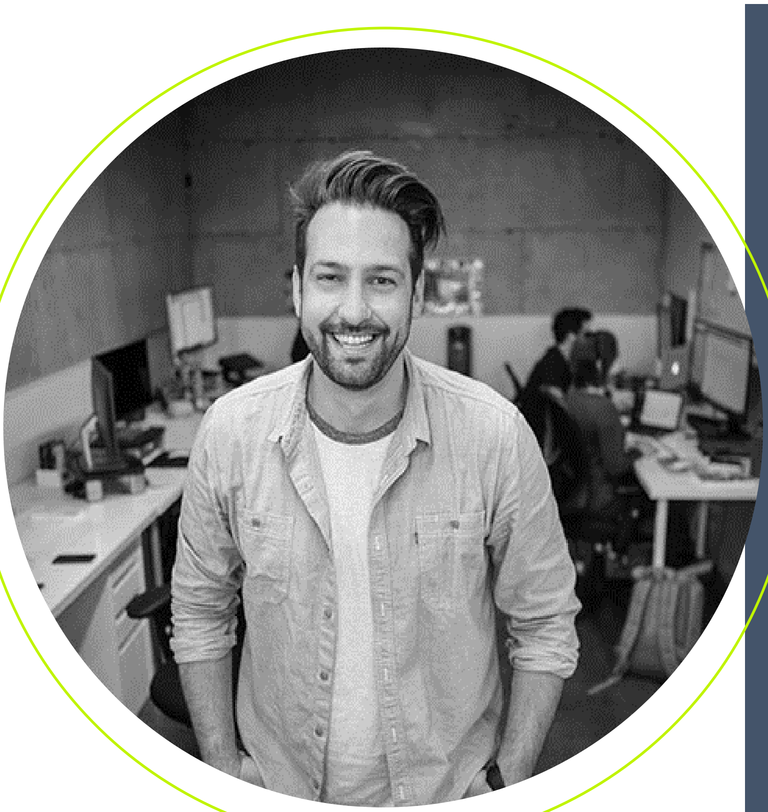
ROBO6K

CYBER SECURITY

IN THIS ISSUE



A LOOK INTO THE ATTACK

Security researchers have identified this as a widespread attack. The first indicator of the compromise will be an email alert that a new email address, many times with the @rambler.ru domain, has been added to the account. Once the threat actor is able to add the new email address to the account, they will reset the password which results in the loss of access to the account. With the new email added and the password changed, it now becomes next to impossible to recover the account. Search terms related to the attack have now been labeled as a "breakout" which means that the search terms have surged 5000%.

LINKEDIN ATTACK

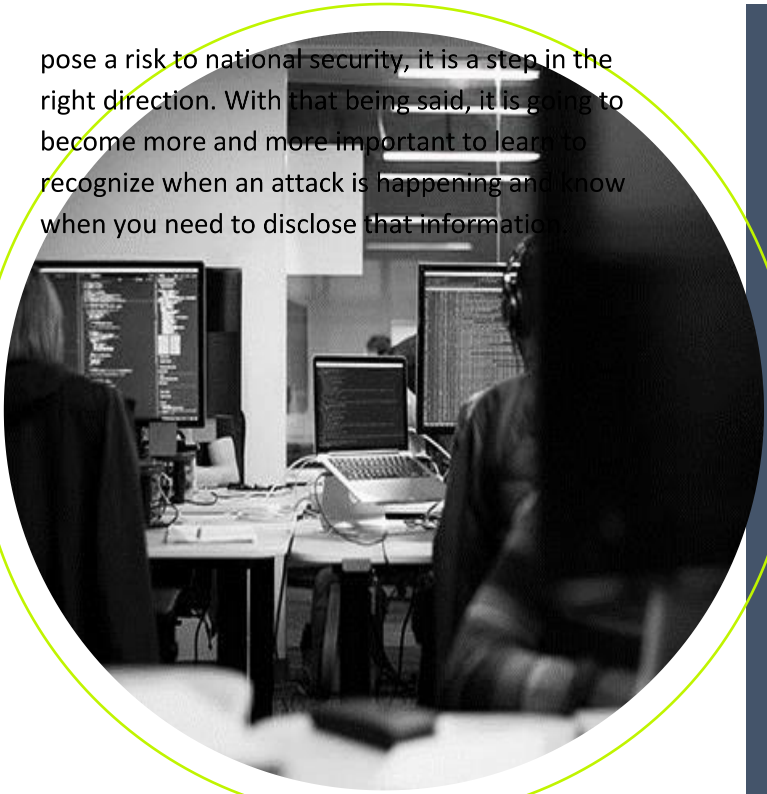
While this one may not seem as important or result in direct financial loss, it is important to remember that even your personal information is under attack. With threat actors targeting your personal LinkedIn account to take it over and, in some cases, demanding a ransom payment to get the account back it is important to remember that man attackers are going to pick targets of opportunity. What this means to you, the end user is that doing the little things, like enabling MFA on the account could help you avoid the potential take-over of your personal information.

NEW SEC RULE

With the need for regulation regarding cyber events in the forefront of many politicians, a new rule released by the SEC now requires companies to disclose the event within 4 days of determining a "material" impact to the company. This is important as it is a strive to gain more transparency to stake holders and the public when an attack causes financial loss. While there is a stipulation that allows companies to extend that by 60 days if it is determined that releasing the information would

"A lack of transparancy results in distrust and a deep sense of insecurity"-Dalai Lama

pose a risk to national security, it is a step in the right direction. With that being said, it is going to become more and more important to learn to recognize when an attack is happening and know when you need to disclose that information.



ELEVATED PRIVILEGE

While privilege escalation is nothing new, a new stealthy technique has been found that allows attackers to escalate privileges within the windows environment. NoFilter, a tool released by security researchers allows the attacker to escalate from user to system which is the highest level in Windows. It uses the WFP, windows filtering platform, a set of APIs to modify network data. By duplicating the token that is sent out, NoFilter allows attackers to escalate to the system privilege. While there is currently now patch to prevent this vulnerability, Deep Instinct has graciously provided a few detection methods to help give you at least some defense against these attacks.

- Configuring new IPSec policies that don't match the known network configuration.
- RPC calls to Spooler / OneSyncSvc while an IPSec policy is active.
- Brute force the LUID of a token via multiple calls to WfpAleQueryTokenById.
- Device IO request to the device WfpAle by processes other than the BFE service.

For a deeper technical review, please refer to Deep Instincts post on the matter.

IN CONCLUSION

While the world of cyber security is an ever changing landscape, it is important to remember that it will take everyone working together to help minimize an attack. As we see in the past couple of weeks that attackers not only target businesses but will go after the less profitable personal data as well.

Caleb Leggett
Account Support

T: 512-501-1223 |
cleggett@robo.net - www.robo.net
2600 S. 1st St, Suite 100.
Austin, TX, 78704