KuppingerCole Report

EXECUTIVE VIEW

by Mike Small | September2017

VeriClouds CredVerify™

Securely authenticating users remains a thorny problem and VeriClouds CredVerify service can provide a useful additional level of assurance. There are many approaches, products and services for user authentication however, the CredVerify service is unique in what it offers.

by **Mike Small**
mike.small@kuppingercole.com
September 2017

Content

Related Research Documents

Leadership Compass: Privilege Management - 72330

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E) - 70319

Leadership Compass: Cloud Access Security Brokers - 72534

1 Introduction

The threats to organizations from data theft, ransomware and other forms of cyber-crime continue to increase. In May this year, the UK NHS hospitals and doctors were hit by a ransomware attack[1] that paralysed many services and led to patients having treatments cancelled. In the same month, an anonymous hacker obtained approximately 1.9 million active email addresses and approximately 1,700 customer names and active phone numbers from the Canadian Telecommunications company Bell Canada[2]. Organizations need to be vigilant and take appropriate precautions to reduce the risk of cyber-attacks being successful. One critical area that needs to be addressed is the security of account credentials and of passwords in particular.

Most organizations have already implemented many layers of defences against cyber-attacks. These will include network firewalls, intrusion prevention systems, access controls as well as encrypting sensitive data. Very few attacks can directly overcome these defences; therefore, cyber criminals look for ways to bypass them. They use a multi-stage approach known as the cyber-kill chain and the first objective of this is to obtain access to one end-user device or system within the organization. By obtaining apparently legitimate access to this the attacker has bypassed all of the primary security controls described above.

Once the attacker has obtained the credentials for a legitimate user account these give access to all the systems available to that user. One common way to obtain these credentials is through a "phishing" attack where the targeted user receives an email containing a URL or attachment which if clicked or opened will install malware. Organizations can use multiple layers to defend against this; spam detection services, using up to date and patched software as well as keeping anti-malware software up to date. However, the user may still provide the cyber-criminal with an easier approach – reused passwords.

Passwords are widely used as a "something you know" check on the authenticity of users. However, while password authentication is relatively easy to implement, users find complex passwords hard to remember. In addition, given the large number of personal systems the average person is now likely to access, which include banking, e-commerce, social networks as well as email and messaging systems, there is a temptation to reuse the same password across many of these systems as well as for the organizational systems to which they have access. Unfortunately, over time many of the external systems used by people have suffered serious breaches[3] [4] where the user credentials have been leaked.

Databases of leaked credentials are widely available on the "dark web" and are used by cyber criminals to target organizational users. If the user has had one of their accounts compromised and is using the compromised password on other personal accounts – the attacker can plant malware on one or more of the other sites used by the user (in one of the user's files for example). Alternatively, where they can

[1] **NHS cyber-attack: GPs and hospitals hit by ransomware - BBC News**
[2] **Bell Canada says customer information compromised in hack - National | Globalnews.ca**
[3] **'One billion' affected by Yahoo hack - BBC News**
[4] **Giant spambot scooped up 711 million email addresses - BBC News**

link the compromised personal accounts to organizational accounts they can simply attempt to log on to the organizational system using the harvested password.

Many organizations implement a forced password change policy where users must change their password regularly and cannot reuse previously used passwords. Most organization force new passwords to comply with a policy regarding their formulation to avoid ones that are easy to guess. However, few implement the recommendations in NIST SP800-63B[5] that require new passwords to be screened to prevent the use of those "obtained from previous breach corpuses".

Breached credentials are a major problem and until organizations implement other forms of authentication passwords are a major risk. This is especially the case where passwords are used to authenticate privileged access – for example for systems administration. Even where passwords are used for access to lower value systems and data, they can still be used by cyber attackers to gain a foothold. Organizations must take steps to protect against the reuse of breached credentials and should fully implement at least the recommendations in the NIST SP800-63B.

2 Product Description

VeriClouds is a credential verification services company that is based in Seattle WA, in the USA. It was founded in 2014 by Rui Wang, a former security researcher at Microsoft with a PhD in cyber security, and the entrepreneur Stan Bounev. VeriClouds provides credential verification services to help organizations detect compromised credentials. This report covers VeriClouds CredVerify™ credential verification service.

