OUT IN FRONT PLAYBOOK

JUNE 2021

EMBERIT.COM

THE FOLLOWING CONTENT MAY BE CONCERNING

BUT THAT'S WHY WE'RE HERE

As IT professionals, every day is an all out war to keep our clients out in front of an ever more perilous cyberthreat landscape.

This reality is what gets us out of bed in the morning and what keeps us up at night. It's what transformed EMBER from an IT services company that cares about security, to a security company that also does IT. If the feat of securing your organization feels somewhere between daunting and paralyzing, there's a good chance we can help.

Out in Front focuses on human factors in the cyberwar and shares untold stories, close-up accounts, and lessons learned from the front lines.

We hope you enjoy the read!

Matt Toto,
Co-Founder & CEO
mtoto@emberit.com

THE INSIDER THREAT

Just a few short years ago, cybersecurity was all about external threats — keeping the bad guys outside of an organization from getting in. While external threats are still a problem, more than a third of all threats are now emanating from within.

This insider threat potential is usually at the hands of current or former employees, business partners, consultants or even board members who have inside information concerning the organization's security practices, data and IT systems. They use that information in a way that could negatively affect that organization.

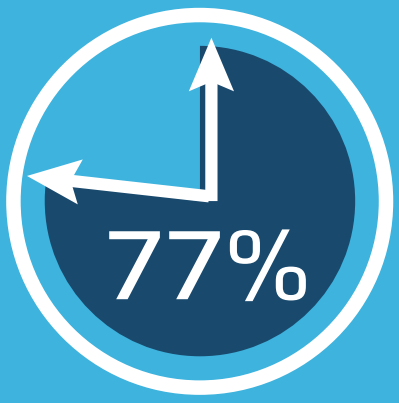
Insider threats are either malicious — or simply negligent — threats that originate from within the targeted organization. The threat may involve fraud, the theft of confidential or commercially valuable information, intellectual property or the sabotage of computer systems. An insider threat may be seemingly innocent — inadvertent employee errors like sharing data on an unapproved USB stick or another insecure device, or as simple as falling victim to a phishing scam by clicking on a malicious e-mail link.

> Insider-originated security breaches are almost twice as costly as the average breach.

The insider threat isn't always intentional. Negligence plays a big role when people make errors, disregard policies or carelessly put their organization at risk by any number of behaviors.

22% **OF ALL FOLDERS ARE ACCESSIBLE TO EVERY EMPLOYEE**

Varonis — *2021 Global Data Risk Report*



OF HEALTHCARE COMPANIES HAVE 500 OR MØRE ACCOUNTS WITH PASSWORDS THAT NEVER EXPIRE

79%

OF HEALTHCARE COMPANIES HAVE 1,000+ GHOST ACCOUNTS*

** USER/SERVICE ACCOUNTS THAT ARE INACTIVE BUT STILL ENABLED*

Varonis — *2021 Global Data Risk Report*

Human behaviors are almost always the primary indicators that alert us to potential insider threats. These behaviors can include users copying large amounts of data from one place to another or accessing data they have never needed before. It could involve the leaking of confidential data or misusing access to systems to inflict damage or disruption for personal gain.

So what drives an insider threat? More than two-thirds of the time, the primary motivation for an inside attack is money. With a staggering 34% of data breaches classified as insider attacks. A quarter of all data breaches are motivated by espionage or attempts to gain a strategic advantage[1]. Quite simply, the majority of insiders are trying to profit off the data that they are stealing.

Research indicates that insider-originated security breaches are almost twice as costly as the average breach.

Understanding the root causes of what triggers an insider threat is critical. Early detection and identification of stressors and behaviors that may be indicative of future threatening activity is critical. It affords the organization a chance to step-in to potentially offer assistance to employees before they commit a harmful act. Perimeter-based security strategies ignore the human stressors and concerning behaviors from insiders.

