IMPERVA®

Top 5 Solution Requirements for Account Takeover Protection

PLAYBOOK

Executive Summary

Account takeover attacks are a significant problem for the customer, partner and employee facing web applications that have become the backbone of the modern business. By providing cyber criminals with authorized access to legitimate user accounts, such attacks threaten to demolish the user-provider trust paradigm and completely unravel the web application fabric upon which so many of today's organizations rely. Left unchecked, the costs can be enormous, ranging from loss of confidential data, customer trust, and brand reputation to significant operational disruptions and financial damages.

This paper puts forth five essential requirements IT security teams can use to evaluate candidate solutions for account takeover protection. It also explains how Imperva SecureSphere Web Application Firewall with ThreatRadar Account Takeover Protection addresses each requirement, providing organizations with an ideal solution to the account takeover problem.

Account Takeover 101

According to the 2015 Verizon Data Breach Investigations Report, more than half (50.7%) of the web application attacks seen in 2014 involved the use of stolen credentials. Losses from related fraudulent activities tally in the billions of dollars per year and extend well beyond the retail and banking sectors. Organizations from all verticals are susceptible. All it takes is a public facing web application with user accounts. In addition, the potential impact extends beyond fraud to include theft of sensitive information, such as personal medical data, tax records, and intellectual property.

"50% of web application attacks use stolen credentials"

2015 VERIZON DATA BREACH INCIDENT REPORT

Account Takeover Fundamentals

As they pertain to web applications, account takeover attacks typically incorporate the following elements:

Step #1 -- Harvest Credentials. Hackers purchase or otherwise gather account credentials harvested from various data breaches.

Step #2 – Test Credentials. Taking advantage of bot networks and hiding behind anonymizing systems (e.g., proxy servers and Tor relays), they then "probe" accessible web applications to find accounts where the stolen credentials work.

Step #3 – Gain Access. With usable credential-account pairs in hand, the hackers can pass right through most perimeter and access control defenses by posing as authorized users of the target applications and services.

Step #4 – Steal Assets. Depending on the nature of the compromised accounts/applications, they can pursue a wide variety of deleterious activities, such as transferring money, cancelling services, viewing sensitive medical information, or even stealing additional credentials.

Alternately, hackers can skip the 'test credentials' step by using man-in-the-browser, keylogging trojans, and other types of credential harvesting attacks to directly obtain usable credential-account pairs from unwitting users with compromised devices.

