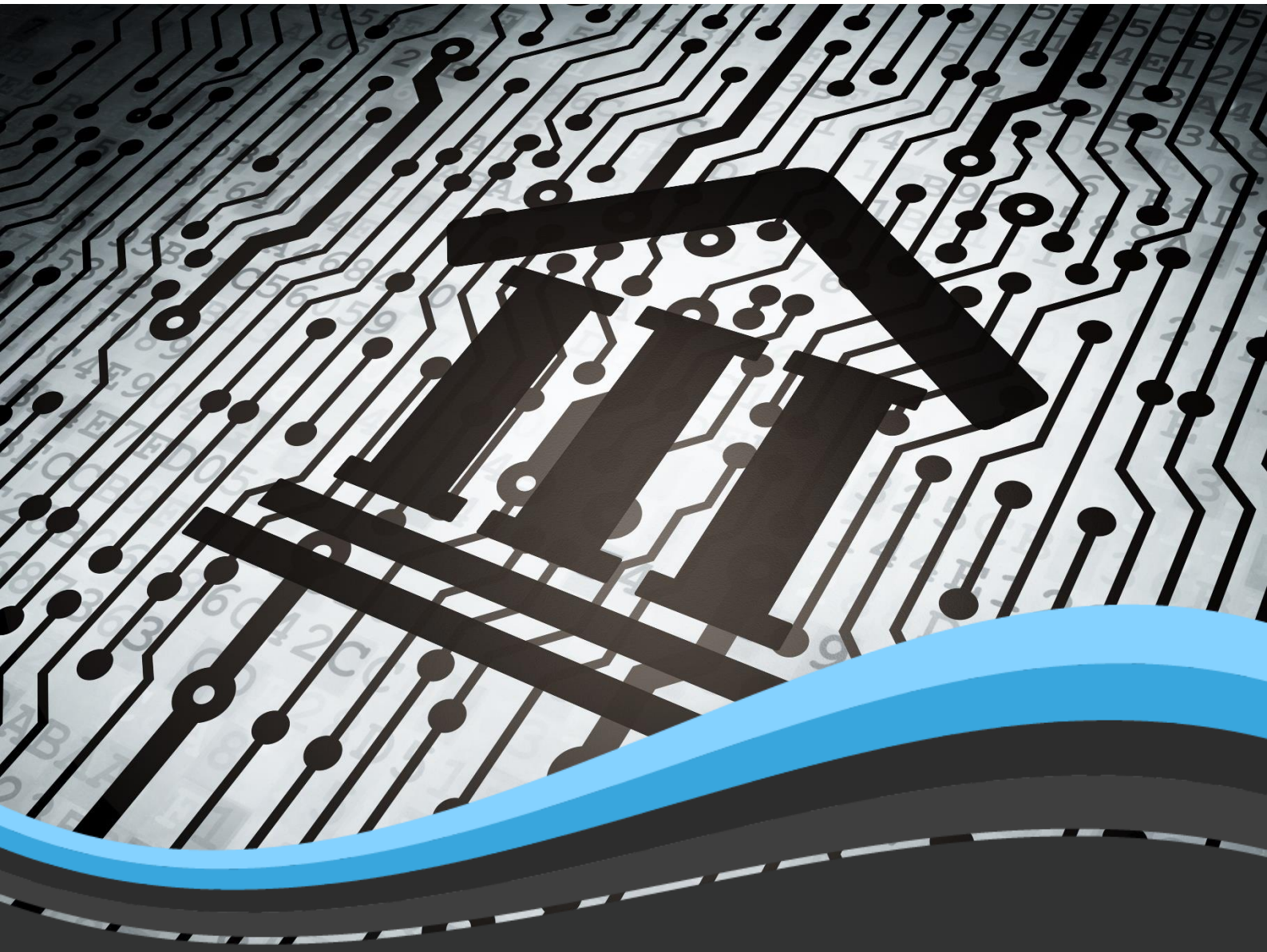
7 Ways Hackers Look to Exploit Federal Agencies



CORE SECURITY

Contents

Bad actors primary focus is to obtain the sensitive and secure data you hold within your organization. For you who work in a federal organization, know that you are often a high target of attackers to obtain access to your environment. You certainly harvest Whether you work for the Department of Defense, Department of Energy or anywhere in between you are collecting data that is critical to not only your job – but for all of the organizations and people that work and live or operate within these borders. You are just as much a target for a cyberattack as anyone so what are you doing to avoid being the next victim?

