XM CYBER

WHY IS IT SO EASY FOR APTs TO MOVE THROUGH OUR NETWORKS?

By XM Cyber Team

These days all eyes are on cybersecurity. Mega hack attacks appear regularly on primetime news, security issues are sitting high on corporate boardroom agendas and security technology companies are the darlings of the investor community.

Given the grim state of global security, organizations are more aware, more prepared and more willing to invest in defense. But although they have drummed up their line of cyber defense and pitched their digital forks, advanced persistent threats (APTs) are having a field day.

THE LOSING BATTLE AGAINST ADVANCED PERSISTENT THREATS

It's mind boggling, when you think of it: How come, despite all the awareness, technology advancements and heavy investment, the fight against advanced persistent threats (APTs) remains a losing battle? The answer could be lurking in the shadows.

To review, an APT refers to a network attack by a third party that gains unauthorized access and remains there undetected for a long time. APTs are characterized by their high-level of sophistication, covertness, and use of bespoke software back doors, as well as zero-day vulnerabilities.

A disturbing aspect is the "persistency" factor, as hackers aim to stay undetected for a lengthy period until they achieve their end goals. They may try to infiltrate hundreds or thousands of times, then learn from their mistakes, modify their behavior, and finally find a way to go undetected under the radar. Once they're in, they often remain hidden inside a network, slowly siphoning data.

APTs CONTINUE TO MOVE LATERALLY THROUGH NETWORKS WITH RELATIVE EASE

APTs ease of movement is almost liquid, largely due to a shadow partner. Unassuming, unintentional and underrated, shadow IT has created a parallel world where APTs tend to thrive.

Although largely unauthorized, shadow IT is common practice and is here to stay. Shadow IT involves employees using systems and software without authorization by the IT unit. Whether we like it or not, SaaS downloads, the unauthorized use of apps, and BYOD (Bring Your Own Device) trends are growing, and expanding to the IoT-scape, casting an even larger shadow.

In effect, shadow IT is the gap between the IT security status, as perceived by the IT department, and the real picture. Here lies the crux of the matter: Hackers often rely on these very network gaps to operate in a stealthy mode and remain undetected under the radar.

WHY IS IT SO DIFFICULT TO DETECT SHADOW IT MISHAPS?

Despite heightened security awareness training, employees are still prone to daily cybersecurity errors; it's part of human nature. Short-lived errors, even with a lifecycle of only 24 hours, can evade security during these timely, but critical gaps. Even if there is an alert, it's difficult to pay attention to each event on a specific PC or device in a large network. At the end of the day, it is an inhuman mission for the IT department or assigned penetration tester, or even red teamer, to find all the problems and recognize their influence on large networks.

HOW COME IT'S GETTING WORSE?

Shadow IT error still accounts for most of the root causes of security compromises—perhaps as much as 90 percent. The trouble is that although shadow IT is not a new trend, malicious hackers are discovering more ways to exploit it. The more people who interact with I-connected endpoints, the more strategies hackers will find to take advantage of them. Now that connected devices are everywhere, the danger is growing.

WHAT CAN BE DONE TO STOP APTs IN THEIR TRACKS?

To combat APTs, security pros should shift their stance to assume APTs are already living in their network. Eventually someone will successfully penetrate a network; perhaps by taking advantage of a technological mishap, or maybe through a social engineering loophole.

Secondly, there needs to be a conceptual shift from passive defense to a threat hunting strategy from an attacker's point-of-view. It is essential to keep a network in a state of perpetual reconnaissance; because the attackers are using a combination of APT methods, they can leapfrog from one network section to another, completely undetected. They can work this way until they reach their final goal, whether it involves stealing data, or disrupting control systems, with potentially kinetic implications.

Today there's a new breed of automated attack simulation platforms that prevent APTs from compromising critical organizational assets and provide, actionable remediation in a continuous loop. These platforms can run multi-vector campaigns simultaneously to simulate an APT with 100% reliability.

It's almost like teaming up with an army of red team attackers that work 24/7, followed by a blue team that responds to actionable and prioritized information in real time. When aptly developed, these platforms can operate in a safe way without affecting the network or the user experience. Maybe there is hope after all.

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.