Account Takeover (ATO) Attacks Simply Don't Matter

Stan Bounev, VeriClouds Chris Olive, RSA

Account Takeover (ATO) attacks seemingly just don't matter. That's the conclusion a semi-informed outside observer might make, based on how these pernicious attacks are being addressed by the cybersecurity community.

That ATO attacks desperately *need* to be addressed, and addressed in the right way, should go without saying. For the last few years, the statistics around ATOs have been fairly eye popping. Individuals are *still* using the same password across accounts at a 60% to 70% rate. Compromised credentials *still* account for some aspect of the breach vector in about 75% of all breaches in the last three years. And a recent Verizon report indicated that 90% of retail login traffic can be attributed to credentials stuffing attempts.

If you believe protecting from ATOs is relatively easy to do and doesn't need a "re-think," perhaps you don't need to read any further. But if you're interested in considering a significant "re-think" around your ATO strategy, we definitely invite you to continue reading.

Convoluted Solutions to a Real Problem

Almost as problematic as ATOs are the attempts by the cybersecurity community and within the ATO vendor space to address this growing problem.

We haven't formulated the correct approaches, we haven't articulated the problem correctly and how to solve it, and the "solutions" presented are fairly pedestrian and therefore far less effective as the statistics above indicate. Amazingly, a number of so-called "solutions" can actually *increase the footprint of ATO attacks through insecure solution offerings, further exposing organizations*. Consider the irony here.

> *When we consider [the] axiomatic trend within cybersecurity, juxta positioned against current pedestrian approaches and the incredible risk around ATO, determining a visionary commercial vendor in the ATO space becomes absolutely paramount.*

The Right Solution

When protecting from and mitigating ATO attacks, organizations essentially can choose between two main approaches.

The first approach involves leveraging an organization's security operations center (SOC) to monitor, detect and attempt to mitigate ATOs through use of threat intelligence. This approach is far too slow, doesn't scale well or cost-effectively, is manually executed, and is therefore prone to a lot of mistakes, oversights and reaction to a lot of false positives.

The second approach involves much more automation around detection and mitigation of ATO attacks. This has opened the door to interpretation within the industry as to the best approach in applying automation.

VeriClouds has solved automating and mitigating ATOs from the beginning with a number of important approach nuances in mind. The best approach is to leverage the existing IAM infrastructure and integrate the compromised credentials intelligence throughout the entire credentials life-cycle in organizations, from account set-up to authentication and password reset.

Most of the few existing commercial solutions – outside of the outright inane approaches, such as completely ignoring the problem, or the "download periodically from Have I Been Pwned (HIBP) and call it 'good'" approach – still aren't delivering a solution effectively in three key areas:

- Delivering key automation, aimed at the right points within a customer IAM implementation
- Delivering accurate results with no false positives, factoring *both* the user ID and the password
- Delivering the most *secure*, zero trust solution

Delivering Accurate Results

VeriClouds delivers pinpoint accuracy and no false positives by comparing all aspects of user credentialing, not just user IDs. A number of other services use only the user ID, which leads to false positives and inaccurate results. It's difficult to drive IAM mitigation and remediation strategies unless high assurance exists around any integrated intelligence.

Invariably, accurate results play hand in hand with a secure approach. **Delivering a secure approach based on zero trust that also provides accurate results is what sets the VeriClouds solution apart** from the rest of the compromised credentials intelligence landscape.

Protecting against ATO attacks will need to go beyond linear, deterministic approaches.

Delivering a Secure Solution

At VeriClouds, we believe providing insecure solutions to problems stemming from insecurity simply makes no sense at all. Some vendors require full uploads of your sensitive credentials data into their clouds, including in some cases, actual cleartext passwords! A solution provider shouldn't be adding additional risk or simply moving the risk to another threat area as part of the solution offering.[1]

VeriClouds has a strong commitment to enterprise security and is heavily invested in taking a zero trust approach to any of our solutions provided in the cybersecurity space. VeriClouds purposefully masks itself from seeing credentials or the results from real-time credential comparisons on the client side using encryption and obfuscation. This approach also shields our customers from seeing or storing passwords that aren't owned by their organization. We even offer a secure, easily deployed, on-premise appliance that provides credentials intelligence for isolated, completely on-prem, offline comparisons.

Consider the value of a zero-trust solution in an area of such high intelligence and high risk in contrast to other solutions in the ATO space that require full uploads of your organizational data, sometimes even in clear text.

