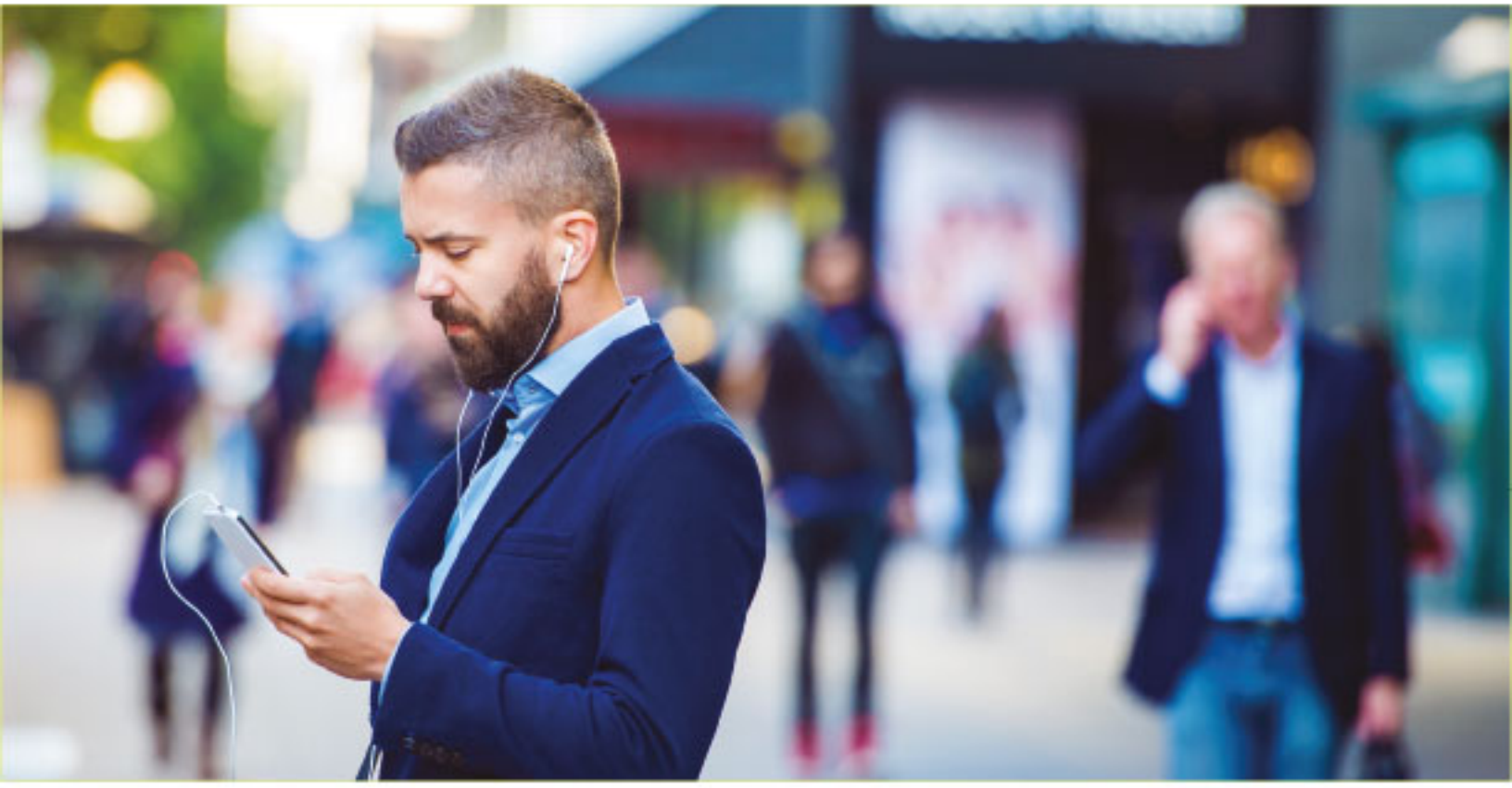
Ping Identity.

