WHITE PAPER

exabeam

DETECTING COMPROMISED CREDENTIALS WITH UEBA

OVERVIEW

All of the biggest data breaches, judged either by number of records breached or the importance of the data stolen, have involved attackers leveraging stolen user credentials to gain access. In many cases, the credentials were phished from a company or government agency employee, meaning an employee clicked on a planted link and unknowingly handed over his or her credentials. These attackers went on to impersonate employees, escalate privileges and, in some cases, create highly privileged phantom user accounts. Most enterprises and government organizations that experience data breaches have traditional security point solutions, log management, and security information and event management (SIEM) solutions in place. However, SIEM is not a comprehensive solution on its own. There has been a great deal of focus on the attack-chain (see figure 1) – or kill-chain – of steps in the process leading to these breaches.

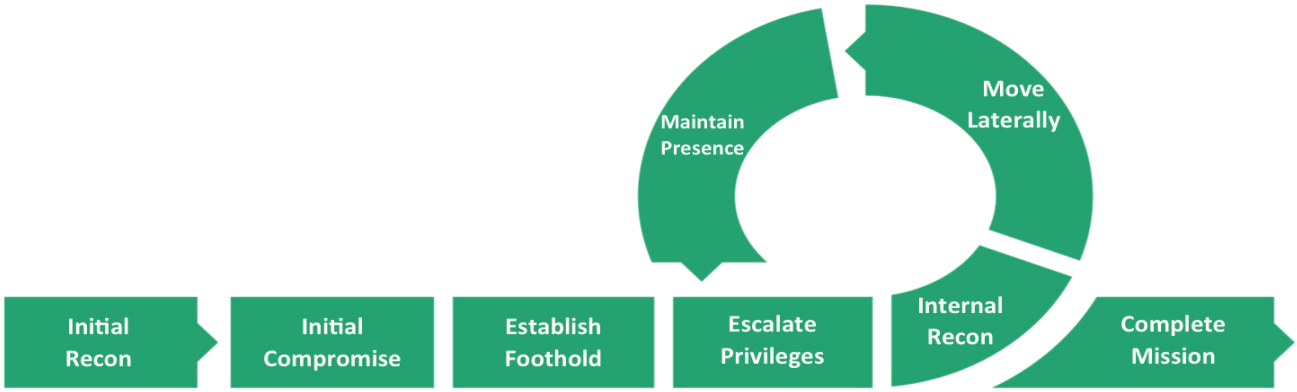

Figure 1 – Mandiant's Attack Chain – APT-1 Report 2013

Monitoring each individual step in the attack chain requires watching for a different set of conditions using different security technologies. If one of the security sensors deployed detects activity in a portion of the attack chain, an alert goes to the SIEM. The current incident response process would be for someone in the security operations center to review the alert and confirm it is not a false positive. Once this is done, it might be forwarded to a tier two or tier three security analyst who would begin the process of asking his own set of exploratory questions, pivoting through large amounts and multiple types of data collected over weeks or months looking for related events that might tie back to the original alert. If related events are found, the next step is to determine attribution for the attack. Finally, a "patient-zero" determination will be made, as a starting point for cleanup and an after-action report will follow. The recommendations in the after-action report, depending on the size or the importance of the breach, will likely get the attention of the CEO and board of directors. Businesses will then often increase the security budget to add more personnel and buy additional, newer security software or hardware that will monitor individual parts of the attack chain. This creates the security version of an arms race that can't be won.

In another organizational silo, IT operations is getting calls from users whose computers are not behaving in a way they expect, and from leaders in different parts of the business that see key business system performance degradations. Subtle clues that the system is owned by an attacker include, among others, the cursor that moves a little by itself, the camera that turns on and then off, or the system that suddenly starts using excessive amounts of the CPU or freezes up, inconveniencing customers or employees.

These clues don't go unnoticed by users; these attack symptoms have all been reported to the IT help desk before. There is usually no work-flow in place to investigate these system behaviors as potential security incidents. In many cases, these incidents either stop by themselves or the user solves the problem by re-booting their system – until the next time.

LEGITIMATE USER AND ATTACKER GOALS

The goals of the attacker and the goals of your employees are not the same, yet both use the same systems and perform the same actions as a means to an end. Employees, depending on their role in the organization, send and receive email, surf the Web, access internal information portals, cloud-based customer relationship management (CRM) products and business process management (BPM) systems. Some employees may be responsible for system or application maintenance and may have credentials that allow them to view and alter files and system configurations. Others may have more sensitive access rights to see customer information, sensitive business data or health information. All of these employees use IT services and communicate via a corporate network, and all the employees are networked together for the benefit of the business.

