

## Checking for compromise

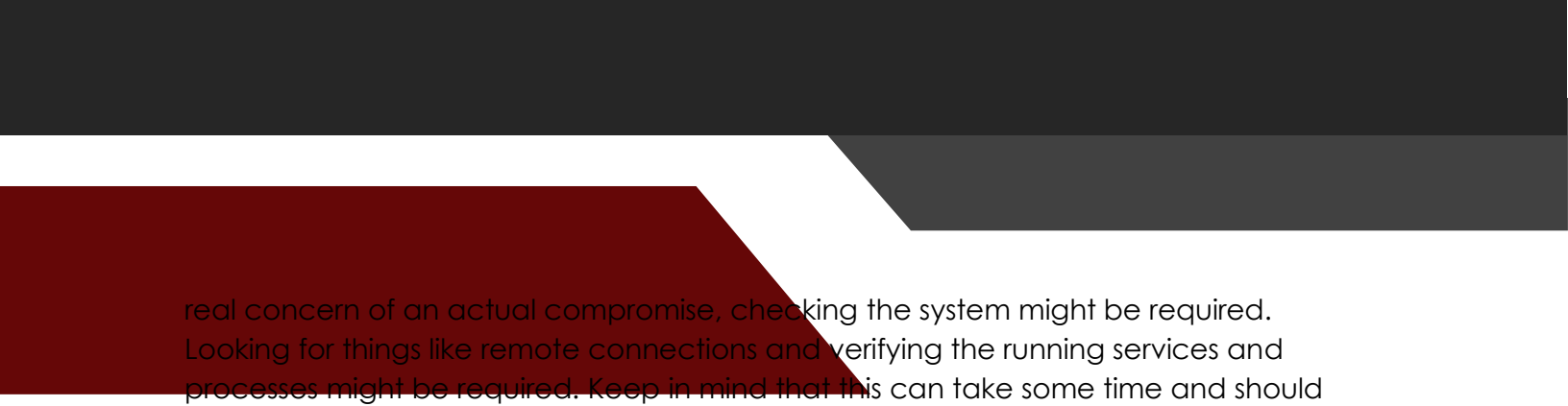
In this week's session I wanted to take a moment to focus on a specific topic as this is how many attacks will begin. Let's take a moment to talk about Phishing and all variations in this family of attack types. While many of you know what a phishing email looks like and while security to help prevent this may be in place, the rate of success is still greater than none. Although one email or phone call may be caught and the attack prevented, join me with the journey through investigating the one that may have gotten through, at least partially.

Many of the phishing emails will include something that requires user interaction to deliver the malicious payload, like a link or an attachment, where do we start when the payload has potentially been launched. Asking the questions is always the best first step to understanding the scope of the attack, however, it is important to remember that you may not get the full answer. Let's begin with the first steps for determining the scope and mitigation that needs to be performed.

Of course, the first step is to determine the system that is in use. Where is the exchange hosted? Is this a domain user or is it running on a local account? Knowing the answer to these helps determine where to begin the search. The absolute first steps should always be to try and mitigate any impact and the first steps should be to reset any passwords. It is also important to check to see if MFA is enabled on this account. While having an MFA does not mean that it is impossible to get into an account, it is good to understand that this brings down the likelihood the account is compromised.

Next, is making sure that the machine has not been infected with any malicious software. Using the Antivirus is always a good mitigation but please understand that this is not a protect all. There are other attack vectors that either the signature is not currently known by the AV or using native applications to run malicious executions.

Once the mitigation part has been taken care of, understanding if there has been any activity will ensure the due diligence into the attack is performed. Verifying the sign in logs for the account is a good first step. Checking things like the IP of the login location is a good indicator if there has been any out of the ordinary log in attempts. If there is a



real concern of an actual compromise, checking the system might be required. Looking for things like remote connections and verifying the running services and processes might be required. Keep in mind that this can take some time and should only be performed if there is a real concern. In the investigation process it is also important to fully document the findings. You may also need to capture an image of the system in order to preserve the evidence.

Knowing when to escalate an issue is extremely important. The findings of indicators is a great first step but knowing when those indicators can lead to a more serious incident is equally important. An infection or account compromise can expand exponentially if an attacker is able to gain a foot hold and escalate privileges. While most issues are mitigated and just documenting the findings may be enough, if the incident results in a breach of the network the evidence collected will be required for the report. This may mean the report is going to an insurance company or in the case of a publicly held company, for the SEC filing.

Catching and mitigating as quickly as possible is always the intent and hopes for any incident. Preventing a small single user accident from becoming a full-blown breach is only possible when the end user has been properly trained on how to handle these types of attacks. Making sure that you handle these appropriately and knowing when it is appropriate to educate the end user helps to ensure that there is a emphasis on staying vigilant at all times.