ProofID
Managing Identity

SECURING YOUR ENTERPRISE CREDENTIALS

Lessons From The 2016 Verizon Data Breach Investigations Report



WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

In its much-anticipated 2016 Data Breach Investigations Report (DBIR), Verizon once again researches and reports on the past year's information security incidents and data breaches. The complete dataset includes more than 100,000 incidents and 3,141 confirmed breaches—and that's just the ones that Verizon knows about. And while the numbers vary, all industries are vulnerable to attack.

Not to be a spoiler, but it turns out there isn't much new in the form of attack. The bad guys generally rely on tried-and-true methods. You might say this is good news, because it's easier to identify known threats. But Verizon did find it relevant to include a dedicated section on credentials in this year's report. Why? Because the DBIR reveals that 63% of confirmed data breaches involved weak, default or stolen passwords.

63% OF CONFIRMED DATA BREACHES INVOLVED WEAK, DEFAULT OR STOLEN PASSWORDS.[1]

This is one of those scary statistics that's impeding digital transformation. But it doesn't have to. Despite all of the doom and gloom, the intent of the report is not to overwhelm, but to educate and prepare. As Verizon aptly says, "forewarned is forearmed."

In this paper, you'll learn the most common vectors of attack based on Verizon's research. These methods—all oldies but goodies with a shared MO of stealing credentials—demonstrate the risks inherent in single-factor authentication. You'll discover how stronger authentication methods can mitigate these risks and provide better security for your enterprise credentials. Finally, you'll learn how to implement an MFA solution that gives you the strongest security posture, so you can confidently manage digital transformation across your enterprise.

1 Verizon 2016 Data Breach Investigations Report

THE VECTORS OF ATTACK

You're rightfully concerned about security, and your customers are, too. But applying the brakes to digital transformation isn't an option. The key is to identify and address the risks, and in doing so, gain the confidence to move forward and even accelerate your digital transformation.

Among the key risks are phishing, web app attacks and point-of-sale intrusions. These aren't new to the threat landscape, but they're also not losing popularity. In fact, the incidence of phishing is on an upward trend, according to Verizon.

PHISHING

Capitalizing on our human need to click things, phishing campaigns try to get the recipient to open an infected attachment or click an equally infectious link. A phishing email might direct the victim to a site to input credentials, by far the most common type of data stolen as illustrated in Figure 1. But more commonly, phishing scams are used to install persistent malware. Regardless of the means, the end goal is the same: to maliciously collect credentials and personal data.

According to Verizon's findings, 30% of phishing messages were opened, up from the previous year. So while phishing isn't exciting or new, it remains extremely effective. In fact, it accounts for 9,576 of the total incidents in this year's DBIR, and almost 10% of those had confirmed data disclosure.

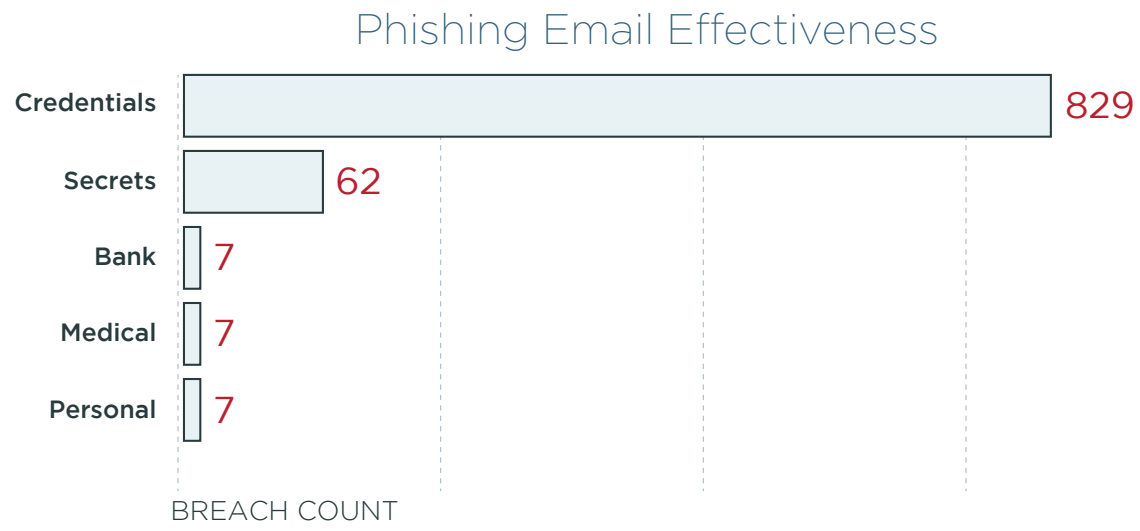


Figure 1: The number one objective of phishing campaigns is stealing credentials.
Source: Verizon 2016 Data Breach Investigations Report