With organizations continually relying on expanding their businesses through technology, this only exacerbates the insider threat potential. To address these challenges, organizations must rely on new techniques to continuously evaluate those risks and measure the effectiveness of these controls. Therefore a thoughtful balance of traditional security and deterrence is necessary.

[1] 2019 *Data Breach Investigations Report,* Verizon Business Ready

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Yellowstone Financial is a high-end financial planning firm in Jackson Hole, Wyoming. They have a portfolio of high-profile, and high-net-worth clients, and they take cyber security VERY seriously. They were among the first to implement multi-factor authentication, they perform regular security training and testing, and have a full-time head of cyber security to protect their clients – because they know that a breach – any breach – would be devastating to their bottom line.

Kevin Casey, a mid-level planner, is a hard worker, but has consistently been passed over for a promotion for other higher-performing planners. He attributes his poor fortune to a less-than-ideal book of business and an increasingly adversarial relationship with his supervisor.

After four years of working his tail off to little benefit, Kevin decided enough was enough and quit. Not satisfied by the scathing exit interview that he performed, Kevin also downloaded a spreasheet of the firm's clients and their account numbers.

Six months after his exit, he shared a screenshot with his estranged boss of a bidding war on the Dark Web for this sensitive information.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

INSIDER THREAT - CYBER
cisa.gov

Intellectual Property Protection: Safeguard Your Company's Trade Secrets, Proprietary Information and Research
fbi.gov

Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense
fbi.gov

Insider Threat: The biggest security nightmare of a company
medium.com // 04.26.18

THREAT SPOTLIGHT: INSIDER THREATS

PLAYBOOK

6 TIPS TO KEEP YOU OUT IN FRONT

PROVIDE SECURITY AWARENESS TRAINING TO FOCUS ON INTERNAL THREATS

Regular and consistent security awareness training is critical. Monitoring awareness and understanding of cyber threat risks can be the best prevention. Periodic ransomware and phishing simulations can provide clues about compliance.

CLOSELY MONITOR AND MANAGE THE ACCOUNTS AND PRIVILEGES FOR ALL EMPLOYEES AND CONTRACTORS

Defining strict data access controls, so employees only have access to the information they need is essential. A regular, careful, review and analysis of requests for additional network or system access is vital.

STRICTLY LIMIT THE USE OF PERSONAL DEVICES

Limit the use of personal devices and the sharing of data outside of your corporate network by implementing strict network access rules.

REMIND EMPLOYEES THAT BIG BROTHER IS WATCHING

Simply reminding employees that all network activity is logged and monitored can make a bad actor think twice. Regularly remind employees that user accounts and permissions should be used for business purposes only and employees should never bypass or disable security controls.

IMPLEMENT STRICT PASSWORD POLICIES AND REGULARLY MONITOR USER ACCOUNT PRIVILEGES

Increasing password length to eleven characters using both upper and lower case letters, symbols and numbers improves security immensely. Turning on multi-factor authentication can reduce your risk of getting hacked by 99%. Closely monitor user account privileges, and make sure all accounts are closed or updated when an employee leaves or changes roles within your organization.

IF YOU SEE SOMETHING, SAY SOMETHING

Let employees know that they should report suspicious behaviors, or if they notice a possible security vulnerability, to their supervisor. The accidental insider threat incident can be reduced simply by double-checking the recipient list on e-mails and file-sharing.

FEATURED PARTNER

Verkada

For surveillance security there's no one "out in front" like Verkada for protecting people, assets and privacy. Verkada's video security solution delivers the most modern physical surveillance security without the need for network recording devices or network configuration — highly scalable, simple to install and fully secure right out of the box.

Verkada camera data is shared with users directly via their hybrid cloud system, so that footage can be instantly viewed from anywhere, at any time. Live-link sharing makes sharing the data easy which can significantly cut down response time in the event of a security incident.

Verkada's proprietary security cameras are plug and play, allowing users to be up and running in just minutes. Highly customizable, their systems allow businesses to set access controls, monitor environmental conditions and even noise sensing based upon needs.

