vericlouds

Protect Sensitive Data and Prevent Account Takeover with Compromised Accounts Detection “as a Service”

www.vericlouds.com

Executive Overview

It's no longer surprising to wake up on any given day to news of yet another mega data breach that has compromised hundreds of millions of user accounts. Most data breaches are difficult to detect and occur despite having moderate to advanced authentication mechanisms in place. What further perplexes high assurance authentication is that Two Factor Authentication (or 2FA) is not always enough to fully protect a company's most sensitive assets.

Cyber-attacks target weak links, and continue to bypass traditional security tools such as log-only SIEM systems. To proactively detect threats before they can do damage, you need a solution that allows you to quickly identify when credentials have been compromised or reused, and to act on that insight in real time.

Very few organizations can distinguish the genuine user from the sophisticated attacker. Even companies combining 2FA with contextual based authentication telemetry (device trust, IP reputation, geo-location, the protocol used to access an app, etc.) are doing so in response to an authentication attempt, and are not proactively identifying and mitigating compromised accounts.

With such large-scale breaches becoming commonplace, it is more important than ever to work with the best threat intelligence sources proactively and decisively, particularly when compromised credentials are detected in your customer or employee directories.

> “63% of confirmed data breaches involved weak, default or stolen passwords.”
>
> — 2016 DATA BREACH INVESTIGATIONS REPORT, VERIZON

Detection is the New Black

For decades, companies have used preventative controls to preserve the confidentiality, integrity and privacy of data which include static authentication schemes, passwords and SSL encryption. As information systems and networks have become more complex, and user’s consumption of data and services has increased, so too have the frequency of policy violations and data breaches that often go undetected for months, if not years. And though companies staff up a security operations center (SOC) to monitor logs of user activities and system events, it is not a sustainable model and clearly more must be done to minimize the risk of improper access.

An effective cybersecurity program cannot and will not prevent every attack. The more that accounts and passwords are stolen by hackers and data thieves, the easier it is for them to get through the front door with valid credentials, and the greater the damage that can be done. In Verizon’s 2016 Data Breach Investigations Report, stolen login credentials moves up the list of attack vectors used in data breaches over time[1] to the #2 position.

To understand how detection plays a role in risk mitigation and safer online experiences, we must first understand how stolen credentials make it easier for attackers to rapidly grow their list of victims at alarming rates.

Minimize Risk from Phishing & Malware Planting

Stolen credentials make phishing and malware planting easier for attackers as they provide access to the victim’s online accounts, re-used from previous breaches, and the ability to access other services, such as social networks, email, or cloud storage. An attacker can send phishing emails from the victim’s email service, increasing success rates. To scale the attack surface, an attacker would then add a malware payload to files (e.g., Word, Excel, PDF, .exe, etc.) in the victim’s cloud storage, so that when the victim opens the file, that machine is hacked. Once a machine has been hacked, the attacker is then able to move laterally throughout the organization until he gets access to accounts with escalated privileges.

What makes phishing problematic is that even sophisticated users, by some counts 34% of them, click on suspicious links out of curiosity[2]. That percentage only increases when the users are on Facebook[3].

Once organizations understand the weakest links, they can direct their resources and limited budgets to prioritize investments for enhanced protection from threats and improved ROI. Many of the existing security systems that detect phishing rely on catching IP addresses or URLs with low reputation (known for phishing) or blocking look-alike URLs.

[1] 2016 Data Breach Investigations Report, Verizon
[2] Source: https://www.scmagazine.com/34-of-users-click-on-links-due-to-human-curiosity/article/528147/
[3] Source: https://www.scmagazine.com/34-of-users-click-on-links-due-to-human-curiosity/article/528147/

Attack Vector	Solution
Malware	Network scanning /log analysis
Intrusion Detection	Anomaly detection
Phishing	Training/network scanning URLs
Server Vulnerabilities	Automated patching/threat intelligence
Account Takeover	Compromised account detection "as-a-service"

Cyber-attacks target weak links and continue to bypass traditional security tools such as log-only SIEM systems. To proactively detect threats before they can do damage, you need a solution that allows you to quickly identify when credentials have been compromised or reused, and to act on that insight in real time.

