PROMPT#

# THE ANTISOC ISSUE

## CONTINUOUS PENETRATION TESTING

IN THIS ISSUE:

ARTICLES

GAMES

COMICS

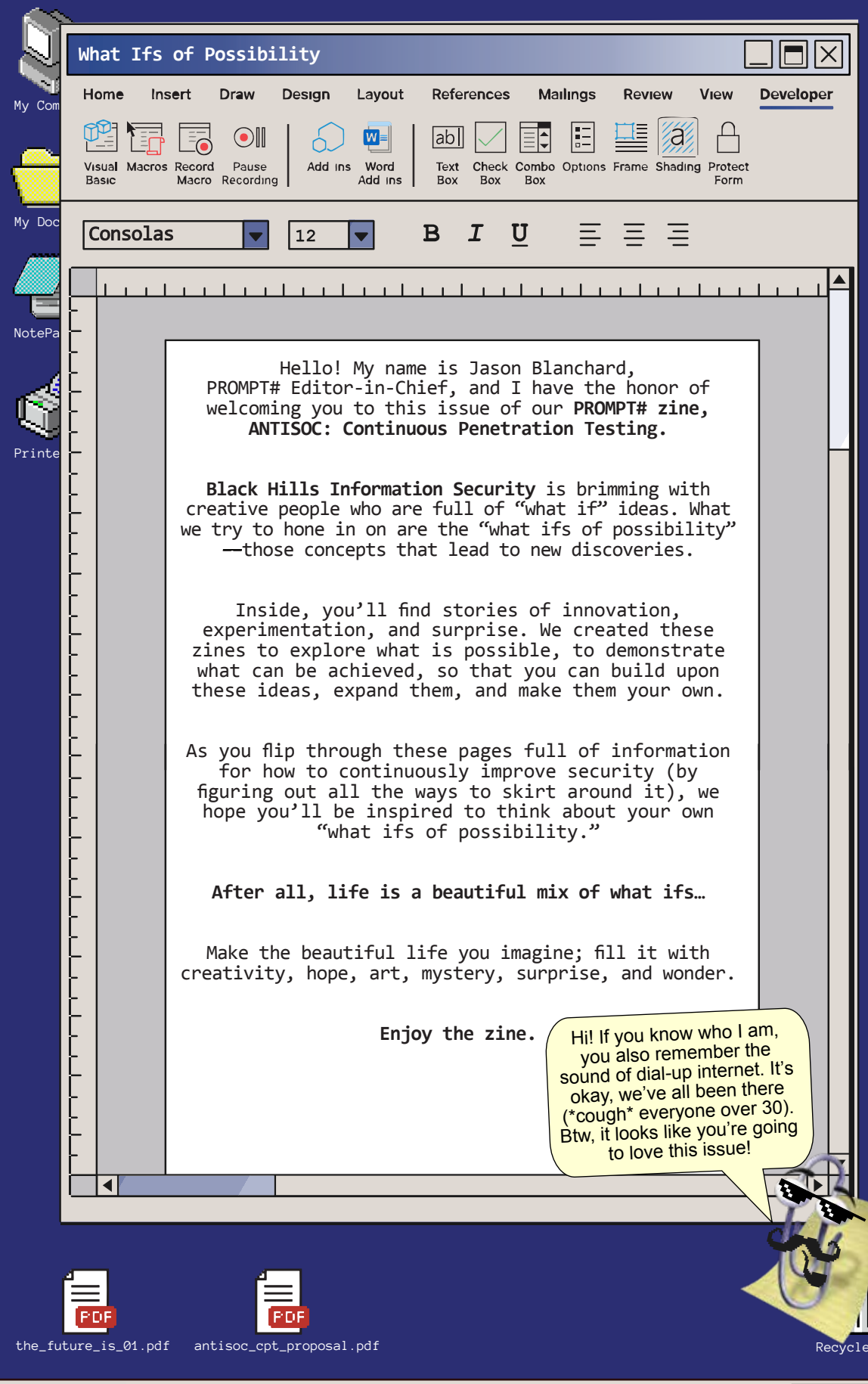
AND MORE...

YOUR FRIENDLY


YES, IT'S free

NEIGHBORHOOD APT


THIS IS THE PLACE... HE SHOULD BE HERE.
I DON'T KNOW... DOESN'T LOOK LIKE ANYONE STILL WORKS DOWN HERE.
HELLO... WE NEED SOME HELP UPDATING THE SYSTEM AND WE WERE TOLD YOU WERE THE ONE WHO DEPLOYED IT.
GO AWAY... YOU'D BE HAPPIER REBUILDING FROM SCRATCH.
PLEASE, SIR, WE'RE DESPERATE.
IF YOU START DOWN THIS PATH, YOU MIGHT NOT LIKE WHERE IT LEADS.
WE'RE READY. WE'RE NOT AFRAID.
OH... YOU WILL BE.
LEGACY KNOWLEDGE
The Defenders must roll again to see if the person who built the system is still working at the site.
NOTES
(1-10) means the happily retired individual is not there to assist them.
-2 modifier on the next turn
(11-20) means the grizzled veteran that deployed the legacy system still works at the site to assist them.
+2 modifier on the next turn
Inject Card from ICS/OT Backdoors & Breaches, created by BHIS + Dragos
ICS/OT_V1.1_0822
Backdoors & Breaches


What Ifs of Possibility
Home Insert Draw Design Layout References Mailings Review View Developer
Visual Basic Macros Record Macro Pause Recording Add Ins Word Add Ins Text Box Check Box Combo Box Options Frame Shading Protect Form
Consolas 12
Hello! My name is Jason Blanchard, PROMPT# Editor-in-Chief, and I have the honor of welcoming you to this issue of our PROMPT# zine, ANTISOC: Continuous Penetration Testing.
Black Hills Information Security is brimming with creative people who are full of "what if" ideas. What we try to hone in on are the "what ifs of possibility" —those concepts that lead to new discoveries.
Inside, you'll find stories of innovation, experimentation, and surprise. We created these zines to explore what is possible, to demonstrate what can be achieved, so that you can build upon these ideas, expand them, and make them your own.
As you flip through these pages full of information for how to continuously improve security (by figuring out all the ways to skirt around it), we hope you'll be inspired to think about your own "what ifs of possibility."
After all, life is a beautiful mix of what ifs…
Make the beautiful life you imagine; fill it with creativity, hope, art, mystery, surprise, and wonder.
Enjoy the zine.
Hi! If you know who I am, you also remember the sound of dial-up internet. It's okay, we've all been there (*cough* everyone over 30). Btw, it looks like you're going to love this issue!
the_future_is_01.pdf
antisoc_cpt_proposal.pdf
Recycle Bin
Start
What_Ifs_of...
4:04 AM



**ANTISOC** is a hacker operations center. The name is inspired by the relationship between matter and antimatter, which are mirrors of each other with complementary components.

When we were creating ANTISOC, we originally called it "Continuous Penetration Testing," which is fine, but "continuous" is annoying to spell and "penetration testing" means different things to different people. I think if you asked ten security folks what a penetration test was, you'd hear at least five different answers, but if you asked the same people what a SOC (Security Operations Center) was, you'd get one consistent answer. We wanted to embed this meaning right into the ANTISOC name, but with a twist.

If a SOC's purpose is to detect and prevent attacks, ANTISOC's purpose is to emulate those same attacks against our clients. A SOC uses data feeds like event logs and alerts generated by security products to defend their clients. We also use data feeds, like dark web data or vulnerability scans, but with the goal of attacking a target instead of defending it. A SOC also operates over a long period of time, building knowledge about an environment to defend it better. ANTISOC does the same, but with the goal of streamlining attacks and bypassing defenses that we previously encountered.

Lastly, a SOC is a team. Some tickets or alerts might be worked by a single analyst, but if there is a serious incident, the whole SOC bands together to investigate and protect the organization. Some analysts have specialties that complement the skills and knowledge of others on the team. We have the same dynamic in ANTISOC. Some operators specialize in initial access, social engineering, or tool development, while others are generalists who can help wherever needed.

ANTISOC might sound antagonistic to some people, but we don't see it that way. We have the utmost respect for our defender counterparts. If you really think about it, we are all blue team at the end of the day.