Most cybersecurity experts agree that the weakest link in an organization's cybersecurity systems is its own employees.[1] According to Dmitri Alperovitch of CrowdStrike, Inc., a cybersecurity consulting firm, research has found that between five and ten percent of employees will click on almost any email.[2] One click, and the victim's computer will automatically run a small program that enables full command and control of the users computer by an attacker malicious executable with no noticeable change to a computer system.

The goal of the attacker is to steal the victim's valid credentials and look like a legitimate employee going about his normal business, for as long as possible. The attacker wants to find out the limits of the victim's access rights and what other employees interact with the victim. If the user happens to have access to the desired systems and applications, the attacker will get what he wants, which can be anything from email attachments, network diagrams, source code or any other data that is of value or will help meet the attacker's goals. If the user doesn't have the desired level of access, the attacker will jump from system to system until he finds the right victim.

TRADITIONAL HOST AND NETWORK-BASED PROTECTIONS

Most businesses use anti-virus software, perimeter security systems and intrusion prevention systems. Some have host- or network-based data loss prevention (DLP) systems in place. Nearly all medium to large businesses have some SIEM in place to gather all security data and monitor for alarms generated by a wide variety of log sources, as well as provide correlations based on the IP address, hostname, common vulnerability and exposures (CVE) or common vulnerability scoring system (CVSS), or time of day. Some of these devices claim to perform anomaly detection through statistical analysis. These systems support monitoring for the number of times something happened how long an action took, or the size of file transfers between to hosts. However, these systems don't tell you who initiated a data transfer or whether the systems are legitimately exchanging data via an application program interface (API). The system simply says what things are statistically anomalous without any prioritization; leaving the response team to piece together the entire event context before realizing valuable time was wasted on responding to a false positive.

WHEN MATHEMATICS ALONE ISN'T ENOUGH

Many SIEM providers have recently added out-of-the-box algorithms that can be used to determine how rare an activity is, how long an activity took, or how much data passed between systems. Canned algorithms are of limited value where people are concerned and can lead to trading one set of false positives for another. Vacations and new employees skew results because most algorithms don't account for days off or new, but normal behavior. The after-hours access by an employee may look like a rare event and fit into an algorithm being used to detect attacker access, but in reality is a false positive. This is especially acute when thinking about organization dynamics. Role changes inside of an organization cause variations in behaviors that aren't easily dealt with by off-the-shelf mathematical algorithms. The larger the organization, the more error prone this approach can be. In a single large organization, there can be many routes to corporate information stored on a group of SharePoint servers. Credential sharing (yes, many organizations still do this) may get you to an anomaly (or not), but not attribution. Security data in general doesn't lend itself to pure statistical analysis when analyzing user behavior.

[1] Chinese Hackers Show Humans Are Weakest Security Link (Bloomberg News, May 19, 2014).

[2] Alleged Chinese Hacking: Alcoa Breach Relied on Simple Phishing Scam (WSJ, May 19, 2014).

USER BEHAVIORS: THE DIFFERENCE BETWEEN TOO MUCH DATA AND THE RIGHT DATA

Many organizations have turned to big data solutions to collect and analyze the large volume and variety of data generated at high velocity by user interactions with systems on the network and from their security infrastructures. With a few exceptions, many of those big data systems are Hadoop-based and bolted onto a SIEM. While capturing and analyzing data is important, without focus and context it can turn into security noise pollution. Turning up the volume from eight to eleven doesn't do anything to help you hear the whispered conversation across the room. Much of the data isn't relevant when looking for attackers who may already have valid credentials. Organizations are beginning to realize that detection of attackers who have obtained authorized credentials requires a new mindset--***the attacker is already inside***. Having this mindset means prioritizing four types of data.

- At the core is normal user credentialed activity data or **behavior data**. This consists of virtual private network (VPN), domain controller logs, lightweight directory access protocols (LDAP) logs, application logs, single sign-on data, and certain Windows (Kerberos) and Unix logs. Understanding the normal behaviors of users makes attacker behaviors easier to spot.
- **Business data** is needed to understand the user's actions in the context of who they are, whom they communicate with and what systems they access. Additionally, the business contact information contained in active directory provides the incident response team with the contact information they need to respond as quickly as possible once anomalous activity is detected.
- **Fact-based data** from systems such as FireEye, Palo Alto (Wildfire) and Sourcefire provide the network perspective of behaviors that can be tied back to the user.
- **Threat intelligence data** is used to relate the discovered bad behaviors with the outside world.