Reducing Mean Time to Detection & Resolution

Key performance indicators used to measure the success of a security program include mean times for incident detection and resolution. On one hand, these metrics can be viewed as arbitrary numbers for the sake of process improvement in organizations that use the ITIL methodology. On the other hand, effective leaders will see these metrics as critical measures of their organization's health and well-being.

In Mandiant's M-Trends 2016 annual report of cyber security trends, it was found that "the median number of days an organization was compromised in 2015 before the organization discovered the breach (or was notified about the breach) was 146." Although this number can easily be skewed by the organization reporting such incidents to make them look more effective than they are, it is only a slight improvement from the 205 days reported in 2014.

Therefore, it is critical for organizations to have the people, processes and technologies that enable them to detect advanced persistent threats. Attackers that can gain escalated privileges and access corporate intellectual property and customer PII are often able to stay long enough to cause significant and irreparable damage.

> "To proactively detect threats before they can do damage, you need a solution that allows you to quickly identify when credentials have been compromised or reused, and to act on that insight in real time."

The speed to detect incidents in real time for enterprise security must be complemented by the scale, correlation capabilities, and automation of compromised account detection. The ability to leverage threat intelligence such as a database of compromised accounts addresses the second most significant threat vectors and mitigates vulnerabilities before they can be exploited by attackers. Compromised account detection "as-a-service" is most effective when implemented in-line with authentication, as it puts the source of compromised accounts as close to policy enforcement and authorization as possible.

While the industry talks about how "continuous authentication" is the future of Identity & Access Management (IAM) – the idea that the username and password are merely a gateway to additional forms of authentication such as behavioral biometrics that monitor things like keystroke patterns – it strikes fear into users who spend much of their day struggling with logging in to multiple websites or resetting forgotten passwords. Knowing in advance which accounts can be used as an attack vector would be valuable to the extent that only users who have compromised accounts would be affected, and those who were affected would be notified interactively during login, significantly reducing the mean time to resolve a security incident.

This has significant implications for Identity & Access Management.

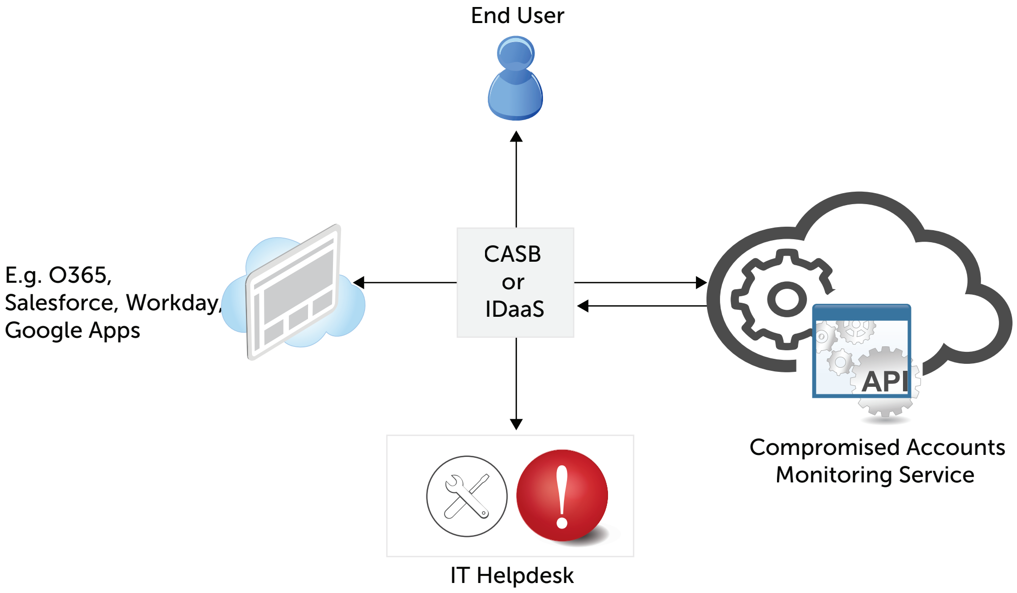
Implications for Identity & Access Management

Actionable Intelligence

Infusing IAM with "actionable intelligence," in the form of real-time risk information will enable a proactive security capabilities previously unavailable, making the next generation of IAM to be secure by default.