Today we are going through seven ways hackers are looking to get into state and local government networks.

#1

Human Error

We cannot automate everything to be done perfectly so, unfortunately, human error comes into play. When working at a company you are given devices and access to different parts of the organization depending on the actual job itself. In an office, there is a certain level of trust amongst employees that's established such as not eating a coworker's lunch in the fridge or taking items from their desk. The same goes for accessing information on your company's fileshare or office network.

Maybe you have been granted access to things you don't normally use or need – but that's exactly what hackers are looking for and how they dig their way into the sensitive information. If you aren't safeguarding your logins, using a secure login or connecting from your home network using a VPN you are putting not just your information at risk but dozens of other's at well.

Complacency is a threat in a work environment. After a while, people tend to get lax in protocols or rules and slip up when it comes to securing that data you've collected. This is a reminder to all businesses and government agencies to continue to host security awareness training – no matter how many grievances you hear, the reminders and trainings will keep security top of mind much better than if no one were talking about them.

#2:

Your Password

This may be something that you hear all the time or may seem obvious—but that means it's just that important. Routinely changing your password, and avoiding the simple one of "Password123" really does make a difference.

Not only that, but having different passwords for each of your accounts is just as important. If a bad actor figures out your one password, why wouldn't they test it against all of the other access points you have to the sensitive data you can reach? Don't have one key for all of the doors you can open. Instead have many passwords, change them routinely and don't use information that can be easily found through a search online.

#3:

Application and Software Bugs

There are various applications and software solutions that you need to use on a day-to-day basis. This could be a program that is downloaded to your hard drive or that you access via the cloud or internet. Oftentimes, bad actors already know the weak points that exist within these programs– especially in software that has been around for decades that is constantly releasing software patches or updates to the latest versions.

However, knowing that you have to use certain tools and resources to get things done, are you also aware that bad actors are attacking those same tools and trying to get into your sensitive data? It's vital to continuously monitor and apply the software patches to your programs and ensure your virus protection is in place – but know and understand that that can't be your only line of defense.

#4:

Phishing Attacks

Another way that bad actors are looking to get in is through placing malware on your network through a phishing attack. There are different phishing attacks that you may have heard of such as spear phishing or whale phishing – though it all boils down to bad actors contacting your employees and tricking them into clicking, downloading or performing an action that will lead them to getting access to your network.

Did you hear about last year's attack on the Ukraine that resulted in a blackout during the coldest part of winter? That was a confirmed phishing attack. The series of events was as follows: an engineer on duty received an email that resembled one from his colleague with an excel file – not realizing that the email was actually from a spoofed email account. The engineer then opened the file and saved it to his computer in order to edit and return it. And that was all it took.

It really is as easy as downloading a file that looks like it's from a coworker or clicking on a link that you think your friend sent you. The best way to protect against phishing attacks is to train your staff to be weary of any and all communication they receive and to test their awareness consistently.

#5:

Social Engineering Attacks

Facebook and Twitter are great for keeping in touch with friends, catching up on news and sharing funny memes. However, they are also a trove of information for bad actors looking to engineer their way into your network. Stolen credentials are one of the most common ways that your networks are compromised and they are often stolen through social engineering attacks.

But how do they do this? When you set up your company profile, you may be asked questions in order to reset your password such as, “What year did you graduate?” or, “What’s your mother’s maiden name?” While these answers seem like genuine questions to ask in order to verify your identity, what you don’t realize is that someone else can also get that information from your social profiles.

An easy way to combat this easy entry point for bad actors is to ensure your password reset options are more than generic questions easily found on the internet. You should institute multi-factor authentication for all password resets which relies on more than a question and answer but requires a one-time passcode or biometric authentication that only the appropriate users will have.

