• Install third-party access |
| | **Use Trusted Accounts to Launch Attacks**<br>• Send internal and external phish<br>• Upload and share malware |
| | **Discover Potential**<br>• View emails and files<br>• Discover organizational structure<br>• Study business processes |

| 4 | MONETIZE |
|---|---|
| | **BEC-Email Fraud**<br>• Wire fraud<br>• Salary fraud<br>• Gift carding<br>• Supply chain fraud |
| | **Data Exfiltration**<br>• Email<br>• Download<br>• Share |
| | **Sabotage**<br>• Cloud ransomware<br>• Destruction |
| | **System Abuse**<br>• Spam<br>• Fraud as a service<br>• Crypto mining |

Risk factors and consequences associated with cloud account takeover.

# How to Protect Your Organization

- Block credential phishing emails from getting into users' inboxes.
- Make users a strong line of defense with training on password best practices and how to recognize phishing emails. Ideally, they should also have a simple way to report suspicious messages.
- Consider a cloud access security broker to get a consolidated view of your organization's cloud services landscape. It should include details about the users and OAuth apps with access to data in cloud services from any device or location.
- Take a zero-trust approach to network and app access to limit the harm from a compromised account.
- Scan internal email, not just inbound email, for threats such as malware and email fraud.
- Use multifactor authentication. While this isn't always a silver bullet against account takeover, it makes an attacker's job much harder.
- Identify users most at risk and monitor for incidents.
- Set up and prioritize alerts based on your organization's most critical risk factors.
- Correlate threats across email and cloud to accurately detect compromised accounts.
- Govern OAuth apps and revoke malicious and other risky apps.
- Prevent clicks on malicious URLs and malware downloads by isolating web browsing activity.
- Investigate security incidents with a solution that offers detailed forensics and customizable reports.
- Prevent unauthorized access to cloud apps and services with adaptive access controls, especially for unmanaged devices.
- Automate your security response with flexible policy controls that respond to incidents or changes in users' risk profiles. Users who are under attack or represent a higher risk because of their digital habits or access privileges may need to reauthenticate themselves regularly.

# Research Insights

Proofpoint monitors thousands of cloud tenants and over 20 million active cloud users. In a study of 2020 cloud threat data, we observed the following:

**95%** of organizations were targeted

**52%** of organizations had at least one compromised account

**32%** of compromised organizations had post-access activity such as file manipulation, email forwarding and OAuth app activity

**10%** of organizations had authorized malicious OAuth apps

And according to 86% of IT leaders polled in a 2021 Ponemon Institute report commissioned by Proofpoint, cloud account compromises cost organizations more than $500,000 a year.[3] Survey respondents also reported 64 cloud account compromises per year on average, with 30% exposing sensitive data.[4]

Nearly 60% of respondents indicated Microsoft 365 and Google Workspace accounts are heavily targeted by brute-force and phishing-based cloud attacks.

Overall, more than 50% of respondents said phishing is the most frequent method attackers use to acquire legitimate cloud credentials.

3   Ponemon. "Cost of Cloud Compromise and Shadow IT." April 2021.
4   Ibid.

# Learn More

To protect against cloud account compromise, organizations should ensure they have robust security in place. Security platforms should be capable of end-to-end encryption and continuous data monitoring and detect incidents quickly to enable administrators to limit and resolve any damage.

To learn more about how to stop cloud account compromise effectively, visit **www.proofpoint.com**.

**proofpoint.**