2.1 VeriClouds CredVerify™ Overview

VeriClouds has built a data repository of leaked account credentials which is used identify and remediate potential threats across a broad range of end-points and infrastructure. The CredVerify platform includes agents that enable protection schemes for popular services such as Microsoft Exchange/AD, Lieberman RED Identity Management, SailPoint IIQ, Splunk and ReST API for custom integration. This platform is illustrated in figure 1.

This platform is offered as a cloud service, a managed hosted service and an on-

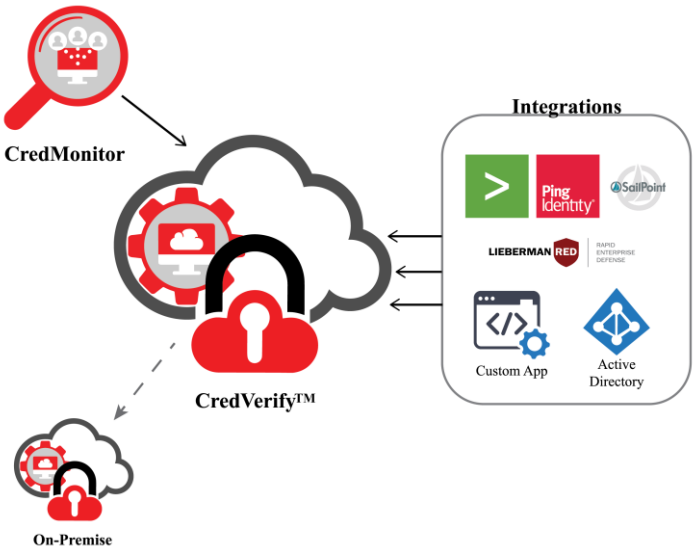

Figure 1: VeriClouds CredVerify Overview (graphic reproduced with permission from VeriClouds)

[5] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

premises appliance. It is also available integrated with partners' products.

2.2 Compromised Accounts Repository

VeriClouds has a large repository of compromised accounts that is built on top of a SaaS platform. It is built and maintained using a proprietary semi-automatic crawling engine to continuously collect breached databases from the dark web. It uses anonymous identities and accounts, and employs dedicated machines to anonymously access dark web sites. In addition, scripts automatically download data files from services where hackers frequently paste leaked accounts. VeriClouds data analysts also monitor various dark web forums and marketplaces to obtain newly breached databases when they are available.

This data is held in an encrypted form using the FIPS 140-2 certified crypto algorithms and Hardware Security Modules (HSM) to protect the encryption keys. The SaaS service is hosted on AWS and the HSM used is administered by a 3rd party.

The product is designed using a privacy by design philosophy that neither VeriClouds, nor its clients have visibility over data that does not belong to them.

2.3 APIs and Queries

VeriClouds CredVerify provides APIs and plug-ins that enable passwords to be checked against the compromised accounts repository during the user login process. The repository can provide intelligent data graphs giving visibility into the risk of an organization's compromised credentials on 3rd party websites and the social web. These include the following functionality:

- Microsoft Active Directory and Kerberos extensions to compare hashed passwords against VeriClouds Service;
- Passwords are matched using patent protected password matching technology.
- ReST API that can be used from the cusomter's cloud and or premises to identify password policy violations such as weak credentials, password reuse and prevent malicious phishing attacks.

2.4 Integration with IDaaS and CASBs

These APIs provide functionality that can be integrated with Identity as a Service (IDaaS) providers and Cloud Access Security Brokers (CASBs). This could enhance the service that they provide through proactively monitoring for the use of compromised credentials when

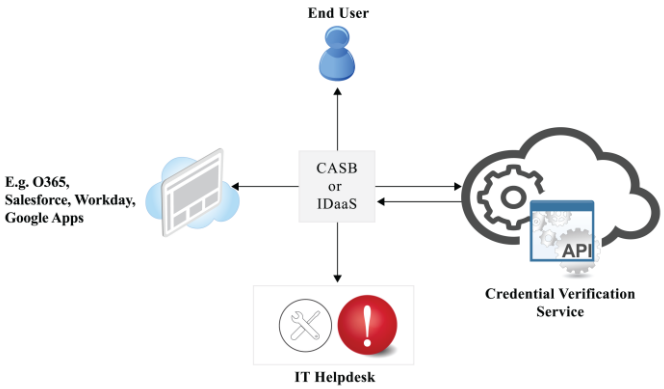

Figure 2: Integration with IDaaS and CASB (graphic reproduced with permission from VeriClouds)

the user logs on and when the user changes their password. This is illustrated in Figure 2.