In addition to cloud data storage, up to a year's worth of data is stored locally on the device ensuring access when internet access is lost. What sets Verkada apart is their software and unique dashboard allowing users to easily and intuitively browse camera history for exactly the data they are looking for. Motion-search, face-search, object-based-search and heat maps are just a few of the virtually limitless ways that a user can analyze camera data.

Verkada uses the most secure and up to date encryption standards and because their cameras are connected to the cloud 24/7/365, security updates are seamless and instantaneous. Verkada systems are simple and the most cost-effective way to scale and integrate coverage across multiple sites. Ideal for schools, hospitals and large businesses.

"We set out to build a system that would be easy to use, highly scalable, and fully secure out-of-the-box."

VERKADA DOME SERIES SECURITY CAMERA

OUT IN FRONT OF	Video Surveillance
WHAT VERKADA DOES	The most modern physical surveillance security that's highly scalable, simple to install, and fully secure right out of the box.
INDUSTRIES SERVED	☒ Education ☒ Large Enterprise ☒ Medical ☒ Finance ☒ Legal ☒ Retail ☒ Marketing ☐ Other: _____
KEY FEATURES	SEAMLESS UPDATES; PLUG-AND-PLAY INSTALLATION; HIGHLY CUSTOMIZABLE; CLOUD DATA STORAGE; MOTION-SEARCH; OBJECT-BASED SEARCH; FACE-SEARCH; HEAT MAPS
BEST FOR	HIGHLY SCALABLE FOR BUSINESSES OR ENTERPRISES SPREAD ACROSS MULTIPLE SITES AND/OR GEOGRAPHIC LOCATIONS

GOING P@S$WºRDLE5S!

PASSWORDS ARE A NECESSARY EVIL FOR ALL OF US – UNLESS YOU'RE A HACKER. THEN, THEY'RE A GODSEND.

Why? Because they are difficult for people (us) to remember and surprisingly easy for the hackers (them) to crack. Something as seemingly complex as an eight-character password using both upper and lower case letters, numbers and symbols can be easily cracked in under eight hours using the simplest hacking tools.

Two interesting facts: 59% of people use the same password for all of their accounts[1], and 81% of successful hacks are the direct result of a compromised username or password[2]. That means that a hacker who gets into your personal Pinterest account could be getting more than access to your collection of rustic entryway decor ideas; they could be getting your financial information and corporate account logins. At the end of the day, passwords are nothing more than a shared secret. A single-factor authentication system that is only as good as that one secret — staying secret.

Fortunately, the industry is beginning to move away from the traditional username and password authentication model that has been the norm and is shifting toward a zero-trust strategy — one in which conditional access is required. Conditional access, also called "informed access", will allow security teams to verify devices or validate users using a set of automated policies. These validation methods may include: time of day, geographical location, type of device being used, the user profile, or the purpose of the specific use.

Multi-factor authentication (MFA) complements a "password-only" gateway with additional authentication factors, such as a PIN, voice recognition, fingerprint or face scan. With multi-factor authentication, two or more authentication methods are required for login verification. When one factor is an authenticator, it's also unique every time — making it even more secure.

n. an alternative to passwords, requiring the user to provide two or more verification factors to gain access to a resource

Industry experts say that merely turning on multi-factor authentication will reduce your risk of getting hacked by 99.9 percent!

[1] LastPass, *3rd Annual Global Password Security Report*
[2] 2019 *Data Breach Investigations Report*, Verizon Business Ready

Fortunately, as technology evolves so, too, do the tools required to get everyone using passwordless authentication. Strong authenticators, like Apple's Touch ID and Windows Hello, are now built into nearly all new devices including laptops, cell phones, tablets and desktop computers.

IT teams are also utilizing other authentication options including smart cards and biometric technology like wearable rings to grant users secure access to resources. These authenticators use private-public keypair cryptography — better known as a credential to grant login permission. A **private key** that is stored securely on the user's device, and a **public key** that can be shared with the server. They are validated by a transmitted token that a user receives by e-mail, via smartphone or through a hardware token connected directly to a user's device. Once confirmed, the user is granted access.

n. a large numerical value used to encrypt data

n. a large numerical value linked to a public key required for decryption

The fact that the server receives no secret key has broad protection implications for the security of users and IT departments. With passwordless access, databases cease to be the attractive targets to hackers that they once were, because the public keys are no longer useful to them.

