UNDERSTANDING THE TACTICS OF RUSSIAN CYBER ATTACKS, AND HOW TO PREPARE FOR ONE

Anxiety is high around the potential for Russian cyberattacks given the current political climate. By learning about the history of cyber conflict between Russia and Ukraine, we can gain strategies to protect our own systems. Combined with conventional military forces, Russia has been using Ukraine as a live-fire cyber range to unleash cyberweapons as part of its military operations for years. These historic cyberattacks can serve as critical case studies of what can come in the future—read on for ways to prepare.

Case Studies

On December 23, 2015, Ukrainian civilians were preparing for Christmas festivities when 250,000 people lost power for several hours due to a cyberattack by the Russian hackers known as the Sandworm Team, which used traditional spear-phishing attacks to target power grid employees and gain initial access to the organization.

From there, they used a combination of custom tools and open-source malware like BlackEnergy to seize SCADA systems and remotely turn off critical substations. The BlackEnergy malware was able to disable and destroy key IT infrastructure components to limit the organization's ability to react to the attack. This case study shows us that Russian Advanced Persistent Threats (APTs) like the Sandworm Team are far more capable than simple attacks on Windows PCs and will target the critical infrastructure to inflict the most damage to an organization.

On June 27, 2017, the largest cyberattack in history was unleashed on nearly 100 companies that do business in Ukraine. The attack that became known as NotPetya was also attributed to the

Sandworm Team and was a worm that compiled several known exploits and open-source hacking tools. This worm automatically spread throughout victimized computer systems and unleashed an irreversible encryption attack that destroyed all the data on the system.

This cyber-attack masquerading as a criminal ransomware operation caused over ten billion dollars in damages, slowed global shipping by crippling shipping giants like Maersk, and demonstrated Russia's intent to target private companies and critical infrastructure as part of its cyber warfare foreign policy. The Sandworm Team did this by attacking one target—Ukrainian tax software company M.E.Doc—and backdooring their software to gain access to all of M.E.Doc's customers.

Security Blindspot

Private companies should take heed of these case studies as they demonstrate Russian willingness to target corporate business' critical infrastructure for devastating impact. Cybersecurity policy design should focus on identifying that key infrastructure, implementing modern and effective security controls, and testing them against dedicated white-hat hackers through penetration tests and cybersecurity simulations. Many organizations likely believe they are doing this, but reality continues to show a specific gap that modern cybersecurity tools and priorities have ignored—the

IBM® mainframe.

The mainframe is often called the backbone of the IT enterprise. It is still running the core business applications for 67 of the Fortune 100 and handles 68 percent of the world's production IT workloads. Despite this, it is commonly an afterthought for enterprise security strategies, and the pervasive myth that "you can't hack a mainframe" is still painfully common. The mainframe is just a server that can be accessed from any personal computer, which means it is just as vulnerable to attack as any other server in the enterprise.

In fact, because it is so often an afterthought, many mainframes are left staggeringly vulnerable by organizations that felt secure because they passed a checkbox audit. This false sense of security would have been pierced by a single mainframe penetration test done by a legitimate mainframe hacker, but many organizations have still not done this. This is dangerous.

A Bank's Sitting Duck

Let's take a look at the case of a bank that thought its mainframe was secure*. A hacker was able to spear-phish the system programmer by directly targeting him through LinkedIn. They knew his credentials based on his work title—we post that information openly for the world to see. Once they gained access to the system programmer's personal computer, they used a keylogger to steal his credentials and access the mainframe.

At this point, the hacker had as much control over the mainframe as that system programmer did—a lot. This bank couldn't detect anomalous or malicious activity, so the hacker built custom ransomware that encrypted dozens of sensitive files, which the bank was then forced to pay the hackers to retrieve. Imagine if this attack was by hackers who just wanted to destroy the entire mainframe environment with an irreversible encryption attack? That would be a catastrophic event for that organization. This is the exact kind of impact that Russia can have.

Secure Your Mainframe

So, what do we do about this kind of threat? For starters, **include your mainframe as a critical asset in any enterprise cybersecurity plan**. This means ensuring you have real-time visibility and analytics in your security operations center to detect anomalous and malicious activity happening on the mainframe.

You should also **build indicators of compromise** to detect whether an attacker gained control of your system programmer's credentials or the system was impacted by destructive damage from an insider threat.

By **implementing advanced controls under a Zero Trust architecture**, you can dramatically limit the scope of a breach should an attacker find a foothold. There is no standalone product that you can install to call Zero Trust complete, but you can implement a combination of solutions that work together enterprise-wide to limit lateral movement and detect malicious behavior.

If you have a mainframe, it is your critical infrastructure. The time to start securing it like one is now—To this end, and in an effort to help European customers go through the Russia-Ukraine conflict, BMC is making its mainframe security software, BMC AMI Security, available to European based customers in the banking and financial sectors, under a limited-term license at no charge, until December 31st, 2022. To learn more please contact your account manager representative.