WEB APP ATTACKS

As websites evolve from primarily providing information to driving business-critical initiatives, they're increasingly at risk. Site visitors are interacting more often and in more complex ways with your website, making it a vector to sensitive data and an obvious target for attackers.

Websites are compromised in all kinds of ways, but almost 20,000 (or half) of this year's web app attack incidents involved using websites to host malware or act as phishing sites. The pervasive Dridex campaign is largely to blame. Deeper analysis into those breaches showed a clear pattern: a phished customer opens the malicious attachment, is directed to the command and control server (C2), it drops the keylogger, exports captured data and uses the stolen credentials.

Aside from financial malware that's everywhere, the top six threat actions associated with web app attacks look similar to last year, with phishing rising up the ranks. When Verizon removed the Dridex data, it also revealed that acquiring web-based email credentials with social engineering is another element of this year's web app attacks.

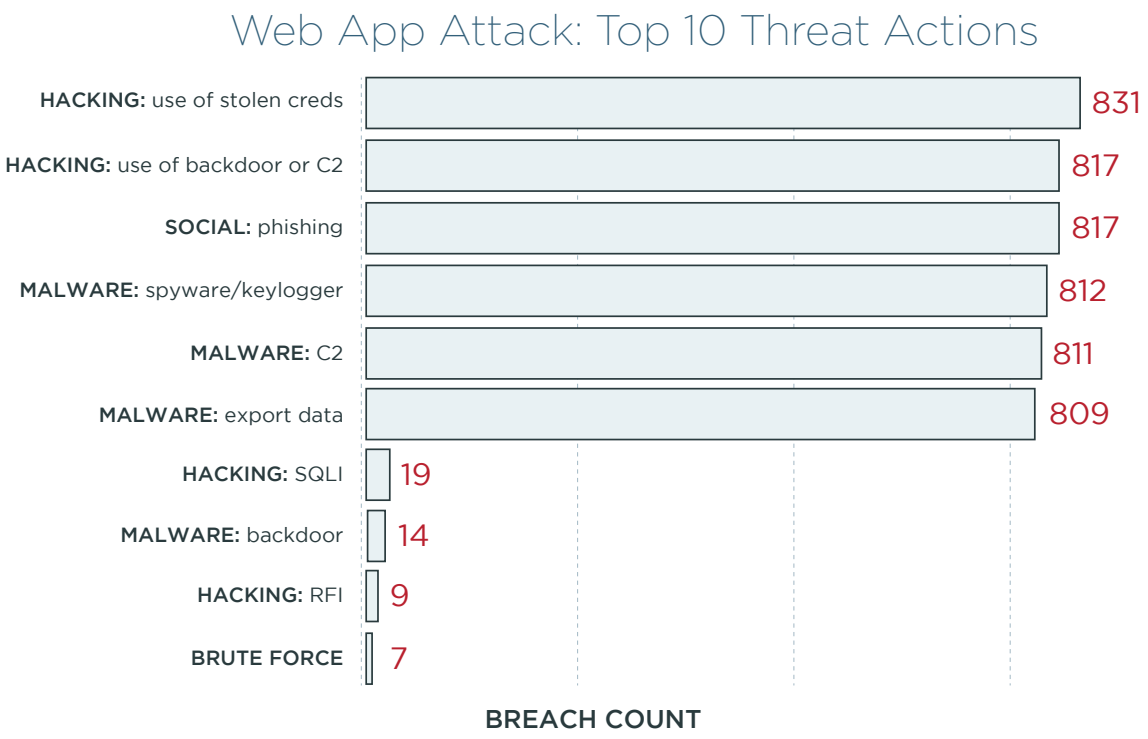


Figure 2: The top 10 threat action varieties within web app attacks.
Source: Verizon 2016 Data Breach Investigations Report

POINT-OF-SALE (POS) INTRUSIONS

Considering that financial motivations dominate the reasons behind security breaches, it's little surprise that POS intrusions remain a vector of attack. And the use of stolen credentials to access POS environments is significant.

