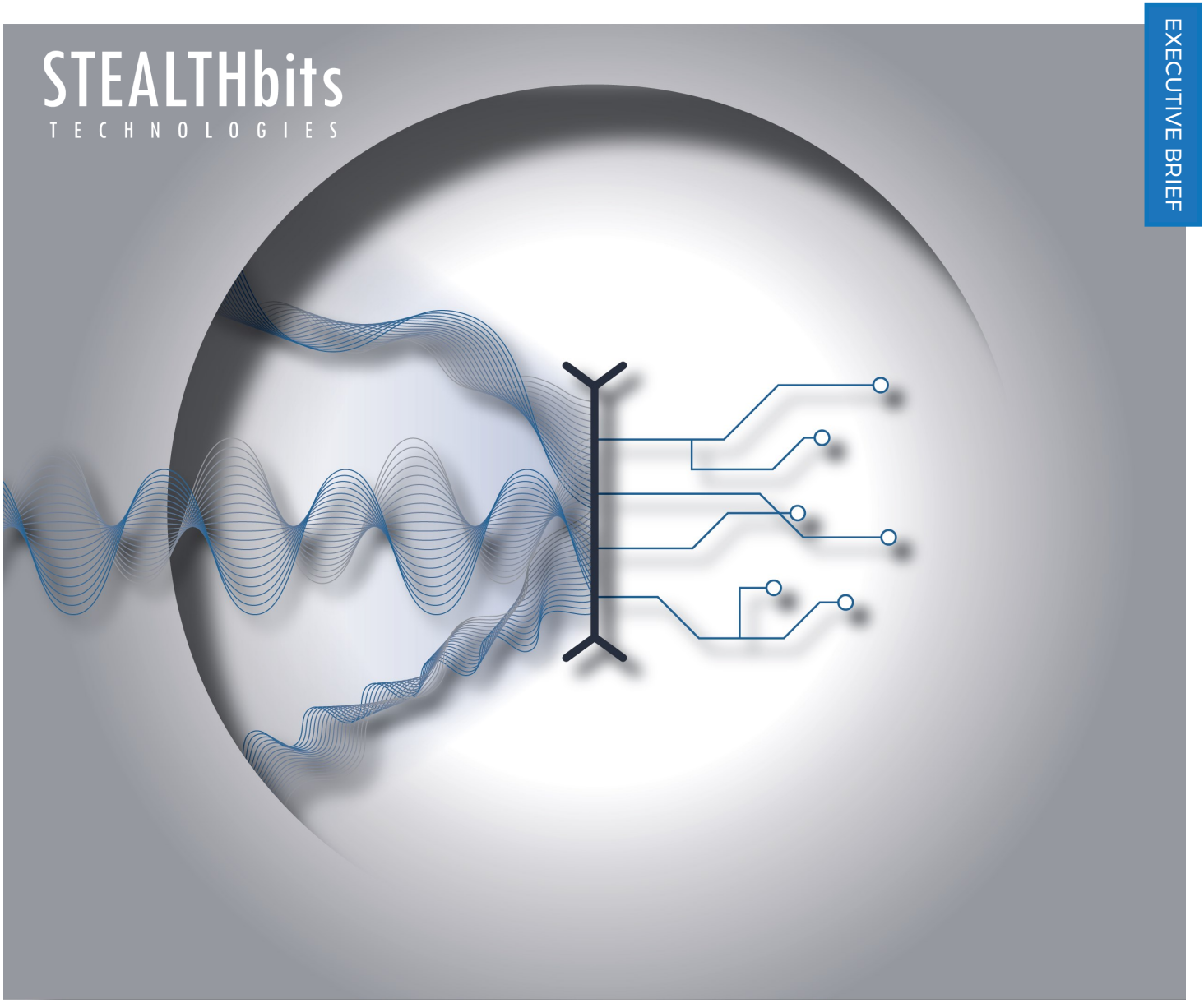
STEALTHbits
TECHNOLOGIES

EXECUTIVE BRIEF



CREDENTIALS AND DATA

The Common Denominator in Every Data Breach

INTRODUCTION

> *"Most people spend more time and energy going around problems than in trying to solve them."*
>
> - Henry Ford

Ever feel like you've been focusing on the wrong thing? Like, you've been spending a lot of time and energy doing something important, yet not impactful? We think that's how a lot of security professionals feel. They work so hard to protect their organizations from harm, but some script kiddie phishes poor, unsuspecting Phyllis from Accounting with the promise of "the most adorable cat videos of the year" and it all goes to hell in a handbasket. It's just not fair!

You've spent the money. Where's the return? You've guarded the gates. How are they still getting through? Listen, where there's a will, there's a way – and that's just the honest truth. This security game is real, and while it might not be a game for you, it is for them.