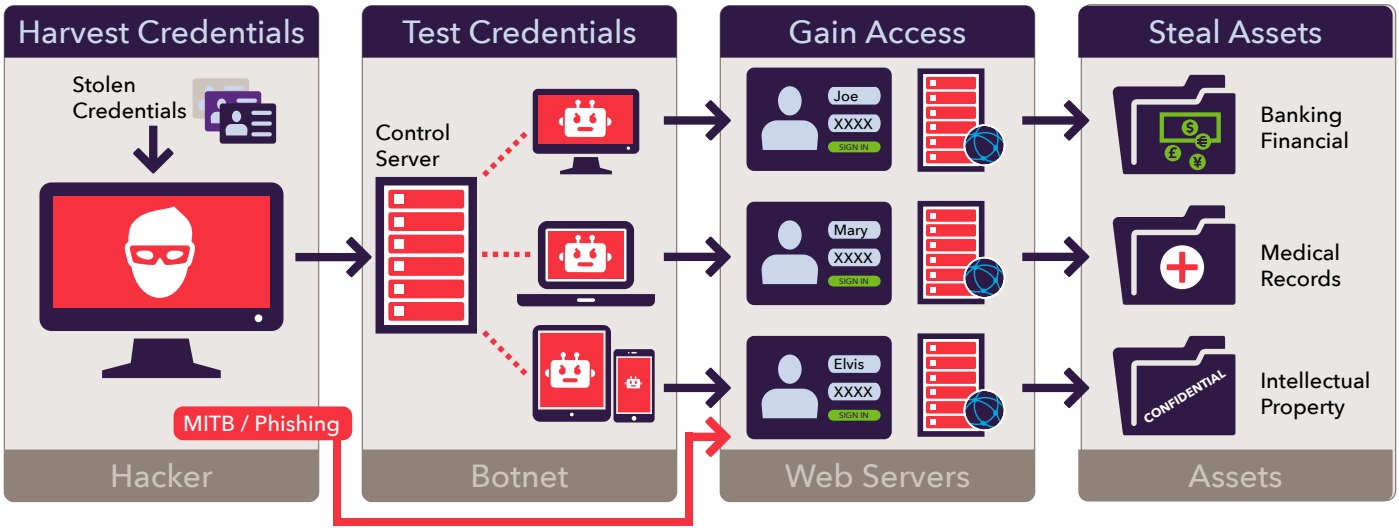

Figure 1: Anatomy of an Account Takeover Attack

Fixes or Flops?

Part of the challenge for IT security teams is the relatively modest effectiveness and drawbacks of the tools and techniques traditionally used to thwart this class of attacks. For example:

- Two-factor authentication technologies are not only expensive to deploy and intrusive to users, but also have proven highly susceptible to man-in-the-browser attacks.
- Real-time transaction monitoring and risk scoring systems that rely on statistical models have, for a variety of technical reasons, consistently been plagued with high rates of false positive and/or false negative indications.
- Fraud analysis systems are typically complex and costly to operate, while also being completely reactive. Instead of preventing unauthorized activities and incidents from occurring in the first place, they only detect them after the fact.

Although each of these countermeasures has a role in an organization's overall security strategy, it is clear that IT security teams require something further to more effectively get a handle on the growing account takeover problem.

The Evidence-Based Indicator Approach and ThreatRadar Account Takeover Protection

The evidence-based indicator approach involves applying intelligence – perhaps about the client device used to connect to a web application – to help address the account takeover problem. For example, if existing intelligence indicates that a device has a history of being associated with malicious or fraudulent activity not only across the broader online community but also on your organization's network, then that would amount to probable – if not definitive – cause for blocking it from ever making a connection to your web applications in the first place.

Although it is only a simple example, this capacity for intelligent blocking demonstrates the tremendous potential of the evidence-based indicator approach. As with any relatively new class of solutions, however, evaluators need to be aware of the considerable variation that exists among available offerings.

To help organizations avoid the consequences of selecting a deficient solution, the following sections describe five important requirements IT security and fraud teams can use to evaluate candidate offerings. Each section also includes details on how Imperva SecureSphere Web Application Firewall with ThreatRadar Account Takeover Protection addresses the corresponding requirement.