Gartner predicts that, by 2022, 60% of large and global enterprises as well as 90% of midsize enterprises will implement passwordless methods for more than half of their users.

More and more organizations are adopting passwordless authentication. Gartner predicts that, by 2022, 60% of large and global enterprises as well as 90% of midsize enterprises will implement passwordless methods for more than half of their users.

59%

OF PEOPLE USE THE SAME PASSWORD FOR ALL OF THEIR ACCOUNTS

TURNING ON MULTI-FACTOR AUTHENTICATION WILL REDUCE YOUR RISK OF GETTING HACKED BY

99.9%

88%

OF SUCCESSFUL HACKS ARE THE DIRECT RESULT OF A COMPROMISED USERNAME OR PASSWORD

2 Varonis — *2021 GLOBAL DATA RISK REPORT*

2019 VERIZON DATA BREACH INVESTIGATION REPORT VERIZON BUSINESS READY)

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Kay Edmunds is an office manager at a law firm specializing in malpractice in Charleston, South Carolina. As the office manager, Kay is the first face many clients meet and is often the one who locates and provides files to the team of 16 attorneys in the firm.

Her role has become increasingly dependent on technology as she accesses the firm's database, local court records, and medical files on an hourly basis – if not more frequently.

To make her life just a little easier, Kay uses the same password for all of her accounts – a creative twist on her Chihuahua's name. She was advised to use upper and lowercase letters, numbers, and special characters to make her password more difficult for a hacker to guess, and because she is aware of the sensitivity of the data that she has access to, she even changes her password on bi-monthly basis. One afternoon, Kay receives an email that appears to come from the firm's Office 365 account, informing her of a pending message. Kay logs in with her new and complicated password and sees that there is no message waiting for her. While Kay assumes that it's a simple error and thinks nothing of it, she has just given her password up to a hacker.

That password has power – giving the malicious attacker access to sensitive information that he can use to extort – or even ruin – the law firm, the lawyers, and its clients.

With multi-factor authentication enabled, that password's power fizzles. Upon attempting to utilize the password, Kay would have received an authentication message alerting her of the attempt to access, which she would have blocked. This version of the story is decidedly less interesting, but excitement is rarely a good thing in the world of cyber security.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

Supplementing Passwords
us-cert.cisa.gov // last revised 01.21.20

What a Passwordless Future Looks Like for Federal Agencies
hstoday.us // 03.09.21

PLAYBOOK

7 TIPS TO KEEP YOU OUT IN FRONT

TURN ON MULTI-FACTOR AUTHENTICATION ON YOUR DEVICES!

Most new devices today have the ability to use multi-factor authentication technology. In many cases, it's as simple as enabling conditional access to these devices and enabling the passwordless technology to enjoy these security features. If you don't do anything else, you'll still be way ahead of the game.

GET THE TECHNOLOGY RIGHT

If your organization is looking to take the next steps toward going passwordless, make sure you're partnering with the right security or technology partner to ensure your implementation meets your business security needs.

UNDERSTAND HOW PASSWORDLESS AUTHENTICATION WILL BE IMPLEMENTED

Know how the technology will be used on your businesses existing technology platform. Ensure that future purchases can utilize the updated technology.

ASSESS YOUR ORGANIZATION'S RELIANCE ON PASSWORDS

With your security partner, examine your security vulnerabilities.

STILL USING PASSWORD-BASED SINGLE AUTHENTICATION FACTOR LOGIN?

Use passwords that have at least 11 characters including a combination of capital and lower case letters, numbers and special characters; consider using a password generator; use a password locker; and steer clear of using passwords with family members names or the name of pets.