Presented here is how VeriClouds approaches and delivers its solution, nuanced and differentiated from other commercial solutions in the three key areas aforementioned.

Delivering Correctly, Aimed at Key Automation

Simply providing APIs does not necessarily equate to automation. What is required to use those APIs, the data those APIs provide, and their intended use or integration points all play into the effectiveness of the solution.

VeriClouds' solutions are specifically aimed at increasing the intelligence offered to and leveraged by components of an organization's existing IAM infrastructure, easily integrated at strategic points of their choosing to provide automated and intelligent remediation.

Active and passive application of VeriClouds' comprehensive credentials intelligence and password analytics is entirely possible throughout the strategic layers of your organization across IAM vendor product portfolios. This is the most effective and strategic approach and follows a clear path into the future as IAM continues to reshape itself as becoming more and more component driven.

Amazingly, a number of so-called "solutions" can actually increase the footprint of ATO attacks by offering insecure solutions, further exposing organizations.

The security of VeriClouds' services is the main reason large organizations from Financial Services, Healthcare, Retail and cybersecurity vendors choose to work with VeriClouds.

The Future of ATO Protection

Very few cybersecurity domains have remained unchanged, or rather should we say unchallenged, over the lifetime of those domains. Nearly every cybersecurity domain has iterated over time out of necessity. When we consider this axiomatic trend within cybersecurity, juxta positioned against current pedestrian approaches and the high risk around the ATO solutions domain, determining a visionary, forward thinking commercial vendor in the ATO space becomes absolutely paramount.

VeriClouds is already investing in the future, developing and offering innovation in the area of credentials threat intelligence and what we believe is the emergence of password analytics.

In the very near future, protecting against ATO attacks will need to go beyond linear, deterministic approaches. We're already working on:

- Protecting users and organizations from *all* previously leaked passwords of their users (not just simply a point-in-time submitted check), including leaked personal and corporate passwords.

[1] Full uploads of critical credentials data (sometimes required in clear text) into a solution providers cloud introduces a lot of new risk to your organization. How secure is their cloud and immune from attacks, breaches and subsequent leakage? Who of their personnel see and have access to this data? What are the data retention and redaction policies on your data? Why add risks while attempting to *mitigate* risk?

- Protecting against passwords *similar* to past leaked passwords. We understand how individuals attempt to formulate, iterate and change their passwords[2], as do attackers.
- Preventing the use of previously leaked passwords by other individuals found across all previous breaches (outside the domain of any user in question)

The above are some of the ways VeriClouds can start protecting now against attack iterations the dark underworld is already formulating and aiming at organizations.[3]

The bottom line is that static, linear comparisons and other inane approaches such as rolling your own integrations with "freeware dumps" or full credential uploads into a third-party vendor cloud service aren't going to cut it. Why invest any of your time, money and effort into any of those approaches?

As already mentioned, VeriClouds offers organizations an **on-site device** that allows offline comparisons without any connection to the internet. No other vendor in the ATO solution space offers such critical intelligence to organizations, completely isolated and offline, and completely safeguarding your critical credentials data.

[Fully integrated into your existing IAM] is the most effective and strategic approach and follows a clear path into the future as IAM continues to reshape itself as becoming more and more component driven.

Putting It All Together

Let's just be real: ATO attacks matter *a lot*. ATO attacks are pernicious threats that difficult to detect and mitigate due to their nature, the attack approach and the attack surface. Solutions provided in this space are problematic because it typically involves providing intelligence to a third-party provider, often in insecure ways, further increasing your risk rather than diminishing it.

VeriClouds believes any solution offered *must* be easily automated at the right points within your organization, *must* be delivered accurately and above all, *must* be delivered securely. And then going beyond the here-and-now, the solution *must* be future positioned, forward-thinking and ever-iterating to continue mitigating the evolving ATO threat domain.

[2] Users create passwords using a certain "psychology" that becomes easier to predict using predictive analytics leveraging gigantic amounts of credentials data, widely available to and already in use by criminals on the dark web.

[3] Criminal organizations do not solely rely on simply trying batches of compromised credentials, but actually generate new attacks based on a corporate email taxonomy and previously leaked passwords. For instance, using the top one hundred thousand leaked passwords along with *iterations* of the corporate email taxonomy to perform a brute force attack, leveraging predictive analytics.