## For Immediate Release

For More PR Information, Contact: Carlo Chatman, Power PR Phone (310)-787-1940 Fax (310)-787-1970 E-mail: <u>press@powerpr.com</u>

# Vulnerability of Login Credentials at Heart of Cyber Hacks and Data Breaches

Corporate entities and retailers are scrambling to shore up network security by addressing the primary vulnerability of network security: the login. Unique "behavioral" biometric may be the solution

Welcome to the "Age of the Cyber Attack."

Staggering numbers from security experts suggest that over 95% percent of all corporations have experienced a data breach of some kind – many of which can go undetected for months or years.

In the wake of the Sony hack and other high profile data breaches at Target, Home Depot, Michaels, Chase and other institutions, corporate IT departments are scrambling to discover and implement solutions that will immediately shore up network security.

At the heart of this search: finding solutions that address the primary vulnerability of network systems, the user login.

It turns out that accessing a network through obtaining the login of a credentialed user is at the heart of the majority of high profile internet data breaches of the past year. The CBS News program 60 Minutes called 2014 "the year of the data breach," and went on to state that forensic evidence showed that 80% of security breaches were caused by stolen or weak passwords.

Once inside the system, cyber hackers are able to install information-stealing malicious software that can reside undetected on corporate servers for months – even years – capturing credit card and other information while slowly expanding its reach.

So, why is the login such a pesky problem for IT departments to crack? And why do usernames with pins/passwords fall so short in preventing unauthorized access?

At the root of this dilemma is how to effectively authenticate that the individual accessing the network is who they say they are with an extremely high degree of accuracy.

To be effectively implemented the solution must also meet two additional criteria: it must be easy to use and ideally would require no additional hardware beyond a normal computer, tablet, or Smartphone device.

In the field of user authentication, meeting all three of these requirements is considered the "Holy Grail" of online identification.

Fortunately, a solution that checks off all these boxes may already exist.

Based on a unique subset of biometric verification, this tool can prove with almost 100% accuracy that the person attempting to login is who they say they are, while being nearly impossible to artificially replicate.

## The Trouble with Logins

The difficulty with login credentials is that they are based on possessing specific pieces of information, most commonly a username and pin/password. Armed with that information, users can access everything from medical records and bank accounts, to credit card information, e-mails and other sensitive information.

The problem, of course, is that anyone armed with the same login credentials can also access the same information.

As was widely reported, the hackers apparently gained access to Sony's computer systems by obtaining the login credentials of a high-level systems administrator. Once the credentials were in the hands of the hackers, they were granted "keys to the entire building," according to a U.S. official.

In this particular case, Terabytes of information obtained (and worse, deleted completely from company servers) is being used to wreak havoc on Sony's movie business interests.

In the case of the Target breach in late 2013 that exposed approximately 40 million debit and credit card accounts, login credentials were also the culprit. In this case it was believed that login information stolen from a third party HVAC vendor was the source of the initial intrusion.

For Target, the losses are estimated at nearly half a billion dollars This includes reimbursement associated with banks recovering the costs of reissuing millions of cards and customer service costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach.

#### **Searching for the Ideal Solution**

To combat this problem, IT personnel have turned to a variety of techniques to improve the security of logins including adding security questions and in some cases a secondary password.

However, these options are simply an extension of the same concept: possessing specific information that others can still acquire.

Another attempt currently in use involves throwing hardware at the problem.

The logic is straightforward: provide each user with a physical device such as a flash drive or a token that provides random authentication codes, credit cards, or personal ID in various forms, including a Smartphone. If someone has the item, they are legit.

Unfortunately, this is just another form of "possessing" something – in this case a piece of hardware instead of a piece of information.

Furthermore, the reason added hardware solutions are non-starters is that it dramatically increases the cost of implementation, not to mention the logistics of upkeep, and because these items can be lost or stolen still does not guarantee authentication of the user.

The answer, then, boils down to the only way to truly identify a person: biometrics.

Biometrics is defined as something physically or behaviorally unique to an individual. Physical examples include fingerprints, iris scans, facial recognition, and even vein scanning.