#6:

DDoS Attacks

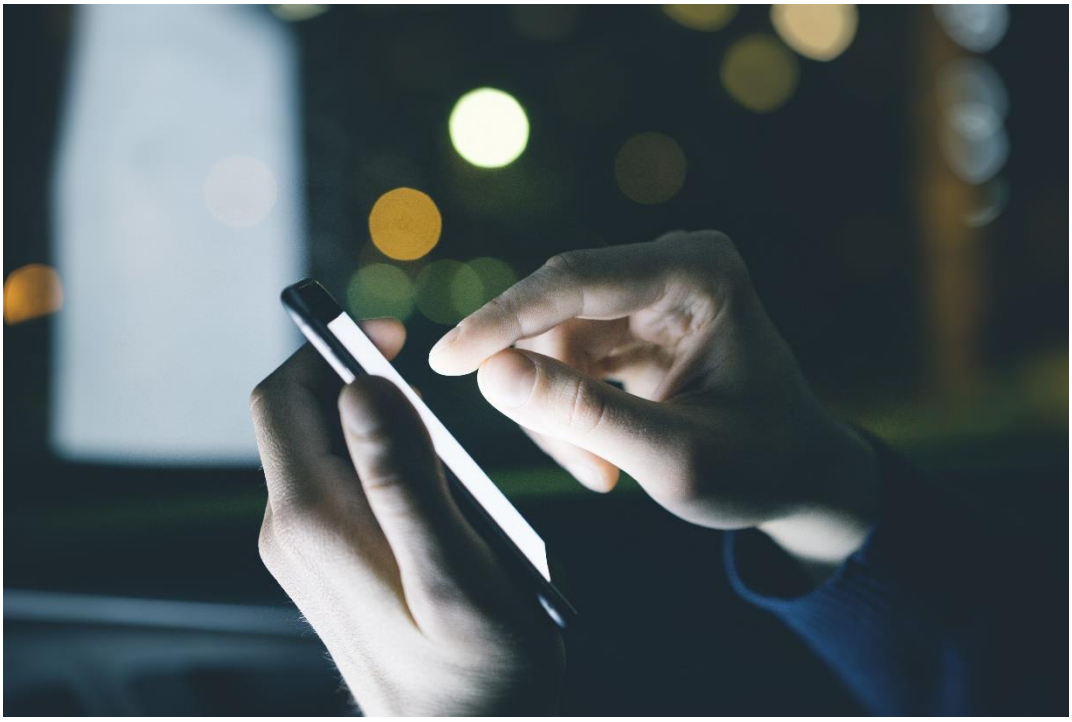
You may have heard of the Dyn attack a few months ago that seemingly took out the Internet as we know it for a few hours. These probing attacks are designed to evaluate the amount and duration of stress required to “knock over” critical pieces of infrastructure that we rely on in our intensely connected world.

The problem is multifaceted – but one of the main drivers for this attack is that we have so many embedded devices on our networks that are often overlooked from a security perspective and this is a fact that our adversaries are taking advantage of. While this may not be something that we can ever completely avoid, there are things we can be doing to make it more difficult for them to try and enter. Being able to quickly detect compromises on the network and understanding the attack path to the critical assets can help you prioritize the vulnerabilities to fix and quickly take action on the right resources before something bad happens. The best defense here is a good offense by knowing where you are vulnerable to these type of attacks and knowing where to patch and protect before the attacks start.

#7:

Your Personal Devices

Oftentimes we get so excited about the latest releases of phones, tablets and computers that we don't think about how to protect them and their longevity. No this doesn't mean buying insurance from breaking them but to ensure we have the right lines of defense implemented on our devices or know how to properly access the different networks we need to on any given day.



Though, there are some actions you can take to make it more difficult for bad actors to come onto your network. Making the switch on your devices from automatically connecting to your home or work network to logging in each time may be a good starting point. Yes, it's easy and convenient for you to automatically connect or search for open WiFi locations but that is incredibly dangerous for your device and the future networks you connect to. Attackers may create fake WiFi connections or implement "Man in the Middle" attacks which obtains your password information for your device.

At the end of the day, we know that attackers are out there and that breaches will happen. Knowing that the bad actors out there are one step away from reaching your sensitive data, you should be well versed on what you can do to protect your government agency and the communities you are serving. Having a strong understanding of what your current IT environment looks like and what vulnerabilities are high priorities for your organization and are great places to start.

Are you ready? For more information on how to get started, contact one of our security consultants about our variety of vulnerability management and network threat detection solutions or our Security Consulting Services. For more information, visit www.coresecurity.com.