PS: Our ANTISOC operators have written the articles in this zine issue, so we hope you enjoy!

BY COREY HAM

# BAD HABITS

## AN ANTISOC OPERATION



ANTISOC uses a mix of techniques from traditional penetration tests like red teams, cloud, web applications, externals, internals, and, of course, social engineering. We combine this mix of techniques with a wide-open scope, with the goal of going beyond what a typical pentest can discover. Let's dive into an example:

**Carl was a helpdesk technician.**

As one of only two technicians working for ACME Inc, he was responsible for anything and everything that users needed help with. Carl was always confused by how many users needed their passwords reset. How could people be so forgetful of something they use every day? This issue was compounded by the fact that the security team had recently added the requirement that all users must pick longer, more complex passwords. It was difficult to even describe to a user what the criteria were: 15 or more characters, including a variety of uppercase, lowercase, numerical, and special characters.

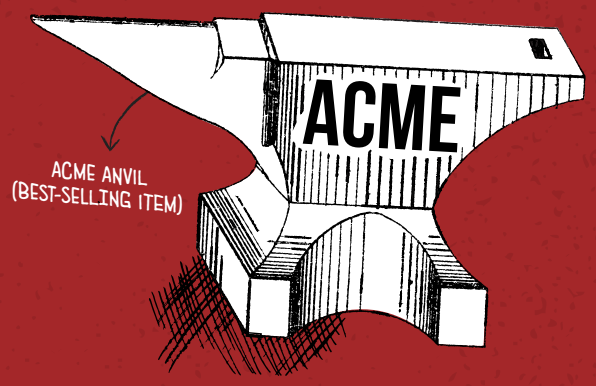
**IceCream99!**

(NOT THE REAL PASSWORD)

At first, he generated random passwords using the tool provided by the security team, but these were difficult to read to users over the phone. "M as in MARY, Janice, and by the way I think you need a new phone; I can barely hear you." These random passwords were slowing things down too much. To save time, Carl came up with a secure password that was easy to dictate over the phone and met the password complexity requirements. He started assigning this password to all users who requested a reset, and it became second nature for him to recite it. He also set that password on any contractor accounts that expired because keeping track of all those different passwords was too complicated.

Carl figured the risks of doing this were minimal, as users would eventually change their passwords. What Carl didn't realize is that when security changed the password policy to 15 characters, they also removed the requirement for users to change their passwords at a regular interval. This meant that over time, more and more users ended up using the identical password that had been set for them by Carl.

Eventually, an ANTISOC operator placed a social engineering phone call to Carl's helpdesk and asked him to reset the password for a target user. Later, when the security team contacted him during an investigation, Carl found out that this particular password reset had led to an account compromise. The security team assured Carl that they had detected and contained the compromise, so he didn't worry too much about it.





ACME GLUE
(VERY EFFECTIVE
ON ROAD RUNNERS)

ANTISOC operators noted that the password set by Carl wasn't random. They had obtained a listing of all users from Entra ID during post-exploitation and decided to spray Carl's password across these accounts. This led to the compromise of more than 100 accounts that Carl had reset passwords for over the years.

Most of these accounts had multi-factor authentication (MFA) set up properly, but some had not been used in years and did not have MFA configured. ANTISOC operators slowly picked through each account, taking note of any accounts that had not completed MFA enrollment. They configured MFA for them and quietly enumerated what access they had. Some of this activity was detected by ACME Inc's security team, but it was difficult for them to determine which accounts might be compromised, as they were not receiving full logs from Microsoft during the original password spray with Carl's password.

With a handful of accounts enumerated that had remote access via virtual desktops, ANTISOC operators deployed a command-and-control presence within ACME Inc's internal network environment. Instead of using a commercial C2, like Cobalt Strike, ANTISOC used SSH to tunnel network traffic from their devices into the ACME Inc network. This, combined with persistence tactics that replaced the zoom.exe binary in the user's profile, led to a long-term compromise of ACME Inc by ANTISOC operators.

**NOBODY PANIC!!!**
**IT IS ALL UNDER CONTROL.**
**RIGHT? RIGHT??????**

EVERYTHING WAS, IN FACT, NOT UNDER CONTROL

ANTISOC operators did their best to circumvent detection on the internal network by avoiding common attacks targeting Active Directory. Instead, they searched SharePoint and discovered a file containing shared credentials for SaaS applications. Most of these passwords were inconsequential, but some were for business-critical applications, like the automated backup solution used by ACME Inc. Within the web portal for this backup solution, operators could view and modify the backup contents from every computer that had been automatically backed up.

This same access, in the hands of a ransomware group, would have been devastating to ACME Inc. After all of this had been reported, ACME Inc knew it would take months or years to fix all these issues. First, they created alerts for as much as possible so that they would receive early warning signs. Next, they changed the affected passwords and disabled open enrollment of MFA factors. They deployed endpoint detection and response (EDR) on all VDIs (virtual desktop infrastructure) and made sure that logging from Microsoft Azure was functional. They also disabled local logins to the backup solution, requiring authentication via SSO to access this tool.

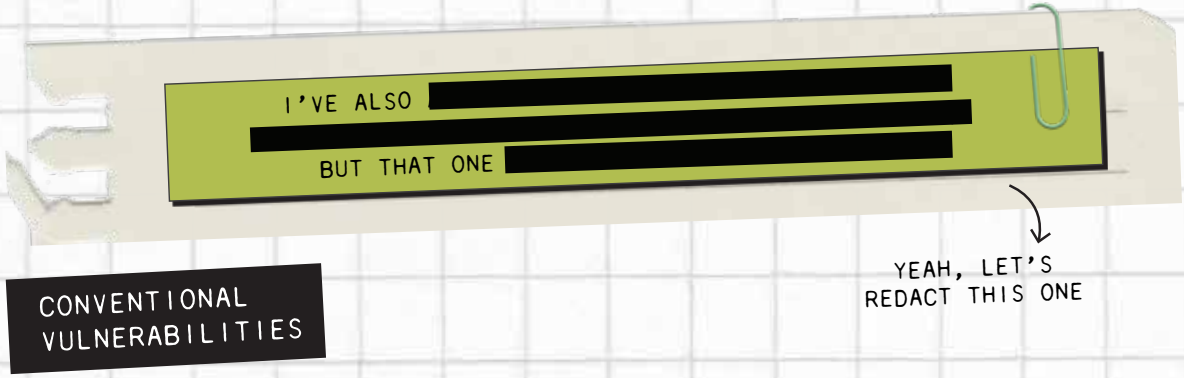

For web developers, success is measured by demonstrating that the built application can do what it was designed to do. Fortunately for **your friendly neighborhood APT**, when an app is built to do a thing, it will often unintentionally allow those who are interfacing with it to do other things. For us, success is measured by finding all the things the app CAN do, rather than just the things it SHOULD do.

Web app hacking starts with two questions. First: "What did the developers intend for this app to do?" Asking this question helps us think like a developer, considering how the app might have been built and what mistakes might have been made along the way. Once we have some context about the app's design, we get to the second question: "Now, how can I cause trouble?"

One reason we like the web is that it adds some spice to the pentesting life by frequently displaying behaviors we do not expect. Like that time my Burp Collaborator began getting callbacks from Bogons.

Bogons are reserved IP addresses, which you should never ever see routed through the public internet. These include internal addresses (e.g., 10.x.x.x) as well as reserved addresses and addresses not yet allocated by IANA. One day, we were sending malicious payloads to an application programming interface (API) endpoint that, among other things, sent a notification email to a user-input email address.

When changing the host header to a Burp Collaborator URL, in combination with a malicious payload in the body of the request, our Collaborator domain would receive HTTP requests from an unallocated IP address. Changing the collaborator URL domain or path resulted in receiving requests from different source IPs; however, we were unable to find a method to that madness. The leading theory for this behavior remains that our payloads were somehow breaking the site's backend, causing the code to inadvertently spoof the source IP of its own requests. Interesting day.




## CONVENTIONAL VULNERABILITIES

Of the more typical web application vulnerabilities, here are the ones I have seen most over the past couple years.

### IDOR

Insecure direct object reference (IDOR) occurs when an application allows access to endpoints but either doesn't check IF a user is authenticated or doesn't check WHO is authenticated.