While these deliver near-absolute verification, this type of identification again requires sophisticated, costly hardware. This is a significant barrier to implementation for reasons already stated above.

Fortunately, there is a surprisingly effective form of biometric verification in the behavioral category based on handwriting that requires no additional hardware beyond a typical computer arrangement or Smartphone device.

It turns out that each person has a unique, measurable way of "drawing" (remember etcha-sketch?) letters and numbers that is extremely difficult to duplicate by others. This includes attributes such as length, height, width, speed, direction, angle and number of strokes.

Passcodes can be entered at login using a finger or stylus for touch screens and Smartphones, or using a computer mouse or laptop touchpad.

Once a simple set-up process is completed, sophisticated software algorithms compare a user's current login attempt against the initial patterns collected and subsequent logins to confirm a match. Using this technique, accuracy rates as high as 99.97% are possible.

One of the companies at the forefront of this technology is Biometric Signature ID, a company that provides a "software only" biometric system in which the signature reader resides in ultra secure cloud based servers. All information is assessed and stored in a database using high encryption technology.

This "software only" system called BioSig-ID<sup>™</sup> utilizes audit trails based on the stored information to uncover suspicious activity by pinpointing the time, location, (including IP addresses) and history unauthorized users can be determined.

"Through continuous and real time forensic checks via neural net technology we can uncover fraudulent activity," says Jeff Maynard, CEO of BioSig-ID. "For instance, is the same IP address used for log-in all the time or does it come in every once in a while from offshore? We use real time alerts for certain targeted events and combine this with comprehensive historical reporting. These alerts are sent in real time to the clients and appropriate further analysis is also conducted."

5

The BioSig-ID system is already installed and currently being utilized by early adopters in diverse industries such as healthcare, education, banking, financial, and even government institutions.

The company is so confident that "signature" biometrics is the solution, in fact, that it has set up a challenge for those that visit the web site <u>www.biosig-id.com</u>. The company is offering \$500 to the first person that can reproduce a simple passcode of the word "Mom."

The company goes so far as to actually show a copy of the passcode (which is usually not available to users or hackers in real life applications therefore giving an added advantage for this trial). Those that attempt the challenge are given unlimited chances to copy the signature and gain entry to the network.

Taking it a step further, the company trained over a hundred users to be experts in the system and asked them to spoof 20 different passcodes previously created by other users. After nearly 20,000 attempts even the simplest of passcodes like 'Mom' could not be duplicated. These results were reported in independent testing.

On their website, after many thousands of attempts, no one has yet claimed the \$500 prize.

According to Maynard, a major corporate concern about implementing any additional layer of security is over potential consumer inconvenience.

"Many retailers and e-tailers have not implemented higher security measures because they don't want their customers to spend additional time going through extra security. Extra time, they believe, may mean loss of clients and sales," says Maynard. This is why the ease of user interface is a critical component of online authentication. If the added security has too many steps or is too cumbersome it is doomed to fail.

Maynard says this is the reason his company puts so much emphasis on keeping the user interface simple and takes only seconds to activate. Mobile apps, PC and mobile device login, and access to cloud based apps are all solutions the company offers. To set up a new user on any device, the individual simply logs on to the website, draws and creates a unique four alphanumeric character or symbol passcode. Upon subsequent logins, the biometric patterns of the created passcode are analyzed. Only the registered user is confirmed and is able to freely access their account. Imposters have no idea "how" the passcode was created, so are stopped at the login step.

To be sure, there are costs involved in implementing additional security solutions – even those that require no additional hardware. However, corporations are well aware that the collateral damage of a major data breach is much, much higher in both cost and potential loss of consumer confidence.

The problem then, is not whether or not they will invest in additional security, but in simply identifying solutions that meet all the requirements.

In this new "Age of Cyber Attacks" that needs to start with securing the login.

## To conduct a "test drive" of the BioSig-ID technology, visit www.BioSig-ID.com

For more information, contact Biometric Signature ID at 708 Valley Ridge Cr., Suite 8; Lewisville, TX 75057; (877)700-1611 ext 1.

###