The IRA once famously said to Margaret Thatcher after a failed assassination attempt, "We only need to be lucky once. You need to be lucky every time." This is what most organizations are left to rely on: luck. If the attackers are any good at their craft, they'll only be exposed if they make a mistake – a big mistake. Companies are still trying to figure out how to sift through the noise of their SIEM solutions and Intrusion detection systems. It's often a stroke of luck that draws their attention to an event that actually amounts to something.

So is it a losing battle altogether? Should we just surrender? Well, we have no choice, we have to fight. But, more importantly, it's not a losing battle, and waiving the white flag doesn't make a whole lot of sense, especially if we want paying jobs. What we need is a healthy dose of reality, and a dash of pragmatism. If we change the rules of the game just a little, we can make it a whole new ballgame altogether. We need to focus on what attackers are after, rather than solely on how they get there. And when they do get there (and they will), we need to know they're there immediately so we can have the smug satisfaction of cutting them off at the knees after they've made it so far. Man that feels good!

SO WHAT'S IT ALL ABOUT THEN?

It's simple, folks. It's about two things: credentials and data. Read any report you'd like. Diagnose any breach. It ultimately boils down to these two things and they're the only two that matter . You can't unlock the data if you don't have the keys. This isn't like the

physical world where you could kick in a door. If you want access to something in the digital world, you need a key; plain and simple. Of course, in the digital world, you can steal keys – even make keys – much more easily, but the attackers are essentially bound by the same fundamental principles as the rest of us. Want to get past the gate? You must authenticate.

It's about two things: credentials and data. Read any report you'd like. Diagnose any breach. It ultimately boils down to these two things and they're the only two that matter.

NO SILVER BULLET

Unless you're talking about an ice cold Coors Light, you've got to accept that there's no silver bullet in this situation. That said, focusing on your credentials and data and implementing a few critical capabilities to protect them could make it so frustrating for an attacker to carry out a successful mission, it might even evoke a little schadenfreude.

DEAD ENDS CAN BE JUST AS EFFECTIVE – AND EVEN MORE SATISFYING

Let's pretend for a minute that we have an opportunity to watch an attacker phish our friend Phyllis and compromise her account. Let's also imagine that in Phyllis' company, they've focused their efforts heavily on credentials and data security. How might this attack actually go down? (Queue the harp music…).

WATCH YOUR STEP

Due to the aforementioned phishing email, our attacker is on Phyllis' machine, and he's stoked; he has the foothold he's been looking for. First things first, though. Let's get the lay of the land. He hits the Windows key, types 6 letters, and hits enter. The first high-powered weapon from his devastating arsenal opens instantly: Windows PowerShell. A few minutes later, he's got a listing of every file server, the location of every SharePoint farm and Domain Controller, and of course, the members of the Domain Admins group. Bad move though. He doesn't know it, but his seemingly harmless directory query that pretty much anyone can do at any time just got flagged like a late hit on Tom Brady.

Now our attacker is getting more than a little discouraged. The account he's compromised has access to nothing of particular interest or value, and he can't find any other accounts that would allow him to access another system. There's only one thing to do in this situation; make them come to him. A quick configuration change in Phyllis' Outlook profile late one Sunday evening starts Phyllis' week off with a call to the helpdesk. She's a regular, you know, and Tony the Domain Admin likes to butter her up a bit because Phyllis is responsible for approving expense checks and his latest trip to

the Black Hat Conference in Las Vegas may have led him to leverage the corporate credit card for an otherwise "personal" expense. Tony volunteers his services and logs onto Phyllis' compromised system with his Domain Admin creds. Jackpot! Our attacker now has access to everything in Active Directory, and thus, everything connected to it. If that sounds bad, that's because it is, but as our attacker will find out, his blissful ignorance in thinking he's won is going to result in an anvil squashing him flat like Wile E Coyote.

Our attacker has made his way to one of the Domain Controllers he identified and now he's going to do what pretty much every attacker does. He creates a new user and adds them to the Domain Admins group. Access Denied? How could this be? He's already got Domain Admin creds, so how come he can't do what Domain Admins do? It just doesn't make any sense. What our attacker again doesn't know is that in Phyllis' company, even the watchers are being watched. Changes like these can't even be made by the most privileged of users, and now, our attacker knows something's up. Things aren't working the way they always have. The way they're supposed to. And now he's got the sinking feeling he's been exposed. And he has. Domain Admins don't make (or try to make) changes from computers like Phyllis' – never have. This is simple for the company's security analytics technology to spot, and our attacker now has an army of Security Analysts descending upon him.

Game. Set. Match.

WHAT JUST HAPPENED?

The aforementioned scenario is not conveniently contrived. In fact, the tactics our attacker employed are far too common, and really aren't that hard for any attacker worth their salt. But what made this situation different? Of course, it was Phyllis' company's focus on what mattered most; credentials and data. It was their focus on protecting what the attacker was after, and not solely on how he was getting there.

