zilla SECURITY

EBOOK

The Security Risk of Orphaned Accounts ...

... and what you can do about it.

The Security Risk of Orphaned Accounts … and What You Can Do About It

Are you leaving the keys where thieves can find them?

The average person will change jobs 12 times in their career. With each new job, they'll receive new credentials including a phone number, email, and access to a myriad of digital assets from corporate intranets to cloud-hosted applications. But what happens to those credentials when they leave? Ideally, businesses would wipe clean identity-based information after an employee leaves. In reality, however, account credentials often remain in place long after an employee has left.

Did You Know?

Only **1 in 3** companies automatically revokes digital access privileges when an employee leaves the company.[1]

These unowned or "orphaned" accounts represent a significant security risk to businesses. Essentially, they are keys to critical applications and information that have been left lying out in the open. Worse, many of these keys are protected by weak passwords, making them easy targets for cybercriminals who would hack into business systems to steal corporate and customer data.

How big of a problem are orphaned accounts? The truth is that most businesses don't know because they don't have tools in place to track them. By some estimates, as many as eighty percent of user accounts may be orphaned due to changing jobs, changing technologies, and changing levels of permission. While most businesses have established processes in place to onboard new employees, those processes tend to fall apart when an employee changes roles within the company or leaves the company.

Hacking orphaned accounts is as easy as 1, 2, 3...

It's not unusual for employees to manage hundreds of different password-protected accounts. Not surprisingly, weak passwords (e.g., "123456," "password") and frequent re-use of passwords are common workarounds to this complexity. Of the 200 most popular passwords used around the world, the vast majority can be hacked in less than a second. Because most enterprises aren't even aware of orphaned accounts—let alone monitoring their activity and ensuring they have the latest security patches—these accounts are especially vulnerable to hackers.

Once a hacker has figured out the login credentials for an orphaned account, they will often try to escalate their privileges and move laterally within the enterprise's IT environment. Because companies are unaware that orphaned accounts have been compromised, hackers can wait months or even years before activating these accounts and using them for espionage or theft. Or they may decide to sell these stolen credentials on the dark web to the highest bidder.

But how do cybercriminals know which accounts are orphaned? After all, it's not as though businesses publish a list of people who have recently left their company. Or do they? The fact is that corporate press releases, LinkedIn pages, and other forms of social media are an unwitting but excellent resource for hackers when looking for potentially orphaned accounts. The higher an employee's role within the company, the more likely their transition is public knowledge—and the

Did You Know?

"123456"

is the most popular password in the world — followed by "123456789" and "12345". [2]

CASE STUDY

How an orphaned account shut down Colonial Pipeline

In 2021, Colonial Pipeline made the news for all the wrong reasons when their oil and gas pipeline was shut down by a computerized attack, causing widespread gas shortages at more than 10,000 gas stations across the southern United States. The hackers behind the attack didn't engage in high-tech espionage or dupe an employee into giving their credentials through a sophisticated phishing attack. Instead, the hackers simply found an orphaned VPN account, figured out the password, and within hours brought over 5,000 miles of fuel pipeline to a grinding halt.

By hijacking the orphaned VPN account and injecting ransomware into Colonial Pipeline's system, the cybercriminal group Darkside was able to walk away with $4.4 million for what was likely a fairly simple hack. While Colonial Pipeline was able to restore their operations shortly after paying the ransom, restoring their reputation will likely take more time. Today, the incident still serves as a sobering reminder of what can go wrong when companies fail to monitor and manage orphaned accounts in a timely manner.

Did You Know?

There are over 15 billion stolen account credentials available on the dark web.[3]

How do I know if I'm at risk?

Orphaned accounts can be a security risk for any business. Yet there are contributing factors that make it more likely your business is at increased risk by exposing a high number of orphaned accounts to potential hackers. Here are four signs that your business is more likely to become a target of an attack mounted through an orphaned account.

1 **High employee turnover**

According to the U.S. Bureau of Labor Statistic (2021), employee turnover rate across industries is 57.3%.[4] This number can be even higher for industries such as retail and healthcare, which have experienced unusual volatility in the wake of Covid-19.