"Secure by default" may be achieved by overcoming one of the worst vulnerabilities that access management/ security solutions suffer from, which is the inability to recognize attackers with valid credentials. Today, security methods are entirely reactive. For example, when a hacker with valid credentials gains access, security measures are only enacted after user accounts display anomalies. By the time the damage may already be done; Files corrupted, corporate and personal data stolen, and client relationships impaired by the bad publicity that follows.

With knowledge of recently compromised accounts, a CASB or an IDaaS service provider can orchestrate the full recovery effort from notifying the end-user, to forcing a password reset and even automating the logging of a ticket in a company's helpdesk system. Backed with additional services such as machine learning and threat intelligence, the next generation of IAM stands to greatly benefit, inevitably becoming more intelligent and more effective than what most companies are used to today.



The value of actionable intelligence from a compromised account detection service increases dramatically when it's leveraged to monitor privileged users. Privileged users accessing protected systems are a greater risk because of their ability to delete log files, modify configurations and download entire databases of account information.

Forward-thinking companies such as Microsoft and Dropbox have publicly acknowledged their success in working with compromised accounts in-line during authentication. At Okta's annual conference, Patrick Heim of Dropbox readily admits that "decision-making processes and education just aren't scaling. We look proactively for threat intelligence." He goes on to explain their processes of working with compromised accounts and forcing password resets when compromised credentials are detected during authentication.

Alex Simons, during his talk *Getting Ready for What's Next with Cloud Computing*, explained, "We got a hold of that [compromised accounts list] and ran it against all of the hashes in our services and it wasn't a bad list. We got about a 0.5% hit rate on it, so we could protect all of those accounts."

The ability to proactively detect and remediate tens to hundreds of thousands of users at once has a huge payoff for the business in terms of preserving user privacy and minimizing the likelihood of a data breach occurring.

> “The ability to proactively detect and remediate tens to hundreds of thousands of users at a time has a huge payoff for business in terms of preserving user privacy and minimizing the likelihood of a data breach from occurring.”

2FA Is No End Game

Attend any conference or webinar on identity or security and you are sure to hear experts urging organizations to rush out and implement 2FA as though it were a silver bullet. 2FA can be effective, but only when implemented and managed properly. And unfortunately, that is not always the case.

Many existing 2FA implementations rely on the use of SMS for sending one-time passcodes for authentication. As of July 2016, the U.S. National Institute for Standards and Technology (NIST) acknowledges the risk that SMS messages can be intercepted or redirected, and encourages any service considering adopting two-factor authentication in the future to "consider alternative authenticators" as explained further in NIST Special Publication 800-63B. Many popular services continue to use SMS based authenticators, including banks, social media sites, email service providers, file sharing services, source code repositories and so on.

Even when organizations move away from SMS based 2FA, other alternatives for sending one-time passcodes such as email or downloadable static passcodes can also be compromised. Whether it be through stolen credentials sold on the dark web, session hijacking, social engineering or numerous other methods, this persistent vulnerability must be mitigated.

One of the most popular methods of obtaining one-time passcodes today is by storing and retrieving them from an authenticator app on a mobile phone. While this is a much more secure method than the previous ones mentioned, this approach quickly runs into usability and scalability problems. It cannot be assumed that everyone carries a compatible smart phone, or that they always have it in their possession. What's more, configuring and re-configuring accounts in an authenticator app can be a hassle, especially for those who are not tech savvy. Authenticator apps can also be challenging when supporting scenarios such as multi-user accounts, multiple accounts on the same service, and so forth.