So what steps can an organization take to be as well-positioned as Phyllis'? Let's first quickly define the security concepts employed in our example that made this attack so difficult to perpetrate.

DATA ACCESS GOVERNANCE (DAG)

Essentially a subcomponent of the Identity & Access Management (IAM) space, DAG aims to provide understanding and oversight into data access, with the added context of data sensitivity, usage, and ownership as pivot-points for determining proper access rights (i.e. achieving a Least Privilege Access model).

In a recent study published by the SANS institute of 12 separate data breaches, it was determined that "only 14% of the information stolen by an adversary was needed by the

owner of the compromised account." This fact clearly illustrates the need for tighter data access controls, as the overwhelming majority of the data stolen by attackers was practically handed to them.

CHANGE & ACCESS MONITORING

Unlike in years past when Change & Access Monitoring was more about compliance and having a record of who did what and when, the role of Change & Access Monitoring has evolved into a mechanism to monitor and enforce security policy. As a practical example, the use of privileged credentials (e.g. AD Domain Admin) on vulnerable systems (e.g. an internet-facing workstation) is what allows attackers to easily escalate their privileges and move laterally and vertically within an environment.

In their paper titled "Mitigating Pass-the-Hash and Other Credential Theft, version 2", Microsoft themselves state that "the attack surface is primarily shaped by operational practices", which means that the very people entrusted to safeguard an organization's assets may be the ones responsible for exposing them to the most risk. Understanding when violations of security policy occur and proactively addressing them is as key to reducing the attack surface as any other single tactic.

USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

Far from a new concept, yet significantly more advanced due to innovations in Machine Learning algorithms, the use of Big Data architectures and enhancements in data intelligence over the past decade, User and Entity Behavior Analytics aims to detect abnormalities in user and system behaviors.

UEBA is leveraged for the purpose of security intelligence; identifying patterns of behavior, and even discrete, individual events that are out of the norm or indicative of account or system compromise, allowing security analysts to easily focus in on outliers without all the extra noise. Careful though. As Frank Rizzo, data and analytics leader at KPMG recently stated in an interview, "Cognitive computing will augment the work we do as humans and not replace it." UEBA is a capability, not a solution in and of itself – at least not yet.

NO TIME TO WASTE

As mentioned previously, this security game is no joke, and like most games, time is a factor – an important one. In fact, a survey given at the Black Hat Conference in 2015 revealed that "73% of IT Pros think they'll be breached next year." We think they're probably right, so if you want to protect yourself like Phyllis' company did, do the following:

1. Focus on what every attacker is after (again, credentials and data)

You can't get any closer to the attacker than you can by attaching yourself to the accounts, passwords, and data attackers are after. This doesn't mean you should forget about the "perimeter" or pull the funding on your SIEM project – they have their place as well – but, it does mean that those other protections will continue to be largely ineffective until they're coupled with proper access and security controls at the credential and data levels.

2. Reduce data access rights and permissions to the fewest number of people and the lowest levels possible

If you want to implement a Least Privilege Access model, you need the ability to collect the following data: effective access, data sensitivity, and data activity. With this dataset, you'll be able to properly identify and remediate vulnerabilities like Open Access, prioritize efforts by knowing where your most sensitive data resides, and implement a maintainable security model with automated governance controls that allow your data owners to review and control access to their data with ease.

3. Monitor and enforce security policy in accordance with the level of risk your organization is willing to assume

If privilege escalation is allowed to occur because an administrator inappropriately uses their credentials on a system they shouldn't, then don't let it happen. If only certain people are allowed to make critical changes that affect administrative or sensitive data access, then monitor and enforce it strictly. Policy is the foundation your security program is built upon. If simple policies can't be monitored and enforced, everything else can and likely will suffer as a result.

4. Concentrate on detecting true outlier behaviors that expose bad actors and their tricks

In the very near future, billions more devices will be connected to the internet and our networks. The "noise" has already proven to be insurmountable for many organizations, strengthening the argument to cut through that noise and hone in on what matters most. Behavioral analytics, when properly implemented, are now able to leverage details and context that were previously unavailable to identify true outlier behaviors as they're happening, enabling the defenders of our enterprises to keep in lockstep with attackers, and sometimes even a step ahead.

THAT WAS FUN!

Wouldn't it be satisfying to catch these kinds of attackers? These are the ones that you ought to be worried about most, after all. If you're catching them at the gate, then you're probably not dealing with an "A Player", and as a result, it's highly likely they're going to make that big mistake pretty early on in the game anyway. These attackers, the ones who slip past your jacked up bouncers and into the dark, noisy, crowded nightclub that is your internal network, are the ones we're looking for and can pick out like a teenager with fake ID by using the right tools, tactics, and strategy.

It's about credentials and data. Wouldn't you agree?

STEALTHbits TECHNOLOGIES

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data.