The result of such a vulnerability is that an attacker can access data they aren't supposed to. For example, if I'm looking at an application and have access to the endpoint website.com/account?patientid=446, I am always going to attempt to access patientId=447. It is surprising how often this is successful.

## SQL INJECTION

While injection vulnerabilities are becoming less common on recently developed apps, many apps still in existence are older or were not developed using modern development frameworks. I discovered several instances of SQL injection last year: one manually that was missed by SQLMap, and the other was found by SQLMap but missed by both manual testing and Burp's scanner. The first was an account number on a bill calculator website. It was not picked up by SQLMap because the payload had to begin with a numeric value. Once I edited the SQLMap config, I was able to automate the data extraction. The latter instance was a time-based blind injection on an application for a "smart" medical device. **Oh, also, cross-site scripting is still around.**

## UNCONVENTIONAL VULNERABILITIES

As security awareness has increased, many easy-to-exploit vulnerabilities have been eliminated. Software development kits (SDKs) and web development frameworks now include input sanitization in their APIs, reducing the burden on developers.

But web apps often interact with a larger ecosystem. From this perspective, a wide range of things can be considered web vulnerabilities. For example, while testing an online shopping app, a Google search for site:targetwebsite.com filetype:pdf revealed product return labels. This meant some customers' names, phone numbers, and addresses were indexed by Google. Not critical, but not great for targetwebsite.com's reputation either.

Another time, I hacked a web app with hand-drawn sketches. It was a shopping rewards mobile app that used optical character recognition (OCR) software to read photos of user-provided receipts from participating stores. The more you spent, the more reward points you could rack up to unlock exclusive coupons or freebies. This process begged the question: "What does the application consider a valid receipt?"

I made some doodles while on a call and quickly discovered that to accept a "receipt," the OCR software required a recognizable company name, the word "total" followed by some number, and a valid date within the past two weeks. Soon I had gold status and any reward of my choosing. Again, not enough to take down the company, but certainly a vulnerability with monetary impact.

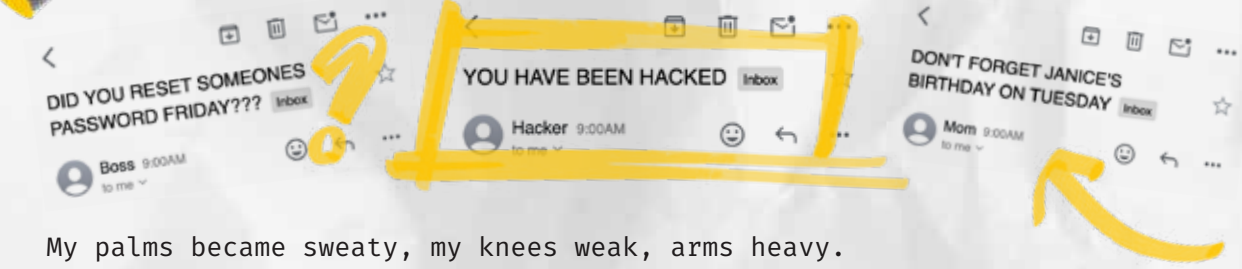
# THE FRIDAY THAT RUINED MY MONDAY

BY ALICE MURPHY

Mondays always felt like a fresh start, a clean slate. Unburdened by the weight of the previous week's mistakes.

I like to start my Mondays with coffee. Black. No cream, no sugar. Bitter, strong, and honest. The morning's cup sat on my desk, steam faintly curling up from it. The initial sip burned the roof of my mouth. But I didn't mind. I always thought the burn was part of the point—a reminder that you were alive.

But despite the heat from the coffee, the subject lines of my first three emails stopped me cold:




My palms became sweaty, my knees weak, arms heavy.

Mondays were supposed to be a fresh start. A clean slate. But this one was already stained.

Bonnie.

A good name for someone who wears sincerity like a mask. She was my last call of the previous Friday.

I remember Bonnie calling in, her voice piping into my headset:
"Hi, I got a new phone and I'm having trouble logging in to my account. Can you help me?"

Always happy to assist, I responded, "I can help you with that. Can I get your full name and email?"

There was a barely perceptible pause, heavy with an unknown weight. Before I could dwell on anything that felt off, she answered,
"Of course. It's Bonnie Palmer. My email is Bonnie.Palmer@example.com."

I typed her information into my system, the key taps echoing like footsteps in an empty hallway.
"Thank you, Bonnie. What exactly are you having issues with?"

Another pause, this one as brief as the previous. "I can't seem to remember my password, and I can't reset it without the authenticator on my old phone or without sending a text to my old phone number. My old phone is in multiple pieces, and the store made me get a new number with the new phone." Her voice was quiet, almost muted with the weight of a clearly bad memory.

I replied, my tone light. "Ok, Bonnie, to verify your identity, I just need to ask a few security questions."

Yet another pause. My headset crackled faintly, the sound of a storm building off in the distance.

She finally responded, her voice tight, like she was bracing for interrogation. "Alright."

"What was the name of your first pet?"

Another pause. Longer than it should have been. "Mittens."

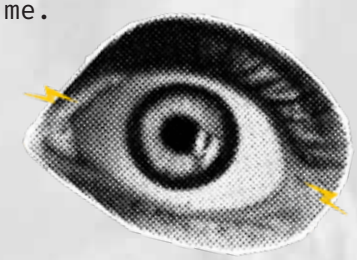
I raised my eyebrow. "That's incorrect. How about the make and model of your first car?"

There was a sharp exhale from the other end of the call. "Honda ..." she started, uncertainty lacing the company name. "Honda ... Accord? Maybe 1983?"

The other eyebrow raised. "That's not right either. What about something easy, like where were you born?"

The answer came through, a question wishing it was a statement.
"... Atlanta?"

I looked over the screen. The security questions and answers that she had set when she created the account stared back at me. Bonnie should know these questions. She had carved them herself into the digital stoneface of our security system.



"You don't know where you were born?" I said, the word PORTLAND glaring at me from the screen.

"Listen ..." she replied, her voice suddenly sad, exhaustion hanging on every word. "I don't know the answer. When I set these questions, I tried to put tricky answers. I know you can find anything you want about anyone. So, I made it up. I thought I would remember the trick answers. But apparently ..." she trailed off.

"But apparently, you don't remember," I said, finishing her thought.

"Yeah," she replied, the word somehow fragile.

I leaned back into my chair and contemplated her excuse. This wasn't protocol. This wasn't how things were supposed to go. Security questions were made to protect people, to help them when all else failed. But Bonnie had turned them into riddles, traps that she had unknowingly set for herself.

"That's ... unusual," I finally replied. "But fake answers to trick hackers is kinda clever too." My fingers hovered over the keyboard. "Things happen. I can go ahead and reset your password to let you back into your account."

She let out a heavy breath, the sound shaky but relieved. "Thank you. I swear, I'm not a hacker. I just ... didn't think I would ever need to answer the questions myself."

"No one ever does," I replied. The security system didn't care if her answers were real or not, it only cared that the answers matched. And they didn't. But her explanation made sense, and her tone felt genuine.

"Your password has been reset," I said. "You will want to reset your password when you log in, and you'll need to update your security questions—preferably with answers you'll remember."

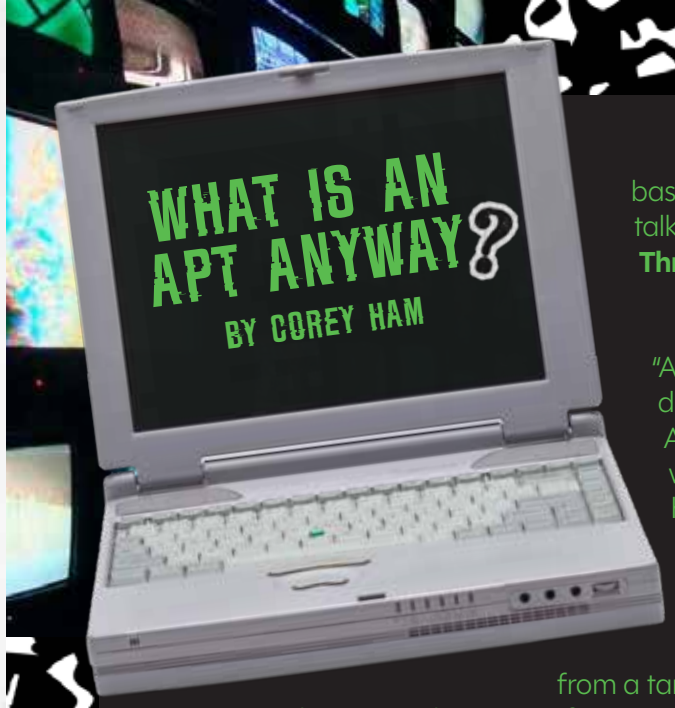
"Yeah, I'll do that," she said, her voice a mix of relief and embarrassment.