These attacks typically involve a single device (often a lone computer) which is used to process payments and communicate to the payment processor, while also being used to check personal email, post to social media and other personal user activities. This combination introduces risk to the POS application which isn't protected by an anti-virus or host-based firewall.

This is most common among small businesses, but the 2016 DBIR uncovered a similar pattern for larger organizations. While the attack factors are different, the weak point (relying on passwords) is the same. Figure 3 illustrates the prevalence of stolen passwords in POS intrusions. While brute force attacks will still occur, these numbers can be lowered by moving away from simple passwords.

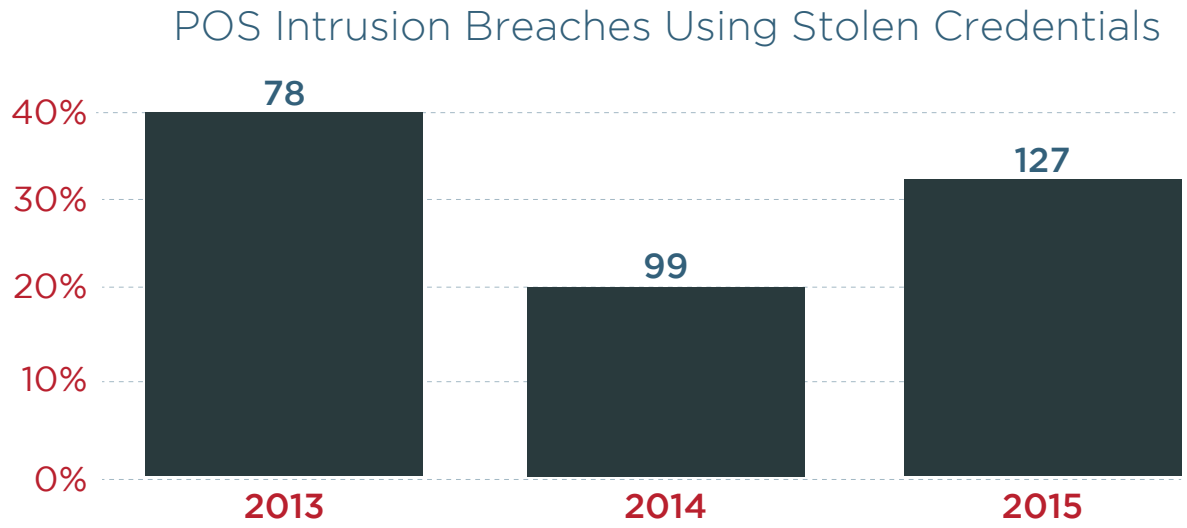


Figure 3: Three-year chart of percentage and number of breaches using stolen credentials within POS intrusions. Source: Verizon 2016 Data Breach Investigations Report

MITIGATING RISK THROUGH TWO-FACTOR AUTHENTICATION

Whether an attack is made through phishing, web apps or POS, the common thread is the vulnerability inherent in single-factor authentication. Verizon says it best, and it bears repeating (because it's obviously true, but also so darn clever): "Passwords are great, kind of like salt. Wonderful as an addition, but you wouldn't consume it on its own."

Said another way, passwords alone are woefully inadequate. So what are your other options?

PASSWORDS ARE GREAT, KIND OF LIKE SALT. WONDERFUL AS AN ADDITION, BUT YOU WOULDN'T CONSUME IT ON ITS OWN.[2]

Two-factor authentication (2FA) is one place to start. As the name implies, 2FA requires users to provide two proofs of their claimed identity before being granted access to resources. The premise is that if one mechanism is compromised, the other is unlikely to be, so there's still some level of confidence in the user's identity.

