**Credential Theft**

With the continuous onslaught of phishing attacks and other forms of social engineering the reality will be that eventually an organization will encounter the successful theft of a set of credentials that could be used to gain access to its systems. This scenario aims to help healthcare organizations think about the various ways that credentials could be stolen, how they can identify the use of stolen credentials, and what they can do to mitigate the damage that could result from stolen credentials being used to access organizational resources.

# **Start of the Scenario:**

After a long day at work a doctor comes home and upon sitting down at his personal computer checks his email. He sees an interesting link to a funny video purporting to be from an old college buddy. He clicks the link a few times in frustration as no video seems to load before giving up. Little does he realize that his user account on his home PC is an administrator level one and that machine, that has not been updated in months, is now infected with a key logger. The next morning before heading into work, the doctor decides to quickly log into the hospital’s Webmail system to check on any items that might need his attention that day. As part of the simple act of logging in, the attacker that planted the key logger now has access to his hospital username and password. Within a few hours, other hospital employees begin to get emails from the doctors now compromised account asking them to sign in to view an encrypted message from him.

## **Questions to consider:**

1. Are there any in place controls within your organization that may have detected the attackers use of the credentials?
	1. Does the geographic area the credentials were used from have any bearing on this?
2. Are there any mechanisms in place to detect the malicious emails to other users or would traditional detection mechanisms be bypassed because the emails are originating from an internal source?
3. Is Multi-Factor Authentication (MFA) in use at your hospital? How would MFA impact this scenario? What about Mobile Device Management (MDM) controls?
4. Are there any policies that cover accessing hospital resources on personal devices?
5. Are there any mechanisms in place for ensuring the security of personal devices used to access hospital resources? Would these mechanisms have detected the compromised device?
6. To support further investigation, are policies in place for the permission to obtain personal devices that may have been compromised to derive forensics? Are they part of the employment agreement or other “acceptable use”policy?

# **Inject 1:**

About an hour after emails were sent from this doctor’s account the help desk starts to get calls that users need assistance accessing the encrypted email sent to them from this doctor. They are complaining that they are entering their username and password as instructed by the login page but that the message never shows. At this point it is clear that more than one hospital account may be compromised.

## **Questions to consider:**

1. Is there sufficient in place logging and a mechanism to search through these logs to identify who within the organization the malicious email went to?
2. What actions should be taken to neutralize the threat of the malicious email for any who have not yet viewed it (e.g. blocking the malicious link)?
3. Do sufficient logs exist to identify who clicked on the malicious link and as a result now also have their credentials compromised? Does a mechanism exist to search these logs?
4. What actions should be taken to mitigate the threat of these additional compromised credentials?
5. Should credential use against any other systems be checked into? Does adequate logging and a method to search such logs exist?
6. Would a SIEM platform be beneficial to addressing these issues?
7. How can users who may be checking their email from home or an offsite location be protected from the malicious email?

# **Inject 2:**

After taking steps to neutralize the threat, hospital IT and IS continue to monitor the situation and to analyze the logs of any system they feel may have been at risk. As part of this process, they notice that the accounts of several of the users that tried to access the malicious encrypted message were used to try to establish SSLVPN access to the hospital.

**Questions to consider:**

1. What should be done to mitigate this threat?
2. What should be done to determine what was accessed if anything? Do sufficient logs exist?
3. Does law enforcement need to be contacted? Does it depend on what was accessed?
4. Have VPN rules been audited to ensure that a least privilege setup is actually in place?
5. What controls could be put in place to reduce the likelihood of malicious SSLVPN usage going forward?
6. What controls could be put in place to identify such attacks against the SSLVPN system sooner?