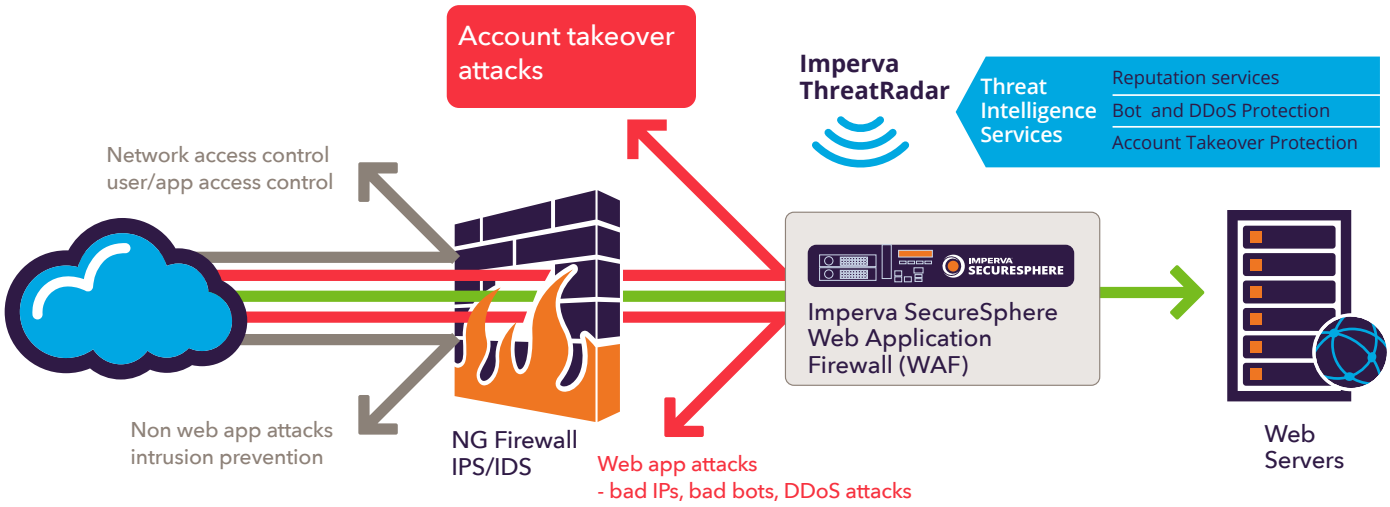

Figure 2: Imperva SecureSphere Web Application Firewall with ThreatRadar

As a subscription service, Account Takeover Protection helps IT security teams get in front of the account takeover problem by enabling the market-leading SecureSphere Web Application Firewall to accurately detect and block these insidious attacks, both during the initial login process and throughout an active user session.

Requirement #1: Intelligence that goes beyond the basics

Information on whether or not a device has been associated with malicious or fraudulent activities is only a starting point. Ideally, available intelligence should be richer and more informative, extending not only to illuminate other device-oriented attributes but also details about the credentials submitted at login.

ThreatRadar Account Takeover Protection arms the SecureSphere Web Application Firewall with a powerful combination of both device and credential intelligence. At the heart of the service is the real-time computation of risk rating of the client device, based on insights into good/bad activity of over 2.5B global devices that is available to the solution. The embedded set of security policies that apply this intelligence, results in the ability to identify and mitigate a wide range of account takeover indicators and threats, such as:

- Repeat offenders – by detecting devices and IP addresses already associated with fraud and abuse at other businesses, or that have been registered on your company's own blacklist
- Anomalous activity – by detecting suspicious scenarios where a single device is accessing too many accounts, or a single account is being accessed by too many devices
- Evasion techniques – by detecting the use of anonymous proxies, Tor, and geographic location masking
- Credential testing, also known as "credential stuffing" – by detecting multiple login failures from the same device using credentials known to have been stolen in a past breach
- Dictionary attacks – by detecting repeated/excessive attempts from a single IP address to login using weak or commonly used passwords
- Privileged account attacks – by detecting repeated/excessive attempts from a single IP address to login into known privileged accounts

To engage these capabilities, administrators simply select which pre-defined detection policies to apply for each site, server group, application, or service SecureSphere is protecting.

Requirement #2: Extended correlation to improve detection accuracy

Maintaining state machines to help detect attacks that stretch out over time and correlating multiple pieces of device and credential intelligence are essential capabilities. But what happens when the system returns a risk rating of medium for a set of detected conditions? Should the corresponding session be blocked, or not? Ideally, it should be possible to incorporate and correlate additional types and sources of intelligence, network activities, and system events to bring further clarity to the situation.

Account Takeover Protection is not the only ThreatRadar intelligence subscription available to Imperva customers. Others include Reputation Services for flagging troublesome source IPs and Bot Protection for identifying known botnet clients/servers. By combining such data with that available from Account Takeover Protection, SecureSphere compiles a more informed picture of what is really going on in any given situation, thereby enabling a more definitive and appropriate response to be taken.

A straightforward example is one where credential stuffing is suspected but the risk rating is only medium because the frequency of attempts does not exceed the threshold that warrants a high rating. In this case, if the system also had evidence that the client was a Bot, then the need to block all activity from the associated source would be crystal clear.