The call ended, but the strange feeling didn't.

Bonnie's explanation made sense on the surface, but something about it gnawed at me, like an itch I couldn't scratch. There was something that she hadn't said, or something she didn't know how to say. Or maybe it was me, reading too much into the call.

Still, the unease lingered after the call ended, the chalk outline around the notes I'd made on the account staring back at me. But ultimately, the case was closed. There was no reason to think about it any further ...

Until Monday.





The package manager in Debian-based systems... *Wait, not that APT.* We're talking about the **Advanced Persistent Threat APT.**

Like many cybersecurity terms, "APT" has military origins and its definition has evolved over time. At first, APT referred to hacking groups who were affiliated with nation-states and had objectives that required long-term access to their targets. One common objective for an APT has always been espionage: gathering and exfiltrating sensitive information from a target. The longer they have access to the target, the more information they can collect. This duration of access is called dwell time. While some ransomware groups may have a dwell time of only a few days before malware is deployed and data is encrypted, APTs could have dwell times of months or even years.

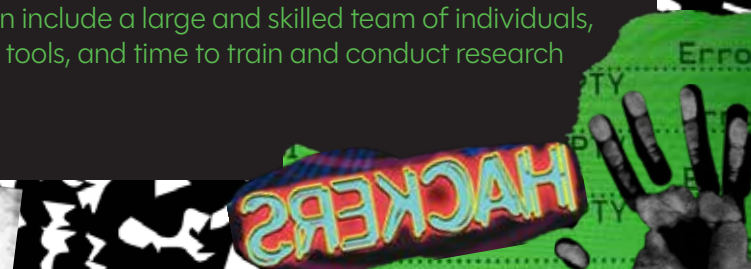
If we're being honest, APT is commonly used in place of "extra scary hackers." But like the term, APT groups themselves have also changed throughout the years. Some groups that were traditionally considered criminal gangs have matured into full-fledged APTs as they expanded their reach and as their attacks became more sophisticated. We have also seen the rise of APTs that are not affiliated with any nation-state, including financially motivated groups, like LockBit and Conti, or groups that have unclear motivations, such as Lapsus$.

Although the term has evolved, there are still clear attributes we can use to classify an APT:

**Sophistication:** This is where we get the "advanced" part. APTs employ a high level of tradecraft across multiple attack types, such as social engineering, malware development, and evasion. They might make mistakes, but they are generally highly skilled operators.

**Persistence:** This is where we get the "persistent" part. APTs have the longest dwell time of all types of hacking groups. Though many of them are now defunct, APTs tend to have more staying power as organizations. Lazarus Group, an APT affiliated with North Korea, has been active since 2009. (That's only one year after BHIS was founded!)

**Resources:** APT groups have more resources at their disposal when compared to other hacking groups. This can include a large and skilled team of individuals, money to purchase commercial tools, and time to train and conduct research on their targets.

# Unmasking the Shadows

## HOW WE IDENTIFY AND EXPLOIT NEW VULNERABILITIES

By Matthew Eidelberg

In the ever-evolving world of cybersecurity, staying ahead of the curve is not just a goal—it's a necessity. As new vulnerabilities emerge, the race to identify and mitigate them begins. But how do we, the guardians of the digital realm, rapidly pinpoint these threats as they become public? **Let's dive into the fascinating world of vulnerability identification and see how the magic happens.**

### PAST LESSONS CAN FUEL NEW IDEAS

Seasoned red teamers know that every engagement leaves behind a trail of lessons. It's not just about pride or curiosity—there's a real operational need to find alternative methods. If you can't stealthily deploy your favorite technique, or if you need a new exploit to bypass a patched vulnerability, you must adapt. By discovering fresh weaknesses or writing custom exploits, red teams gain an edge, ensuring they can continue to test their targets effectively and raise the bar for an organization's defenses. The first stop is often the collective wisdom of the security community. Researching existing vulnerabilities, blog posts, or advisories related to your target technology can help you understand the current landscape and locate opportunities to investigate.

### THE MINDSET: CURIOSITY, TENACITY, AND A BASEMENT FULL OF TOOLS

Many aspiring security professionals who dream of tapping into malware and exploit development envision a hacker hunched over a keyboard in a dimly lit basement, running IDA Pro or Ghidra late into the wee hours of the night. While the caricature might be extreme, it's not that far from reality for dedicated reverse engineers. And yet, it's crucial to emphasize that discovering exploits isn't some unattainable black magic. All it takes is patience, a hefty dose of curiosity, and a willingness to experiment. It really boils down to three things:

PATIENCE: Identifying a vulnerability might mean combing through hundreds of functions or debugging a complex crash scenario dozens of times.

CURIOSITY: You have to want to understand how something works (and breaks) at a deeper level, beyond the obvious functionality.

EXPERIMENTATION: Break things. Step through code. Try weird inputs. You might be surprised at what you discover.

For new red teamers, the biggest hurdle is often psychological. Reverse engineering with tools like IDA Pro, Ghidra, OllyDbg, or Radare2 may seem daunting at first, but there are tons of great resources on the internet that will help you get started. **There are also freely available non-reverse engineering tools such as System Informer, Process Monitor, API Monitor, and more.** Once you know your way around these interfaces and build a methodical process, they become powerful allies in your hunt for exploits.

Don't believe me? Well, during one of our After-Action Reviews (AARs), the conversation came up that our bag of tricks was lacking initial access droppers and persistence. So, I began by studying what was currently being used and what was public. This search clued me in to some of the most recent techniques. I then looked at what was getting us caught.

I started looking at my research virtual machine (which I always recommend you have) and used Process Explorer to examine applications. I then ran Process Monitor over and over again, watching every event and digging into events I was not familiar with. (For example: I noticed a lot of queries to the same area of the registry that were returning different results. Since I did not recognize these calls, I scrutinized them further.)

It sounds tedious, but it works. **This is how I was able to discover several key deficiencies that led to the research that eventually created the tool FaceDancer (https://www.blackhillsinfosec.com/a-different-take-on-dll-hijacking/).**

So, the next time you hit a wall during a red team engagement—be it a failed payload, an uncrackable privilege escalation, or a non-persistent backdoor—remember that this challenge is often the spark that leads to major breakthroughs. Reverse engineering isn't some dark art reserved for a few geniuses in poorly lit basements; it's a practical discipline, grounded in patience, curiosity, and a willingness to learn from each new lead.

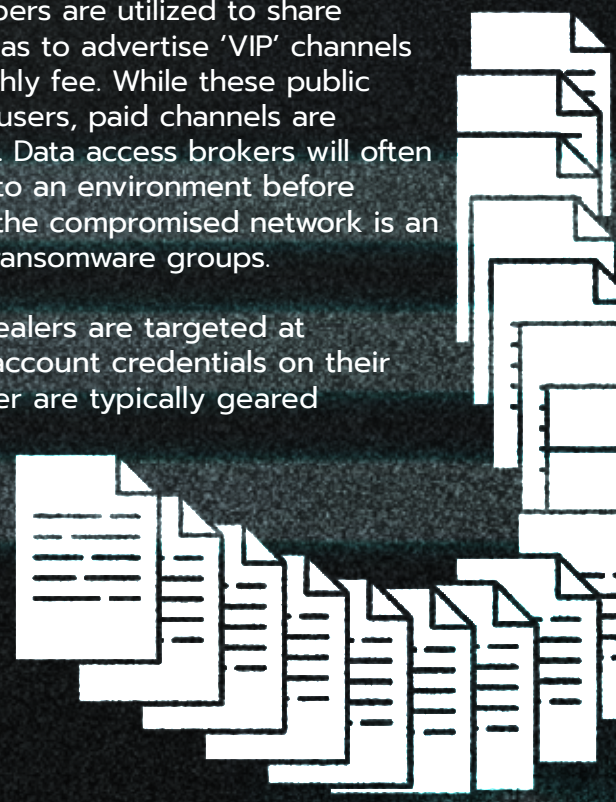
By defining the specific need (the "why?"), conducting thorough research, systematically reverse-engineering potential targets, and rigorously testing new exploits, red teams continually push the envelope. **This is how they help organizations harden their defenses, educate security professionals, and keep the digital world a little bit safer from the threats that lurk around every corner.**


If you still aren't using a password manager in 2025, I have some bad news for you. Infostealers exist, and they are gaining in popularity. While credential theft has always been a threat, initial access through valid accounts grew 71% from 2023 to 2024 (ibm.com/reports/threat-intelligence). If you're unfamiliar with infostealers, you aren't alone. Imagine every username, password, credit card number, autofill form, cookie, clipboard data, wallet file, and more, quietly siphoned from the browsers of your sticker-blasted ThinkPad to a remote C2 server. If that doesn't scare you, the fact that they also capture your browser history might.