> “Prevention is a failed strategy.”
>
> — AMIT YORAN, PRESIDENT, RSA, THE SECURITY DIVISION OF EMC

Amit Yoran, President of RSA, is fond of saying that "prevention is a failed strategy." Organizations can and should do more to compensate for weak security and human error to improve their security posture. Organizations are looking to their IDaaS providers and CASBs for the answers.

VeriClouds Services Platform

VeriClouds has built a data repository of leaked account credentials that tells you in advance which accounts can be used as an attack vector. VeriClouds services are designed to be used in-line with authentication to proactively detect and remediate potential threats across a broad range of applications and infrastructure.

If a user's account credentials are stolen and leaked, or sold online, you can easily force users to reset their credentials immediately to mitigate any risk. VeriClouds makes it easy to both detect those users that have been affected, and prevent a compromised account from doing any further damage.[4]

When working with compromised accounts, Patrick Heim, Head of Trust & Security at Dropbox, has a reported "success rate of 85% when combined with other contextual attributes." [5] Dropbox manages credentials for over 500 million users, and considers the use of verifying compromised account credentials during authentication a mandatory access control, such that it functions in-line with every authentication to their service.

Deployed on AWS, the VeriClouds Services Platform is architected to be both secure and highly available. Other advantages of choosing VeriClouds as a provider of compromised account detection "as-a-service" include:

Largest Repository of Compromised Accounts VeriClouds leverages the dark web and other sources to build a database of compromised credentials and make it available to customers to help them secure their networks. With one of the largest repositories of compromised accounts in the industry built on top of a SaaS platform, VeriClouds customers can be confident that they have the best source of compromised accounts, continuously updated, to reduce the risk and harmful effects of a data breach.

Increased Speed & Superior Visibility When there are known incidents, the speed of response and remediation of compromised credentials make up more than half of the total cost of an incident. But not all compromises are known right away, and many of them can be avoided.

Custom Integrations The value of VeriClouds services increases rapidly as VeriClouds continues integrating with popular IDaaS and CASB solutions, leveraging holistic monitoring of SaaS services, threat protection and automated incident management. Integrating and uniting these platforms closes the loop. It unleashes the full power and potential of compromised account detection "as-a-service."

[4] VeriClouds service maps to the Detect function of NIST's Cybersecurity Framework Core Structure, whereas the service provider is responsible for developing their own algorithms and implementation of Respond and Recover capabilities.

[5] CSO Panel: Cloud + Mobile Security Strategies at Oktane 2016 in Las Vegas

Built on Trust Principles VeriClouds engages in “white hat security research” to prevent threat actors from gaining unauthorized access to customer accounts, and operates to promote security and safety for the true owner of the data or person entitled to the data.

VeriClouds works closely with a team of attorneys to proactively address liabilities and mitigate some of the risks of handling compromised accounts for you. The VeriClouds Services Platform has a patent-pending technology utilizing a one-way hash function to ensure privacy and compliance when handling potential PII and other sensitive data.

VeriClouds can provide an on-premises version of its compromised accounts database for customers with strict data handling requirements, or who wish to have a local instance to minimize the effects of network latency.

Conclusion

Data breaches can pose severe financial and reputational consequences for businesses. Organizations need to think differently about cyber-security. The emphasis should be on proactively improving security posture through leveraging threat intelligence sources, such as Compromised Account Detection "as-a-service", rather than worrying about what users are doing.

With knowledge of recently compromised accounts, an IDaaS provider or a CASB can orchestrate the full remediation from notifying the end-user, to continuous authentication and automating the logging of a ticket in a company's helpdesk system.

By automating the detection and response of known and future compromised accounts, VeriClouds Services can minimize the risks and costs that occur as a result of phishing, malware, or more wide spread data breaches.

About VeriClouds

VeriClouds is a SaaS company that resolves authentication security issues in cloud services. Founded in 2014 by Rui Wang, who has a PhD in cybersecurity, and Stan Bounev, a successful entrepreneur with over 14 years of corporate and startup experience in the banking and technology industries, VeriClouds has built one of the industry's largest databases of compromised accounts.

Contact Info

For more information:
info@vericlouds.com
www.vericlouds.com
@vericlouds