HOW 2FA WORKS

With 2FA, you gain a second level of authentication to an account login. Instead of entering only a username and password, for example, you must authenticate using an additional credential.

Traditional authentication is based on three types of credentials:

1. Something you **know**, such as a PIN, password or pattern
2. Something you **have**, such as an ATM card, phone or fob
3. Something you **are**, such as a fingerprint or voice print

Single-factor authentication relies on only one credential, typically the first. Two-factor authentication requires that you authenticate using an additional credential, typically the second or third.

Paying for gas at the pump is a good example of 2FA in action. You swipe your credit card (something you have) through the pump's card reader, then you must also enter your zip code (something you know) to complete the transaction.

2 Verizon 2016 Data Breach Investigations Report

HOW 2FA FALLS SHORT

Traditional 2FA adds an additional layer of security and could be a good starting point for many organizations to move beyond passwords alone. But it isn't without its challenges and limitations. The common shortfalls of 2FA are:

- **POOR USER EXPERIENCE:** Adding clunky hardware tokens with additional passcodes and sign-on steps is painful for users, resulting in notoriously low adoption rates. Another device to carry often translates to another device to forget. Time-sensitive, one-time passcodes make quick tasks like checking email an undesirable challenge for many users resulting in lost productivity.
- **COST:** Traditional hardware and software tokens (a "something you have" credential) are expensive to purchase, maintain and administer. The initial deployment of hardware tokens includes costs such as management software licenses, end user software licenses, professional services for implementation and shipping costs. Ongoing maintenance costs include hardware and software support, professional services for patches and upgrades, lost and damaged tokens, and help desk costs. Additional costs for highly available server infrastructure, the additional load on backup infrastructure and all of the associated management costs can add up quickly.
- **COMPLEXITY:** In addition to being costly, setting up a dedicated infrastructure for 2FA can be complex and time consuming. Professional services are often involved in the implementation and ongoing maintenance of these solutions with little expertise transferred in house. This can mean when a problem arises, it may not be solved until third-party resources become available, decreasing productivity across the workforce.
- **SECURITY:** 2FA is not impervious to attacks, and it's increasingly being called into question. You can find numerous articles from a year or two ago about how to bypass 2FA through Google's account recovery process. More recently, the National Institute of Standards and Technology (NIST) is recommending that SMS no longer be used as a method of 2FA authentication, particularly with services that virtualize phone numbers because of the risk of exposure and tampering. [3]

At the end of the day, traditional 2FA is better than a single factor, but that bar is pretty low. There are even stronger and more user friendly authentication options to protect your enterprise from common attacks.

3 Devin Coldewey, "NIST declares the age of SMS-based 2-factor authentication over," TechCrunch.com, July 25, 2016, accessed at https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/

MOVING BEYOND 2FA TO MODERN MFA

While 2FA is a form of multi-factor authentication (MFA), there is a more advanced MFA solution that provides a better defense and a better user experience: contextual MFA. It uses a risk-based approach that extends beyond the traditional "something you know, have or are" protocol to include the following characteristics:

- Utilize any number of authentication factors commensurate to the level of risk.
- Use contextual data (e.g., location, network, device, resource requested) to determine level of risk.
- Set policy that steps authentication requirements up or down based on context.
- Provide authenticating users options including mobile device, email, SMS, YubiKey, desktop application, etc.

By providing both an active and passive assessment of the user, such as the computing environment and the nature of the transaction being attempted, contextual MFA works in the background to determine the right level of security. It collects data about the user to establish a typical behavioral profile. If the user's behavior falls outside of this, it can step up authentication requirements to apply the correct level of security based on the associated risk.

The benefit and beauty of using contextual MFA is its ability to strengthen security only as warranted and without burdening the user for more information or extra steps to gain access. Easy to use, contextual MFA offers many advantages over other authentication methods:

- Delivers an optimal user experience by demanding the minimum acceptable level of authentication for a given operation.
- Is more cost-effective by only utilizing more expensive authentication when warranted by the risk.
- Improves fraud detection relative to traditional binary rule sets.
- Creates a flexible and future-proof architecture that can adapt to emerging technologies and data assets.