Modern infostealers often present themselves as a Malware-as-a-Service (MaaS) package. Redline is a good, common example. A threat actor takes advantage of Redline's subscription model for about 100 bucks a month and then distributes the malware through email, malicious social media ads, and cracked software downloads. Little Timmy downloading free 'Robux' on the family computer is a commonly encountered scenario.

Once the disguised application executes in memory, it begins to package and exfiltrate data from your browsers. More advanced infostealers might automatically check and report on account balances, supply details on Steam account inventories, or provide direct command and control via a Telegram channel. To remain undetected, infostealers employ a range of evasion techniques. Code obfuscation and process injection allow them to blend into legitimate system activities. More advanced variants incorporate sandbox detection or frequent refactors to alter their behavior and avoid analysis by automated security tools.

Once stolen, most of this data ends up being resold. Public Telegram channels with thousands of members are utilized to share massive packages of example logs, as well as to advertise 'VIP' channels where fresher logs are available for a monthly fee. While these public Telegram channels may have thousands of users, paid channels are typically capped at under twenty members. Data access brokers will often use stealer logs to gain their initial access to an environment before selling the access to the highest bidder. If the compromised network is an enterprise environment, it is often sold to ransomware groups.



However, the vast majority of infostealers are targeted at individuals who may have Steam or bank account credentials on their computers. Logs acquired by the infostealer are typically geared toward gaining access to accounts that can be quickly turned for a profit. More concerning is what can be contextualized from what is stolen. The BHIS ANTISOC team and other APTs often use stealer logs for context when social engineering. While gaining access to a credential is helpful, the real value in stealer logs is that they can provide enough context to pose as an employee and often bypass multi-factor authentication.

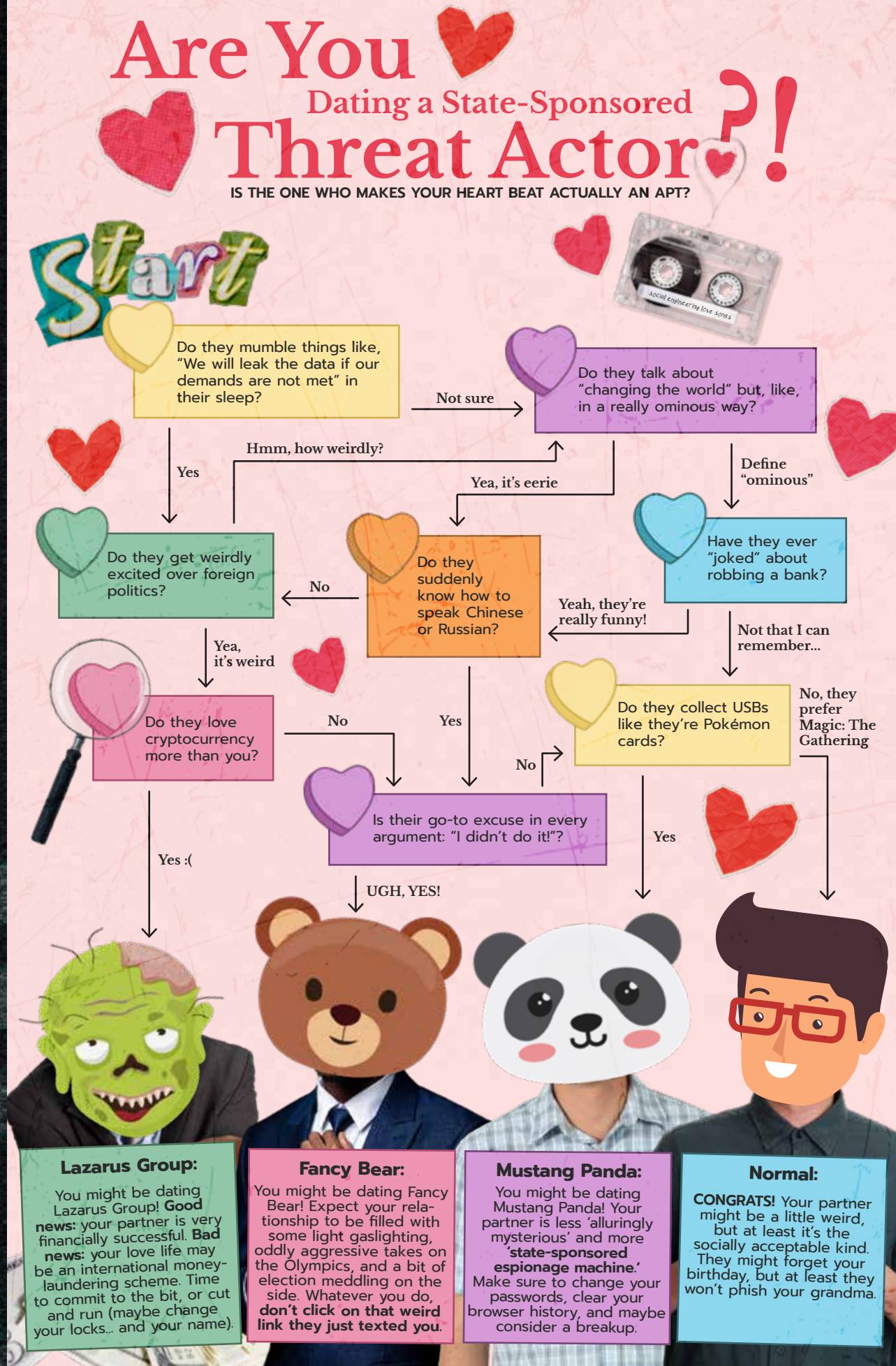
The **BHIS ANTISOC team** will regularly use fresh stealer logs to attempt breaching our corporate clients. By taking advantage of security failures like password reuse or improper MFA controls, BHIS regularly has success utilizing stealer logs to ascertain internal details on a multitude of networks. This allows us to inform our customers of the extent of a compromise and how to effectively remediate the problem. Flare, a threat exposure management company, tracks approximately 400,000 new stealer logs per day–meaning this is a threat to everyone. Losing company credentials is bad enough, but oftentimes, companies will not inform the employees of the source of the breach, leading to repeated breaches when the user signs in at home again.

To avoid blunders like this, there are a few things to focus on when mitigating the risk posed by infostealers. The most effective method we've found is to monitor and remediate the data exposure as we previously mentioned. However, we can also take proactive measures:

- Forcing MFA, while not 100 percent effective, significantly raises the bar for accessing exposed accounts. Logging and parsing your logs to look for unusual behavior, like logins that did not complete secondary authentication, can also be effective for single sign-on portals.
- Keeping an inventory of SaaS (Software-as-a-Service) providers was proven to be a necessary measure during the Snowflake breach. Nowadays, attack surfaces often include external tools or data sources that might not be monitored with the same scrutiny as internal tools.
- Prevent saving passwords into your web browser. They aren't secure or encrypted. Use a dedicated password manager.

While educating users seems like an annoyingly rehashed subject, not many people are aware of the risk posed by infostealers. This class of malware affects end users at a significantly higher rate than corporate accounts.