By crafting custom policies, administrators can also correlate any other piece of data available through SecureSphere, such as irregularities in how HTTP or XML services are being used.

Requirement #3: Real-time protection (not just detection)

A significant shortcoming of many alternative tools and techniques is that they only detect compromised account activity and fraudulent transactions after the fact. Intelligence-driven solutions can be similarly deficient depending on the point at which they apply intelligence in the "lifecycle" of an application session. Sooner (e.g., at login) is better than later (e.g., when analyzing transaction records). Another important consideration involves the capacity – or lack thereof – to actually block offending sources and their traffic.

A major strength of the Imperva solution is that protection against account takeover is provided upfront, right when a user first logs in. Because the SecureSphere Web Application Firewall is deployed in-line in front of protect web applications – as opposed to being an out-of-band management system – the solution is also fully capable of blocking designated devices, IPs, and traffic. The net result is that known bad actors and devices are stopped in their tracks, never getting the opportunity to execute fraudulent transactions or otherwise cause harm.

For successful logins, the solution continues to monitor ongoing application sessions, both for any changes to a device's risk rating (e.g., due to updated intelligence data), as well as for any behaviors that might be indicative of an account takeover attack (e.g., accessing multiple different accounts in a short period of time).

Configurable options for responding to different combinations of event types and risk ratings include allowing a session to proceed, sending an alert, and – of course – blocking all activity from a given source.

Requirement #4: Seamless deployment and user experience

Solutions that are challenging to deploy or negatively impact the user experience are a drain on valuable resources and run the risk of being circumvented.

Cloud-based ThreatRadar subscription services arm an organization's existing SecureSphere installation with pre-defined security policies that are very simple to deploy and customize. With the Imperva solution:

- There is no need to re-code/compile your web applications to include API calls or, for that matter, to modify them in any way at all;
- There is no additional software or hardware to deploy;

SecureSphere delivers robust protection without the need to restrict choice of device or impede user progress with extra steps, such as multi-factor authentication, device registration, or confusing schemes where "step-up" authentication is required in the middle of an active session. Highly accurate intelligence and extended correlation capabilities further reduce the impact on users by minimizing the occurrence of false positives and inappropriate blocking of legitimate application requests.

Requirement #5: Streamlined security operations

Solutions that require considerable effort to configure, operate, and maintain – perhaps because they are little more than a set of APIs and/or a software development kit – are less than ideal for today's time-challenged security, operations, and incident response teams.

With SecureSphere and ThreatRadar, not only is initial deployment a snap, so too is configuration and ongoing operations. For each resource requiring protection, administrators simply select from pre-defined sets of detection and enforcement policies those they wish to enable. Administrators also have the flexibility to fine-tune the sensitivity levels for individual detection policies so they better align with their organization's specific tolerance for risk.

Powerful, pre-defined reports provide visibility into the finer details of what is happening and the need, potentially, for further action. Examples include reports identifying both compromised devices and compromised application accounts. In addition, having fewer false positives and negatives to contend with translates into fewer incidents to investigate, fewer fraudulent transactions to "back out," and fewer security breaches to clean up.

Finally, automated content updates not only ensure the freshest, most accurate device and credential intelligence, but also provide immediate access to new protection policies and report templates as they are released.

Conclusion

Account takeover attacks are a growing problem that threatens to unravel the web application fabric upon which modern business relies. With multi-factor authentication and transaction analysis tools failing to stem the tide, IT security teams need to consider deploying an intelligence-driven solution that is capable of accurately detecting account takeover threats and actually stopping them before they cause any damage. Solutions that fully address the five essential requirements explained herein – like Imperva SecureSphere Web Application Firewall with ThreatRadar Account Takeover Protection – not only mitigate the risk of account takeover accounts, but also minimize the workload placed on security and fraud teams, streamline forensic investigations, and ensure a hassle-free user experience.

To learn more about SecureSphere, ThreatRadar, and other Imperva solutions for protecting your organization's data, applications, and reputation, please visit imperva.com