XM CYBER®

SIMULATING ATTACKS TO SECURE BANKS: TO PROTECT YOUR GREEN, GO PURPLE

By XM Cyber Team

Hackers are constantly finding new ways to get through bank defenses, whether they are targeting a large international institution or a local community branch. These aren't just brute force attacks either; they often go undetected by employing legitimate tools, mimicking real users, and impersonating user behavior. The $60 million Taiwanese SWIFT bank cyber heist, $31 million Russian Central Bank theft, and $81 million Bangladesh cyberattack are just a few of the cases that have made headlines.

Although finance isn't the industry that's most often attacked, the cost per attack is much higher than in other sectors. Credit card numbers and security codes have a stronger appeal to cyber criminals than just names and passwords.

Banks are trying to protect their customers and their critical assets by investing in tools to help their security and risk personnel better close the gap between their own defenses and the threat actor's capabilities. In fact, they are early adopters who are very concerned about putting in place the most modern products and procedures.

Nevertheless, it is quite impossible for them to know whether their critical assets are truly safe at any given time. If financial institutions are at the forefront of cybersecurity, deploying all the latest security controls, policies, and processes, how are they still vulnerable to attacks? The answer is simple: They aren't looking at their network and assets from the hackers' perspective.

WHY ARE BANKS LAGGING BEHIND CRIMINALS?

While banks mainly have to deal with simple phishing and botnet attacks, financial institutions have become top targets for highly sophisticated advanced persistent threats (APT).

Organized cybercrime groups have much larger goals than just scamming a bank customer out of a few hundred dollars, and they have the time and tools to break into even the most well-protected banks.

In the case of the SWIFT hack, according to a police report, the assailants "spent several months inside the network of one customer, preparing for the eventual attack by stealing user credentials and monitoring the bank's operations using software that recorded computer keystrokes and screenshots." These aren't two-bit criminals looking to make a quick buck. They have the patience and diligence to wait until a strike will be the most effective.

A SOLUTION: CHECK YOUR SECURITY FROM THE HACKERS' PERSPECTIVE

In order to fight back, banks need to think like hackers. Some use penetration testing and red/blue team drills to assess the security of their network. However, with these types of tests, too often red and blue teams act separately, because of elements like cost and human availability, which makes it impossible to gauge how well the defenses would stack up in a live situation. This leads to stagnant security because the two teams can't react and adapt to what the other is doing.

One solution is to automate and combine the red and blue team functions into a single automated "purple team." Most banks currently use some automation, but not in the area of breach and attack simulation (BAS). These solutions are a relatively new category of tools that enable organizations to test network security in a risk-free environment.

One type of BAS solution is the automated purple team, which can simulate, validate and remediate the latest threats and APT techniques along the entire network from breach point to critical assets. This mixes the best aspects of penetration testing and proactive defense while removing such downsides as high cost and human error. It can detect vulnerabilities and shadow IT issues that a hacker could potentially exploit — from software that hasn't been updated to unencrypted password hashes stored on a shared drive. Once the attack vectors are identified, the defense kicks in to analyze the attack data and prioritize remediation strategies accordingly.

As countless new opportunities to breach the network arise and cybercrime costs continue to skyrocket, banks must do more to mitigate risk and combat cyber threats. Setting up an automated threat hunting team that continuously tests your security is an effective method of unearthing security shortcomings and turning the tide against the organized criminals that attack our financial organizations.

> *While banks mainly have to deal with simple phishing and botnet attacks, financial institutions have become top targets for highly sophisticated advanced persistent threats (APT).*

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

XM CYBER TEAM

The XM Cyber team consists of the best cyber security specialists in the world. Their thought leadership helps inform and educate customers globally via webinars, videos, articles, books and industry presentations. Join us online at xmcyber.com for more in-depth analysis and recommendations on cyber security best practices.