HOW CONTEXTUAL MFA WORKS

Contextual authentication passively collects data points about users and their context. These data points, or authentication signals, might include their location (both physical and network), their computing environment and the resources they're trying to access. Signals can be collected by:

- The web pages where they authenticate.
- The mobile devices used for MFA.
- Other network hardware.
- The application (or gateways in front).
- Other sensors in proximity to the user (e.g., wearables, smart watches, etc.).

Once collected and aggregated, the risk and policy infrastructure can analyze these signals to look for anomalous patterns that might indicate an attack or fraudulent behavior. This analysis can be:

- **CONTEXTUAL:** comparing a given signal value to a prescribed list of allowed or disallowed values (e.g., not allowing sign-on for any IP address coming from Uzbekistan).
- **BEHAVIORAL:** comparing a given signal value to the expected value based on a previously established pattern (e.g., an employee often travels to Uzbekistan on legitimate business, and therefore is allowed to sign on with MFA, whereas any other employee is prohibited from signing on from Uzbekistan).
- **CORRELATIVE:** comparing a given signal value to a different collected signal value and looking for inconsistencies between the two (e.g., according to the laptop IP, an employee is in the United States, but according to their mobile phone, this employee is in Uzbekistan).

SAMPLE USE CASES

Contextual MFA in action can take on many forms, stepping authentication up or down as determined by the risk of the actions being performed. The following are common use cases that demonstrate the range of flexibility of contextual MFA.

ZERO PASSWORDS

If the threat level is very low, a user can be given access to an application without explicit request for a password or any authentication information. Let's say a user makes a request for a low-sensitivity application from a known and trusted device on a trusted network, and is within a secure geo-fence. There's very little risk, so they're signed on without a password.

STEP-UP AUTHENTICATION

If a user has already been authenticated, but now wants to perform a riskier transaction, the application can request additional factors before granting access. For example, a user accesses an application with a simple sign-on (username and password). Then, the user attempts to make a purchase. The application steps up authentication, requiring additional factors—such as a swipe or fingerprint on a mobile device—to raise the level of authentication to match the increased level of risk.

STAY SIGNED ON

For some applications, it might make sense to allow a user to stay signed on for an extended time period. In this case, contextual MFA can monitor the user's behavior and utilize that data to determine if the session can continue or if it should be terminated. For example, if the user signs on from two different devices with IP addresses coming from two different continents a couple minutes apart, the application can be terminated or require additional authentication to maintain or regain access.

IMPLEMENTING CONTEXTUAL MFA

Some may argue that MFA is difficult to implement, but it doesn't have to be. In fact, it can be surprisingly simple and cost effective. Here are a few of the implementation characteristics of modern MFA solutions:

- Offered as a cloud service with no need for software installation.
- Self-service registration for mobile device.
- User selection of authentication methods based on admin configuration.
- Enable MFA for select users based on app, group, device, location, or IP address.
- Online mode for improved security and convenience—sends push notifications, not SMS.
- Offline mode with one-time passcodes when needed and allowed by policy.
- Integrated with SSO authentication flow.

Still skeptical? Verizon asserts that implementing MFA is worth the effort. As they put it, "implementation of stronger authentication mechanisms is a bar raise, not a cure-all." But, given that 63% of confirmed data breaches involved weak, default or stolen passwords, Verizon recommends that it's a bar worth raising.

CONCLUSION

The statistics don't lie. Stealing credentials is the primary motive for those intent on attacking your enterprise. And you're only making it easier for them by continuing to rely on usernames and passwords.

Static authentication is convenient, but it offers little defense. You'd be better protected with 2FA, but its negatives—like poor user adoption—are well documented, and its effectiveness is in question.

A risk-based approach using contextual MFA provides a strong security posture for your enterprise—without compromising user experience. By utilizing only the level of authentication warranted by the risk, contextual MFA is a more efficient and cost-effective solution that's flexible to accommodate an ever-evolving landscape. And it's easier to implement than you may have thought.

To learn more, visit pingidentity.com.

#3139 | 3.17 | v008