SHUT THE FRONT DOOR

While anti-virus systems, secure firewalls and vulnerability tests are necessary security elements, without user authentication ability enabled, it's just a matter of time before being compromised.

MAKE SURE YOUR CREDENTIALS COME FROM AT LEAST TWO PLACES

Something you know (like a password or PIN), something you have (like a smart card, or token), or something you are (like your fingerprint or face scan).

RED CANARY DISCOVERS macOS MALWARE BREACH

In early 2021, security experts at Red Canary discovered a new malware that silently infected nearly 40,000 macOS systems running on Apple's latest M1 chip architecture – keeping the global behemouth out in front of imminent disaster.

Named Silver Sparrow, the malware has been found in a dormant state on computer systems and appears to wait for commands from its operators. Its true operational purpose is still a mystery. This is the second discovery of malware designed to run on Apple's chipset for Macbooks.

The Silver Sparrow malware is considered a serious threat due to its forward-looking M1 compatibility, global reach, and relatively high-infection rate. While it hasn't caused any harm to infected computers, it just means that security experts don't yet know the true intent of the malware.

For now, users should remain vigilant by only downloading apps from reliable places like the official Apple App Store. Make sure you're regularly running an up to date antivirus software. And keep your Mac up to date by always running the latest security updates from Apple.

Red Canary provides security operations solutions, open source tools, and education for the information security community.

Q&A with Brian Donahue, Intelligence Analyst at Red Canary

Q: CAN YOU TELL ME A LITTLE BIT ABOUT THIS MALWARE, WHAT IT IS DOING?

A: Most malware has an ultimate goal. It might be to steal sensitive information, cause damage to devices or servers, or block access to data. In this case, we don't actually know what that ultimate goal is, because we haven't observed Silver Sparrow engaging in malicious activity. However, most malware operations consist of multiple supporting functions that occur prior to the execution of said activity. This would include things like initial access (i.e. how the malware infected a machine in the first place) or lateral movement (i.e. how the malware moves between devices on a network). In the case of Silver Sparrow, while we haven't observed the final payload, we have seen other parts of the malware operation. For example, we've observed it using built in functions of macOS to install itself on victim machines and to maintain persistence across reboots.

Q: HOW WAS IT DISCOVERED?

A: A member of our cyber incident response team (CIRT) detected this threat based on suspicious behaviors emanating from a customer macOS machine.

Q: WHAT SORT OF DEVICES DOES IT IMPACT AND HOW MANY DEVICES HAS IT IMPACTED?

A: As of today, we can confirm that the threat has infected nearly 40,000 macOS devices. This is based on detection data gathered and published by antivirus company Malwarebytes. Given their limited visibility, this is probably an underestimation of the total scope of the threat.

Q: WHAT SHOULD MAC OWNERS DO IF THEY ARE WORRIED ABOUT BEING IMPACTED BY THE MALWARE?

A: It's very difficult for us to offer consumer-level guidance for macOS users, given the disparities in technical proficiency and tooling available. That said, as a general rule, we typically recommend that users run third party antivirus or antimalware products to supplement the existing antimalware protections maintained by operating system manufacturers. While we're talking specifically about macOS in this case, this advice is just as applicable to Windows machines.

Q: WHAT IS THE PURPOSE OF THIS MALWARE AND DO YOU HAVE ANY IDEA ABOUT ITS ORIGINS?

A: We do not currently know what is the origin or ultimate purpose of this malware.

Q: WHAT MAKES THIS MALWARE SO "MYSTERIOUS" AS IT'S BEING CALLED?

A: There are two things about Silver Sparrow that we don't quite yet understand. The most obvious is that it lacks an ultimate payload, which, by extension, means that we can not determine what is the purpose of this threat. The second relates to a file that, if present on an infected machine, causes Silver Sparrow to uninstall itself. We do not know why this file is present on certain systems or why its presence causes Silver Sparrow to uninstall itself.

EMBER™

Delivering best-in-class cyber security, IT management, and consulting services to small-to-mid-sized businesses

EMBERIT.COM