The rise of infostealers highlights the growing sophistication and accessibility of cybercrime. As these methods are further refined, the volume and intensity of attacks will only increase. Implementing strong authentication practices, monitoring for compromised accounts, and fostering an environment where security is paramount can help organizations mitigate the damages caused by infostealers. Alternatively, just don't share a computer with little Timmy.

# ADVERSARY in The MAILBOX

By Michael "Rhino" Allen

When is it too late for the fly to escape the pitcher plant?
Is it when he lands on the edge?
Or starts to slide down the inside?
Or when he is stuck, unable to escape, at the bottom?
No.
It is when, smelling the nectar inside,
he believes there is something good to be had.

**It's five o'clock.** Quitting time—finally.

It's been a tough week. Even after six months, your newest team member is still more of a burden than a help. And even though you've been working extra hard to meet the deadline for that big project—along with training up the newbie—you doubt your boss has noticed. He's not exactly the "attaboy" type.

**It's six o'clock now.** Finally home.

As you walk in, you grab the mail and flip through the assortment of paper annoyances.

Neighborhood coupon packet, advertisement, bill, bill, bill, and... something from work? It's got the company name and return address printed on it.

"What now?" you sigh as you open it up.

There's a postcard inside. Big, bold letters printed above your company logo read:

**YOU ARE AMAZING**

And there's a photo of a woman smiling. Something from HR?

**ON THE BACK READS:**

**[Your Name],**
It is my pleasure to inform you that a teammate recently nominated you for a peer recognition award:

**ON THE FRONT READS:**

On behalf of our company family, please accept this **$50 Amazon gift card*** as a small token of our appreciation for you and all the hard work you do.

Sincerely,
**Carol Roberts**
**Chief Human Resources Officer**

SEO Your Company Logo

mamazon

*Use your phone to scan the QR code above and sign in with your company email to claim your electronic gift card.

What a surprise! All that hard work hasn't gone unnoticed after all! You wonder who nominated you. Was it your boss? Maybe the new hire?

Excited, appreciated, proud—you sure feel a lot better now than you did leaving the office today!

Elated, you rush inside to share the news... and claim your gift card.

•••••

What you don't know is that your brain has just been emotionally hijacked.

That surprising piece of mail greeting you at the end of your beleaguered day with unexpected praise and a reward all triggered a flood of positive emotions. And that emotional reaction works faster than the logical part of your brain can keep up.

Before you even realize it, you're telling yourself a story:

*i deserved that award.*

*My hard work is paying off.*

*i'm good at my job.*

*My boss finally noticed.*

*My team values me.*

You're looking for the evidence to support the story you want to be true.

The attacker doesn't have to convince you of anything because you're convincing yourself.

Now, your brain is working for the attacker.


•••••

**It's six o'seven.**

Inside, you set down the pile of mail and pull out your phone. Could it really be true? Is there any possibility this is one of those phishing campaigns the company gets every quarter? Or maybe even a real attack?

"No, that's impossible. That stuff happens at work. How could someone targeting my company know my home address? That doesn't make any sense."

"I deserve this reward. I've been working really hard. I'm a valued part of the team. If this were an attack, it might mean that none of that is true."


You push the thoughts away. You don't want to believe it's not real.

You open the camera app on your phone and scan the QR code.

A prompt asks: "Open https://bit.ly/work-rewards in web browser?"

This URL makes sense for a QR code. After all, when you scan the QR code for the menu at the restaurant, it's a Bitly URL too.

You tap OK and watch the company sign-on portal appear in your browser.

In your rush to log in, you accidentally make a typo in the password. And when you submit the typo'ed credential, you get the same error message you always get when you mistype your password. That gives you even more confidence, since a fake website wouldn't know if you typed your password incorrectly or not.

You try again.

Finally, you get the correct password submitted, and you get the usual prompt to accept the multi-factor push notification from the app on your phone.

The notification looks like it always does. The location and the phone model displayed on your screen are exactly correct—same as always—so you tap the button to complete the sign in.

Bing! The code for your Amazon gift card appears on screen. You scribble it on a nearby pad of paper and open the Amazon app. It takes a bit of navigating to find the gift card redemption form in the app (it's always hard to find), but finally you do and enter the code.

**Sure enough, a $50 credit gets added to your Amazon account.**

Well, that settles it. You've seen a lot of empty promises in the quarterly phishing campaigns over the years, but none of them were ever kept. Everyone knows that an attacker isn't really going to give you $50.

You smile and walk off to show everyone the card you got from work, excitedly thinking of things to spend that $50 on.

•••••

What you didn't consider was that $50 was a very small price for the attacker to pay in exchange for access to your company's network. They knew that the $50 gift card would reinforce your belief that the whole scenario was real, so you'd be less likely to report the incident to your company's security team.

And what your security team never considered was that the attacker would strike at your home address. Your company spent thousands of dollars on security software, monitoring services, and penetration tests—all focused exclusively on the company network.

By asking you to scan a QR code, the attacker was certain you'd open the malicious web page on your mobile phone, not your work computer. And by sending the postcard to your home address, the attacker knew that your phone would be connected to the cellular network or your home Wi-Fi, not the well-defended network at your office.

It was a perfect attack: completely bypassing all those thousands of dollars of corporate security by just avoiding it altogether.

•••••

## AFTERWORD

I'm Michael Allen, and in addition to writing this little story, I created the **Adversary-in-the-Middle** campaign you just read about during a red team exercise at BHIS. Since then, my team and I have been perfecting and executing this attack with massive success against highly secured organizations of all types, as part of BHIS's red team and ANTISOC continuous penetration testing offerings.

If you're interested in learning to do this attack yourself (including the high-tech, behind-the-scenes stuff not mentioned in the story), check out my class: **"Red Team Initial Access" at Initial-Access.com/zine.**

Or if you'd like to learn how your organization can defend against unconventional attacks like this one, **reach out to the BHIS team to get started.**

WATCH MICHAEL ALLEN'S WEBCAST ON

**How to Bypass Modern Phishing Detections**

– YUP, THIS IS DEF AN ANTISOC AD –

# ANTISOC MENU

YOUR FRIENDLY NEIGHBORHOOD APT

*Fresh Insights. Reliable Results.*

NEW

## 1ST YEAR EXAMPLE TIMELINE OF ACTIVITIES → CONTINUOUS PENETRATION TESTING

### FIRST QUARTER

**1 ESTABLISH RULES OF ENGAGEMENT**
Define out-of-scope assets or users; establish goals and communication procedures.

**2 BASELINING**
Discover external attack surface, gather OSINT including dark web data exposure. Scan for low-hanging fruit, credential stuffing.

**3 FIRST CAMPAIGN**
Social engineering attacks targeting IT support helpdesk.

**CONTINUOUS SCANNING***
Real-time monitoring for dark web data exposure, combined with weekly vulnerability scans for N-days.

DEBRIEF MEETING

### SECOND QUARTER

**4 SECOND CAMPAIGN**
Assumed compromise starting from previous successes, or customer's choice of another initial access campaign.

DEBRIEF MEETING

### THIRD QUARTER

**5 THIRD CAMPAIGN**
Customer's choice in collaboration with ANTISOC.

**6 RETESTING**
Testers available to retest identified findings on request.

**ON-DEMAND HACKING***
If you can dream it, we can hack it. ANTISOC clients can request ad-hoc testing at any time.
*Note: some limitations apply.*

DEBRIEF MEETING

### FOURTH QUARTER

**7 FOURTH CAMPAIGN**
Customer's choice in collaboration with ANTISOC.

**REAL-WORLD ATTACKS***
Based on news articles or customer requests, ANTISOC seeks to emulate successful attacks against each customer.