While other types of data are important and can be related to parts of the attack chain, they aren't the most relevant when searching for attackers impersonating users using behavior analysis.

FOCUSING ON USER AND ATTACKER BEHAVIORS AND CHARACTERISTICS

While all the employees in an organization have different roles, rights and responsibilities, they all have several things in common:

- **Credentials are required to perform job responsibilities**. These are either provisioned for them as part of a process or are self-provisioned and logged.
- **Remote access is used enabling BYOD**. This is done on a system or application basis, via VPN, single-sign-on portal or other means. Users log into cloud-based or locally hosted applications and operating systems.
- **Mobile devices are used for work functions**. Mobile devices that are used by employees outside of the corporate network usually don't have the same protections of mail filtering or proxy servers. This makes them easier targets for phishing and other social engineering techniques.
- **People are creatures of habit** – When accomplishing legitimate business tasks, the characteristics of users' access (to what, from where, what time, what system, which identity used, etc.) conform to a pattern over time as compared to themselves or their peers.

Attackers with valid credentials look just like regular users; the only difference is the objective. The objectives of your regular employees and attackers diverge when examining behaviors and the characteristics of the access. It's the characteristics and anomalous behaviors that make attackers detectable.

ENTER EXABEAM

Exabeam is a security intelligence solution that will take the mountain of data collected by a log management or SIEM system and identify anomalous characteristics of access and behaviors. Remember our attack chain? Many of the phases in the chain are enabled by the attacker's use of stolen credentials. To make this plain, we've added the potential use of credentials in the gaps in the original illustration.

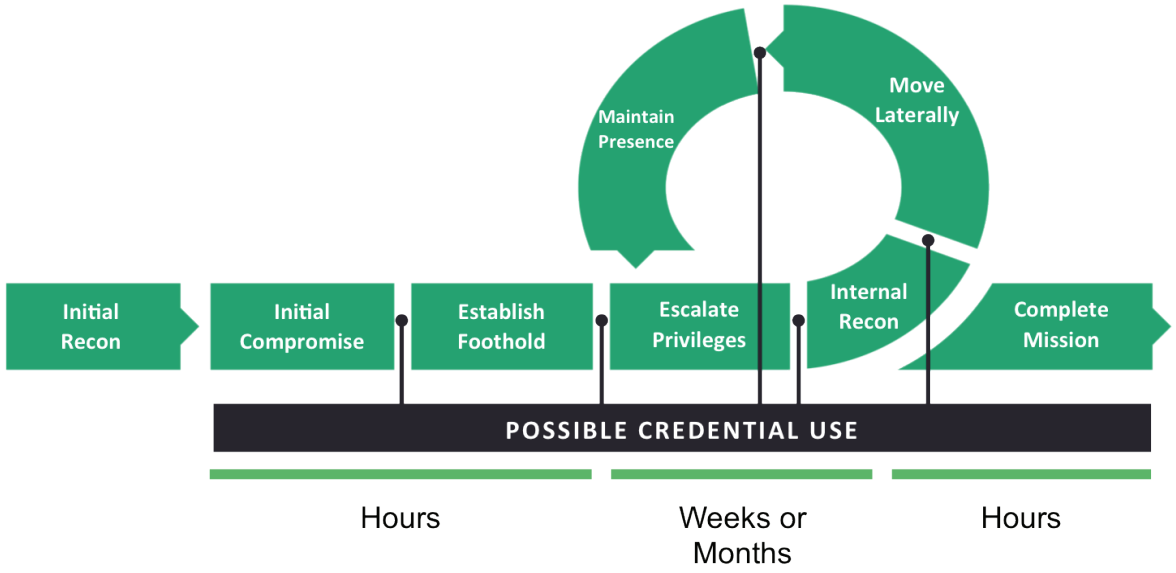

Figure 2 – Credential Use Added by Exabeam Overlay in Mandiant's Attack Chain

There are security point products that watch for initial compromise and there are in-line data loss prevention products that watch for data exfiltration. Exabeam monitors the portion of the attack chain where the attacker spends the most time and is the least visible.