2.5 Support for NIST SP 800-63B

VeriClouds CredVerify introduces credential verification into the authentication workflow, using the database of compromised credentials and patent protected password comparison methods to detect and prevent password reuse. VeriClouds CredVerify helps enforce the NIST password requirement guidelines for Identity Providers by screening of new passwords against lists of commonly used or compromised passwords. CredVerify™ NIST password compliance check capability supports and verifies all the following that are specified in the NIST document:

- Passwords obtained from previous breach corpuses;
- Dictionary words;
- Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd');
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

2.6 Security and Privacy

The VeriClouds CredVerify service and appliance are designed and implemented to provide a high degree of assurance that the information they hold about their customers is secure and private. The VeriClouds CredVerify service or appliance does not hold copies of the customer organization's actual credentials. It simply provides an API that allows a user's current credentials to be compared with the database of compromised credentials when they log on. These current credentials can be encrypted before being sent to the service for comparison. The API supports:

- Password as plaintext and as HASH;
- For hashed password, the appliance supports most commonly used password-hashing algorithms, including MD5, SHA1, SHA256, and BCRYPT both with or without salt.

The database of compromised credentials held in the service are encrypted using AES -256:

- A unique IV (Initialization Vector) is used for each encrypted username;
- A random IV is used for each encrypted password;
- Cryprographic keys are held in an HSM

2.7 Integrations and Partnerships

VeriClouds CredVerify is fully integrated into the Lieberman RED Rapid Enterprise Defense™ Suite Identity Management module. VeriClouds transforms the visibility of compromised credentials discovered on the deep and dark web into actionable intelligence through this integration.

In addition, it is also integrated with the IDaaS offerings from SailPoint and Ping Identity.

3 Strengths and Challenges

Securely authenticating users remains a thorny problem and VeriClouds CredVerify service can provide a useful additional level of assurance. There are many approaches, products and services for user authentication however, the CredVerify service is unique in what it offers. It does not replace existing approaches, rather it provides information on certain potential risks when a user logs on or changes their password. It also provides additional security intelligence that can be used to assess and remediate risks relating to organizational users' password credentials.

In general terms, the use of passwords alone to verify identity of an entity using an IT service, provides only the lowest level of assurance in that identity. This is recognized in the previously mentioned NIST SP 800-63B where "memorized secrets" (i.e. passwords) provide only "some assurance that the claimant controls an authenticator bound to the subscriber's account". Furthermore, other forms of additional assurance such as one-time passcodes sent by SMS (or other routes) to verify a password based logon can also be compromised. So, wherever passwords are used there is a risk, and this risk is further exacerbated by the large number of compromised credentials that are available to cyber criminals. VeriClouds CredVerify service helps organizations to manage this risk.

Although VeriClouds CredVerify is available as a SaaS service some work is still needed to fully implement it within an organization. Furthermore, some organizations may be hesitant to allow sharing information on their organizational credentials with a cloud service in spite of the assurances from VeriClouds. To cater for this VeriClouds offer an on-premises appliance.

One challenge for VeriClouds is how to most effectively market this service to get the widest possible take up so as to ensure a return on the significant investment in collecting and maintaining the data. One way to achieve this would be through partnerships with identity providers and the providers of other services that use passwords for authentication. This would allow those service providers to offer an enhanced level of assurance to their customers. The current integrations with IDaaS from SailPoint and Ping Identity IDaaS as well as with Lieberman RED are examples of this. To succeed VeriClouds needs to get a much wider take up by IDaaS providers, CASB solutions and other security intelligence tools.

Strengths	Challenges
• Provides insight into compromised organizational credentials that are available to cyber-criminals. • Provides support for the requirements for password checking defined in NIST SP 800-36B. • Available as a cloud service and an on premises appliance. • Integrated with a small number of IDaaS services and security tools.	• Getting integration with a wider range of Identity providers. • Adoption and integration with CASB tools. • Managing concerns over how organizational credentials are shared and where data is stored.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com