2 **Part-time and contract employees**

Seasonal workers, contractors, freelancers, consultants, and other "part-time" workers may come and go in the life of a business without ever being officially terminated. This oversight can lead to orphaned accounts with access to corporate networks, confidential data, business applications, and communications systems after the contract or relationship is over.

3 **No "de-provisioning" process**

It's not unusual for companies to have a detailed onboarding process for new employees and a less detailed process for exiting employees. A strong de-provisioning process is more than just decommissioning single sign-on (SSO) applications and removing an employee from their active directory. Companies need to have a thorough understanding of each account associated with an employee and make sure those accounts are closed when an employee leaves the company.

4 **Shadow IT**

IT departments are no longer the sole gatekeepers of technology. Cloud services and mobile apps have replaced traditional office suites, to the extent that nearly half of all business applications exist outside the data center as "shadow IT" services. De-provisioning shadow IT accounts can be problematic because the responsibility to de-commission them often rests with the employee.

How the cloud and Covid formed the perfect storm

The rise of cloud-based services and the continuing effects of Covid-19 have conspired to create a perfect storm for orphaned accounts. With more than half of all knowledge workers expected to work remotely[5], and cloud usage continuing to rise, there are more opportunities than ever before for orphaned accounts to be created and exploited.

The average employee uses dozens of cloud-based services every day to do their jobs, including:

- Virtual private network (VPN) accounts
- Cloud storage accounts (e.g., DropBox, Google Drive)
- Cloud-hosted email accounts
- Social media accounts (Twitter, LinkedIn, etc.)
- Travel and expense management accounts (e.g., SAP Concur)
- Customer relationship management tools (e.g., Zendesk)
- Legal and accounting tools (e.g., DocuSign)
- And dozens more!

Now, think about how you manage and control these accounts as a business. In most cases, they're probably managed by the individual employee. When that employee leaves the company or no longer requires access to an account, do you have a formal de-provisioning process in place? If not, your business is probably overrun with orphaned accounts you don't even know about.

Did You Know?

4 out of 5

companies (83%) companies fail to encrypt at least half the sensitive data they store in the cloud.[6]

What can I do?

To fix the problem of orphaned accounts, the two most powerful tools in your toolkit are visibility and automation. **Visibility** means the ability to view, catalog, and monitor user accounts across platforms, whether the account was created on a user device, in the data center, or in the cloud. Ensuring that security policies are consistently enforced across business applications is critical, as employees tend to choose the path of least resistance (e.g., using weak passwords or re-using passwords) when unmonitored.

Automation is the most efficient and effective way to implement consistent policies around account de-provisioning. Manual processes, by contrast, introduce the potential for human error and divert precious IT and security resources away from critical tasks. Extending automation to periodic account audits is also important to keep track of new accounts, inactive accounts, and potential issues such as signs of account takeover.

A third best practice for account security is to make sure that permissions and privileges are aligned with a user's current role. Accounts can be unwittingly orphaned as employees change jobs or departments and forget to de-provision their old accounts, creating an opportunity for hackers to move in and assume control of those accounts without being detected.

Of course, the *best* best practice is to use Zilla Security's automated access security and compliance solution. Formed in 2019 to address the growing problem of access security, Zilla is trusted by leading companies around the world to automate, manage, and ensure compliance and access security in today's multiplatform, cloud-centric business environment.

Learn More

To learn more about what Zilla Security can do for you, visit us at **www.zillasecurity.io.**

Sources

1. TBD.
2. NordPass, "Top 200 most common passwords," (https://nordpass.com/most-common-passwords-list/).
3. ExploitLabs, "15 billion stolen passwords on sale on the dark web, research reveals," March 03, 2021, (https://exploitlabs.de/news/data-breaches/15-billion-stolen-passwords-on-sale-on-the-dark-web-research-reveals/).
4. Apollo Technical, "19 Employee Retention Statistics That Will Surprise You," January 6, 2022, (https://www.apollotechnical.com/employee-retention-statistics/#:~:text=In%20the%202021%20Bureau%20of,looking%20at%20only%20high%2Dperformers).
5. Gartner, "Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021," June 22, 2021, (https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021).
6. Ehrlich, Chris, "83% of Companies Don't Encrypt All Sensitive Data in Cloud," Datamation.com, November 22, 2021, (https://www.datamation.com/security/83-percent-companies-dont-encrypt-all-sensitive-data-cloud/).