COCC White Paper

Preparing For Increasing Russian Cyber Threats

By Jamie Perry, FVP – Chief Security Officer

It has been slightly over one month since Russia invaded Ukraine with no immediate resolution in sight. As a member of the Armed Forces, this is the first time I personally have witnessed an act of war involving traditional military warfare and the threat of cyber warfare made directly by the President of Russia. Never before have we seen news reports on military conflict also include a discussion of cyber preparedness specifically directed at the Critical Infrastructure Sector. Compounding this threat is the increasing pace at which cyber-attacks occur. As a result of this new and expanded threat landscape, most of us faced a challenging year renewing our cyber insurance policies as insurers have to pay claims at an increasing rate.

The Landscape Threat

Nation-state threat actors are nothing new. These threat actors have the funding and support of their country to unleash attacks against other nations at a low cost, most notably for cyber espionage but also to destroy, disrupt and threaten the delivery of essential services.

The Cybersecurity and Infrastructure Security Agency (CISA) website lists four current nation-state cyber threats: Russia, China, North Korea and Iran. For detailed information on the Russian threats, learn more here.

As the news coverage continues to surround possible attacks, C-suite Executives and Boards are now finding themselves actively engaged in asking the question, “What should we do to prepare?”. While the answer isn’t as easy as flipping a switch, these events are what mature security programs are designed to mitigate. Unfortunately, in this day and age it isn’t a matter of “if” but a matter of “when” an organization will find itself in a situation where it must defend itself against a threat. For most organizations, this is already happening on a smaller scale. More than likely your users are receiving phishing e-mails designed to steal passwords or potentially download malicious software. However, due to security awareness training and security tools that are in place to prevent software from installing, this low-level type of attack often goes unnoticed at the C-suite. What makes nation-states such a threat is their advanced persistent nature. These attackers are highly sophisticated with vast resources behind them and will often keep working until they reach their objective.

In the case of Russia, their objective is disruption. So now you are saying to yourself, “How can I protect my organization against these threats that have a nation behind them?”

Protecting Your Institution

Attackers tend to have an M.O. for their operations. Like a typical crime, we can use these known techniques as a way to mitigate them. While some have very specific techniques, the majority of protections involve a solid, tested security program based on industry-accepted standards.

- Multifactor authentication has been a buzzword in the security space for a while. However, requiring a token in addition to a password can make the difference between an attacker successfully compromising an account. A simple attack that continues to be seen is compromising a Microsoft Office 365 account that does not require multifactor when used outside the organization. There is a treasure trove of information in people's e-mail. Recently many insurance companies have started to require multifactor authentication for critical accounts as a requirement for coverage.

- Performing security patching may seem like an unimportant, mundane task. However, the vulnerabilities can expose a window big enough to gain a foothold into your environment to cause damage. Measuring and reporting on your patching progress to close these windows should be a high priority. In conjunction with an effective patching program, you can employ vulnerability scanning or penetration testing to identify where these vulnerabilities actually reside. This gives a view of the weaknesses attackers can target.

- Minimize accounts with elevated access to the domain. These accounts hold the so-called 'keys to the kingdom' for your network. Most ransomware attacks need these accounts to be successful in disrupting your operations. Losing control of these accounts is no different than losing the master key to your home. It gives attackers free rein to compromise the majority of your environment.

- Everything you do in your environment create a log. These logs are critical in identifying whether your computers, users or network have been compromised. Not having enough systems recording these logs or not reviewing them can allow an attacker to hide unnoticed until they disrupt operations or prevent forensic firms from adequately understanding the extent of a breach or how they got into the environment. In other words, keeping and reviewing a log is similar to you remembering to lock the windows in your house and trying to determine which window was opened that allowed the intruder to enter your home. COCC, in addition to other security firms, offers this as a service. Specifically trained individuals armed with specialty software sift through the hundreds or thousands of logs to pick up on activity that isn't normal.

- Cyber insurance, like any insurance, is something you hope you never need. But does your organization know the process with your insurer if a situation arises? Who will make that call? These are questions you should not wait to ask or understand until an event, such as a ransomware attack, occurs as time is of the essence. Just like disaster recovery, people should have a solid understanding of who to call and the process involved.

While these items are not all-inclusive of a mature program, given the current environment, these are among the topics that should be top of mind. Building a culture of cyber readiness is a tone that must be set at the top to permeate throughout the organization. CISA has numerous free resources for leaders, IT staff and security professionals in critical infrastructure to help you mature your security programs. Furthermore, the FFIEC IT Handbooks provide a roadmap of the things an organization should be leveraging as best practices. The pace of cyber threats will only increase and everyone must be prepared.