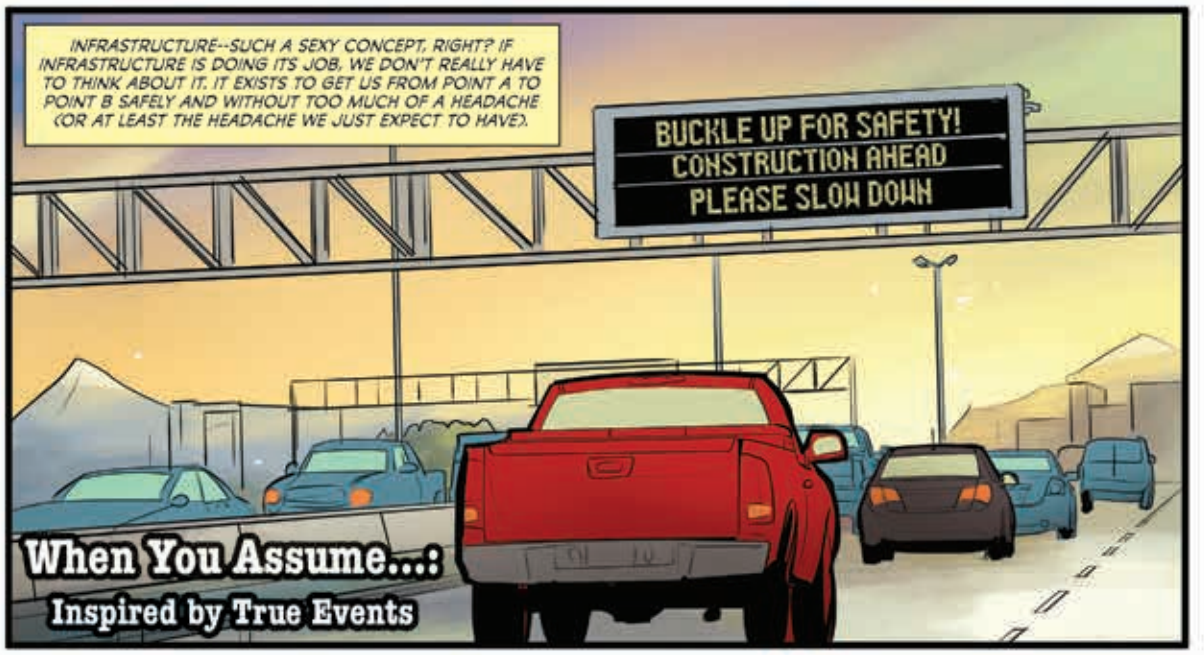
DEBRIEF MEETING

**Tasks happen continuously during their respective quarters.*

*Contact Us Today:* 701-484-BHIS OR CONSULTING@BLACKHILLSINFOSEC.COM

www.blackhillsinfosec.com/services/antisoc/

– YUP, THIS IS DEF AN ANTISOC AD –





MY NAME IS STEVE, AND IT'S MY JOB TO PROTECT AN ENTIRE COASTAL STATE FROM CATASTROPHIC DISASTER.

ALONG WITH MY COLLEAGUE, WHOM I WILL CALL "FRANK," I'M GOING TO PROVE--OR DISPROVE--HOW EASY IT IS TO CAUSE SUCH A DISASTER.

911 RESPONSE CENTER

FRANK AND I ARRIVED AT THE ADDRESS WE WERE GIVEN. AND ALREADY IT WAS CLEAR HOW HIGH THE STAKES WERE TO KEEP THIS KIND OF PLACE PROTECTED. THIS IS WHAT'S CONSIDERED **CRITICAL INFRASTRUCTURE.**

SO, THIS IS OUR CALL CENTER, AS YOU CAN CLEARLY SEE. ABOUT 50 PEOPLE, ALL OF WHOM ARE AT THE BECK AND CALL OF ANYONE WHO NEEDS ASSISTANCE WITH ANYTHING INFRASTRUCTURE RELATED.

BROKEN HIGHWAY SIGN, TRAFFIC LIGHTS, WORK SITES ON THE ROADS--IF IT HAS ANYTHING TO DO WITH MAKING PEOPLE IN VEHICLES MOVE AND THERE'S SOMETHING WRONG WITH IT, WE GET THE CALL RIGHT HERE.

OKAY. SO, PRETTY HIGH PRIORITY.

EXTREMELY. BUT WE'RE NOT TOO WORRIED. THIS SYSTEM IS ***ABSOLUTELY*** UNHACKABLE.

REALLY?

IMPOSSIBLE TO HACK.

A WISE MAN ONCE SAID, "NEVER TELL ME THE ODDS." BUT I LIKE HEARING ODDS LIKE THIS. IT MAKES ME WANT TO BEAT THEM.

NOW WE WOULD DIVIDE AND CONQUER. I WOULD SET UP SHOP HERE AT HQ...

...WHILE FRANK TRIES TO HACK IN FROM THE OUTSIDE.

THIS GUY SEEMED PRETTY CONFIDENT IN THE SECURITY OF THIS PLACE, LIKE HE WAS DARING US TO HACK IN.

DO YOUR WORST!

IT'S FINE TO THINK YOU'RE DOING YOUR BEST TO PROTECT YOUR COMPANY AND ITS EMPLOYEES (TO SAY NOTHING OF THE INTELLECTUAL AND PHYSICAL PROPERTY INSIDE OF ALL OF THAT). BUT WHENEVER SOMEONE GETS COCKY, I IMMEDIATELY BECOME SUSPECT.

I ALSO BECOME CREATIVE.

BUT FIRST THINGS FIRST: FIND A WAY INTO THEIR SYSTEM.

TURNS OUT THAT THIS WAS EASIER THAN EXPECTED. BY EXPLOITING THE BACKUP SERVER--WHICH WAS RUNNING ON AN OUTDATED PROGRAM--I GAINED ROOT ACCESS INCLUDING THE \ETC\SHADOW FILE CONTAINING EVERY PASSWORD IN THE SYSTEM AND SAW RIGHT AWAY THAT THESE WERE SOME PRETTY WEAK PASSWORDS. (FRIENDLY REMINDER THAT PEOPLE WHO KNOW THE IMPORTANCE OF A STRONG PASSWORD CAN SEE YOUR WEAK PASSWORDS. SO, PLEASE, TRY HARDER.)

GETTING INTO THE MAIN SYSTEM REQUIRED A LITTLE DIGGING. OR, MORE ACCURATELY, TUNNELING.

USING REVERSE X11 TUNNELING, I FOUND MY WAY THROUGH ALL THE OTHER COMPUTERS THAT WERE HOOKED UP TO THE MAIN SYSTEM.

WORKSTATION TO WORKSTATION...

...AND BACK THE WAY I CAME...

...BACK TO MY OWN TERMINAL...

...WHICH NOW DISPLAYED THE CONTROL PANEL OF THE MAIN SCREEN. I HAD EVERY SYSTEM AT THE DISPOSAL OF THE TRANSPORTATION HIGHWAY DEPARTMENT'S CALL CENTER AT **MY** DISPOSAL.

SO MUCH FOR "UNHACKABLE."

IN ANOTHER PART OF TOWN, FRANK WAS ALSO ABLE TO HACK IN FROM THE OUTSIDE--WAY TOO EASILY.

EASE OF ACCESS ESTABLISHED, THIS CERTAINLY BEGS THE QUESTION: WHAT WOULD THIS KIND OF ACCESS MEAN IN DIFFERENT HANDS THAN OURS?

SESSION
OPENED^^

NAMELY, HANDS THAT WANT TO CAUSE MASS DESTRUCTION AND CHAOS?

BUCKLE UP
PHONE DOWN

LET'S LET OUR IMAGINATIONS RUN WILD FOR A MOMENT...

PICTURE THIS: INSTEAD OF ME AND FRANK COMING HERE IN THE NAME OF SECURITY AND SAFETY...

...WE'RE HERE TO CAUSE SOME DAMAGE. SERIOUS DAMAGE. **CATASTROPHIC** DAMAGE.

WE HAVE CONTROL OF EVERY SIGN...

ROAD SIGNS
ROAD SIGNS
ROAD SIGNS

...EVERY LIGHT...

...EVEN MECHANIZED PIECES OF THE ROAD LIKE THIS...

...ALL OF WHICH I CAN MANIPULATE WITH A FEW SIMPLE KEYSTROKES IN A MATTER OF **SECONDS.**

'PYTHON SENDDASHBOARDMESSAGE^P
'MESSAGE "INCOMING TSUNAMI"

I CAN PUT ANY TEXT I WANT INTO THIS HIGHWAY SIGN.

COASTAL FLOODING WATCH
EVACUATE IMMEDIATELY

I CAN ALSO SHUT DOWN ALL THESE TRAFFIC SIGNALS.