As log data is collected, it's enriched with business context information that is appended to each log entry. For each user's behaviors and characteristics, security session assembly is performed so that all activities from log on to log off can be examined. These sessions can include fact-based information (as described above) that can be attributed to a user's activities. Meanwhile, the system learns and remembers behaviors and access characteristics for all monitored users, and identifies anomalous characteristics and behaviors. The risk engine then scores all anomalous characteristics and behaviors based on a proprietary combination of algorithms and provides a per-session risk total. The session risk tipping point at which an alert can be generated is set by an individual enterprise.

ACCELERATING THE SECURITY INVESTIGATION PROCESS

User sessions can be viewed on a timeline for trending purposes and to know whether a risk score built up slowly over time or all at once. For each session, reasons are provided showing all scored actions. Drilling further into a session places all user behaviors and associated characteristics on a log-on to log-off timeline.

For the traditional SIEM user, building a session of activity and characteristics is only done once an alert is generated by some piece of the security architecture or by the SIEM itself as part of a correlation. Once the alert is generated, the first tier-one action usually performed is to determine if the alert is a false positive. If it is determined to be legitimate, the tier-one member of the security team will involve someone on tier two or tier three for further analysis. The tier-two security analyst will start the process of asking questions related to an alert and begin to assemble a timeline of activities pivoting through a variety of data sources. If the attacker has switched identities, manual investigations become extremely difficult. Additional log data (and a lot

of time and patience) is required to link the next set of activities together, if it's possible at all.

Exabeam accelerates the investigation process in two ways. First, many of the questions asked by the tier-two or tier-three security analyst are already asked and answered by the system. Second, the session of activities, which includes facts from security network and host based solutions, is already assembled, eliminating the tedious point-click-and-pivot tasks.

When a member of the tier-one security operations center team sees a high-risk session, their first response becomes picking up the phone, dialing the number provided in the context data section of the user interface and asking the same questions a credit card fraud analyst might ask when seeing anomalous behavior: "Hi Bill, did you just initiate a VPN session from Uruguay accessing these five servers, then assume the service account identity and access the database?" Finally, additive risk scoring elevates risky behaviors above the noise generated by users that are going through normal organizational changes, such as job role and department changes, replacement of user systems or changes in user location.

COMPLIANCE AND USER AND ENTITY BEHAVIOR INTELLIGENCE

Compliance is no longer a snapshot in time. The concept of continuous monitoring has been written into NERC-CIP, HIPAA, NIST 800-137, PCI and the globally accepted SANS Top 20 Security Audit Guidelines. Each set of compliance guidelines contains a section of requirements for access management and monitoring. The continuous diagnostics and mitigation (CDM) initiative currently underway in the civilian sector of the federal government specifically calls out security behavior monitoring as one of its required core capabilities for managing accounts for people and services. Below is a list of each of the areas of compliance listed above and where user behavior intelligence fits into each one.

- PCI
  - Requirements 8 and 10
- HIPAA
  - Technical Safeguards 164.312(a)(1)
- NERC-CIP Version 5
  - CIP-0007-5 R4
  - CIP-0007-5 R5
- SANS Top 20 Security Audit Guidelines
  - Control 12 – Controlled Use of Administrative Privileges: CSC 12-1
  - Control 14 Maintenance Monitoring and Analysis of Audit Logs: CSC 14-5, CSC 14-8
  - Control 16 – Account Monitoring and Control: CSC 16-5
- NIST 800-53
  - AC-2 Account Management
  - IA-2 Identification and Authentication
  - AU-2 Auditable Events
  - AU-12 Audit Generation
  - AU-14 Session Audit

SUMMARY

In spite of large increases in company security budgets and the hiring of additional personnel, an increasing number of exponentially larger data breaches continue to occur. For the attacker, valid credentials are the most coveted item. Valid credential use by an attacker facilitates many actions in the attack chain. In spite of efforts by businesses and government agencies to train employees to be wary of social engineering schemes, human beings are fallible and will always be susceptible to attackers that will con and coerce employees into giving them their credentials. Valid credentials are the key to an attacker's ability to stay resident inside the network for long periods of time and cause the most damage.

User behavior intelligence and security session assembly can help enterprises find and root out attackers that impersonate

employees. Adding the right solution can mean being able to give more complex tasks to more junior security analysts while speeding up the data analysis process. Analyzing SIEM and log management data repositories with Exabeam is like adding a security savant to your team that can work 24/7, remember all credentialed activities over the last ninety days for 150,000 employees, compare current activities to those in the past detecting anomalous behaviors, perform security session assembly and surface those users whose behaviors exceed risk thresholds.

For more information, please visit http://www.exabeam.com, or send email to info@exabeam.com