BUT MAYBE ONE OF THE MOST TERRORIZING THINGS I CAN DO IS SHUT DOWN THIS WHOLE CALL CENTER WHILE ALL OF THIS IS GOING ON.

IF ALL OF THAT WASN'T ENOUGH. THERE'S ALL THE OTHER STUFF THAT FRANK AND I FOUND WHILE WE POPPED THIS CRITICAL INFRASTRUCTURE.

WE COULD SEE EVERY TEXT MESSAGE COMING IN AND OUT OF THIS CELL TOWER.

Does your wife know?

Don't tell your boyfriend

Can you even do that in the Capitol?

I wanna get my hands all over...

...your mouth...

What does it mean if it's swollen?

I'm scared to go home

I think that's against the law but ok

WE NOT ONLY HAD CONTROL OF WHERE PEOPLE WERE GOING, WE KNEW WHAT THEY WERE SAYING AND DOING.

IF FRANK AND I HAD SUDDENLY DECIDED TO BECOME CYBERTERRORISTS AND CAUSE A PANIC, WE COULD HAVE DONE IT SO EASILY.

WE COULD JUST SEND A MESSAGE TO THE MEDIA TO INFORM THEM THAT **WE** CONTROL THE HIGHWAY DEPARTMENT NOW, AND IF THEY DON'T COMPLY WITH OUR DEMANDS, WE HAVE **ALLLLLLL** THOSE TEXTS.

WE WOULDN'T EVEN HAVE TO DO THAT OURSELVES. THERE'S DEFINITELY SOMEONE ELSE OUT THERE WITH NEFARIOUS INTENTIONS. READY TO BUY THAT KIND OF INFORMATION.

BUT THAT'S EXACTLY WHY FRANK AND I ARE HERE–TO STOP SOMEONE LIKE THAT FROM CAUSING ALL THAT TROUBLE.

TO WARN A PLACE OF SUCH CRITICAL IMPORTANCE THAT THEY NEED TO PROTECT THEMSELVES BETTER.

BUT THAT DOESN'T MEAN I CAN'T HAVE A LITTLE FUN WHILE I WARN THEM.

HEY, I'M DONE WITH YOUR ASSESSMENT! YOU READY TO CHAT?

SURE THING!

SO, ARE YOU READY TO DECLARE US THE FORT KNOX OF STATE HIGHWAY DEPARTMENTS?

Ummmm...

I EXPLAINED EXACTLY HOW EASY IT WAS TO HACK INTO HIS SYSTEM AND MANIPULATE EVERY WIRED INSTRUMENT CONNECTED TO THE SYSTEM. WHAT HE'S LOOKING AT IS A SCREENSHOT OF A HIGHWAY SIGN THAT I CHANGED.

TEST

WHAT DID YOU THINK I'D PUT THERE? "VOLCANO"? I MEAN, I COULD HAVE...

AFTER HE SWALLOWED HIS PRIDE, I OFFERED UP SOME SOLUTIONS FOR BETTER SECURING HIS SYSTEMS.

I ALSO TOLD HIM TO CHECK IN ON THAT SYSTEM JUST TO MAKE SURE NO ONE CAN BREAK INTO IT IN THE FUTURE.

RUN ANOTHER PEN TEST. CHANGE YOUR PASSWORDS EVERY COUPLE OF MONTHS. UPDATE YOUR SOFTWARE REGULARLY.

MAKE THE INVESTMENTS IN THE NAME OF PROTECTING THE PEOPLE LIVING IN THIS STATE.

AND NEVER–**NEVER**–ASSUME YOU'RE COMPLETELY UNHACKABLE. THAT'S JUST ASKING FOR TROUBLE.


ORIGINAL STORY: Steve Borosh
WRITER: Jamie Frevele
ARTIST: Joe Eisma
COLORIST: Shari Chankhamma
LETTERER: Taylor Esposito
EDITOR: Kassie Kimball


THE END

# MAD HACKING

## A Fun Word Game!

To play this game, you need a leader and a player. Without showing the player the story, the leader asks the player for words (as categorized under the spaces) to fill in the blanks. Once all the blanks are filled, the story is read out loud, resulting in hilarious nonsense. The game can be replayed endlessly with different players taking turns. Happy hacking!

This is the story of when the _____ APT group known as
(ADJECTIVE ENDING IN -OUS)

_____ _____ decided to infiltrate a highly
(ADJECTIVE OR NOUN) (ANIMAL)

_____ government server. Their leader, _____ _____,
(ADJECTIVE) (U.S. STATE) (FIRST NAME)

who was known for having the best _____ in the business,
(PLURAL NOUN)

gathered the team of _____ for the mission. Everything
(PLURAL JOB TITLE)

was going well until they hit a _____ firewall.
(ADJECTIVE ENDING IN -ING)

"_____!" said the team's resident _____.
(UNHAPPY INTERJECTION) (PROFESSION)

After a long battle, they finally used a trick up their sleeve

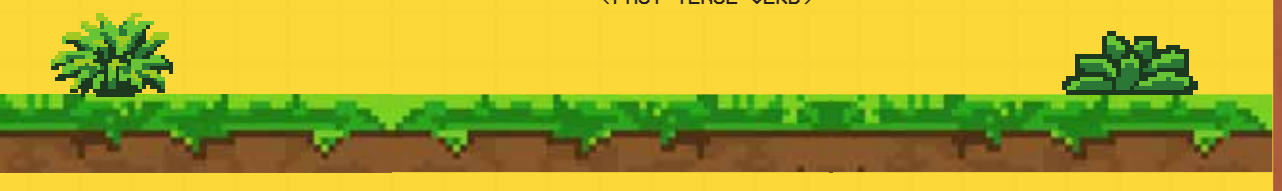
called the _____ to find a weakness in the system:
(SILLY MADE-UP PHRASE)

_____ _____. They couldn't believe their
(ADJECTIVE) (PLURAL NOUN RELATED TO COMPUTERS)

eyes when they uncovered pictures of _____ instead
(SILLY PLURAL NOUN)

of the _____ data they were looking for. "FOILED
(ADJECTIVE ENDING IN -Y)

AGAIN!" they shouted as they _____ off into the sunset.
(PAST-TENSE VERB)



# CREDITS

CHECK OUT OUR PAST ZINES:

## OUR COLLABORATORS, THE ANTISCOC TEAM AT BHIS:

**COREY HAM**
linkedin.com/in/coreyham/

**CAMERON CARTIER**
@__pen__ linkedin.com/in/hippi3hack3r/

**ALICE MURPHY**

**KAITLYN WIMBERLEY**

**MICHAEL "RHINO" ALLEN**
@Wh1t3Rh1n0

**ZANE PRALL**
linkedin.com/in/zaneprall/

**MATTHEW EIDELBERG**
@Ty10us linkedin.com/in/matthew-eidelberg

CREATIVE CONTENT AND COMMUNITY TEAM

**PUBLISHER** JOHN STRAND
@strandjs.bsky.social

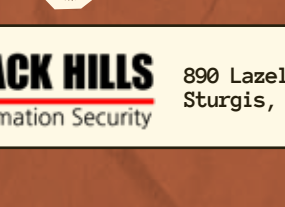
**EDITOR-IN-CHIEF** JASON BLANCHARD
linkedin.com/in/jasonsblanchard

**GRAPHIC DESIGNER & PRODUCTION** DANI DIEM
danielledcosta.com

**EDITOR** KASSIE KIMBALL
linkedin.com/in/kassiekimball

**ASSOCIATE EDITOR** MELISSA LAURO
linkedin.com/in/melissarsl

**PROOFREADER & MORALE OFFICER** DEB WIGLEY
linkedin.com/in/deborahwigley/




BLACK HILLS Information Security
890 Lazelle Street
Sturgis, SD 57785

Contact Us: 701-484-BHIS or consulting@blackhillsinfosec.com
PRINTED IN CANADA. STICKERS PRINTED IN USA.

ANTISYPHON TRAINING

POWERED BY BHIS

# WANTED

## NEW STUDENTS

### FUELED WITH A DEFIANT URGE TO MAKE THE WORLD A BETTER PLACE

**NO SKILLS NECESSARY**

ONLY A COMPUTER IS NEEDED!

# APPLY WITHIN


Learn More

ANTISYPHONTRAINING.COM