Analysts at Gartner Group are forecasting that it will account for 50% of all communication by 2018. CISOs are aware that BYOD messaging presents fresh vulnerabilities within the enterprise. It can only be a matter of time before a high-profile data breach or a significant penalty is traced back to inappropriate use of messaging apps by an insider. CISOs have no shortage of options for taking preventative measures but first they must overcome industry-wide scepticism over whether to invest in another layer of security.

About the author
Omri Sigelman is co-founder of NURO Secure Messaging (www.nuro.im), a secure group messaging platform that allows organisations, including enterprise, government and the armed forces to regain privacy and ownership of group collaboration between employees and authorised third parties for security and compliance purposes.

Sigelman is an experienced entrepreneur, having co-founded DroidSecurity, the first security suite for Android mobile devices in the market. The company later became AVG Mobile after being acquired by AVG Technologies. Sigelman led the AVG Mobile marketing and product management teams.

References

The evolution of the digital insider trader

Joseph Carson, Thycotic

The insider threat has been a major risk to all governments and organisations around the world for many years. High-profile examples are numerous – Nick Leeson and the collapse of Barings bank; Jeffrey Skilling, the former Enron president; and the more recent intelligence leaks from Chelsea Manning, Edward Snowden and Reality Winner that disclosed sensitive information that was damaging to the security and reputation of the US.

This is a reminder of how powerful and impactful trusted insiders can become because they have elevated privileges and are therefore able to leak sensitive data undetected. This type of behaviour has been controversial for years and it will long be debated whether or not Snowden is a hero, a whistle-blower, a patriot or a traitor. It has always been the assumption of hackers that governments are performing massive surveillance on citizens. However it wasn’t confirmed until Snowden revealed sensitive documents that provided the truth of its existence and started huge debates about government surveillance, encryption, national security and privacy.

Also a topic of recent debate has been the revelation and disclosure of the NSA
hacking tools that are now available online. This enables hackers and cyber-criminals to reuse powerful tools that were created for national security purposes, political advantage or intelligence gathering on other nation states. This has been a contributing factor to the recent major cyber-attacks, which used those tools to cause global havoc with ransomware such as WannaCry and NotPetya causing disruption and fear around the world.

It is thought that the insider threat represents approximately 43% of all data breaches.1 Some of these are intentional abuse or misuse. However, many are unintentional configurations or accidental data loss where the employee was likely the victim of a targeted phishing scam and unknowingly gave sensitive credentials to an external hacker. The hacker was then able to use that access to simply walk past the expensive complex security controls undetected.

In some cases, employees who have left the organisation still have active credentials, often for months after walking out the door. For a disgruntled employee it is then easy to return, to cause sometimes significant financial damage. The definition of the term ‘insider threat’ is evolving and the criminal underworld is bursting with this hidden secret that many organisations have yet to discover. We are entering the era of the cyber-security digital insider trader.

A new era

The new cyber-security digital insider trader is a cyber-criminal who has stolen valid credentials and has a trusted identity allowing him or her to gain access to the most sensitive confidential information the company owns. This can include a myriad of financial details and forecasts. For the cyber-criminal the goal is not to install malicious malware or disruptive ransomware forcing the company to pay out. These cyber-criminals do not even steal the data or threaten to disclose it.

Just like nation state cyber-security units that keep surveillance tools hidden and undisclosed, so criminals quietly use these exploits to gather intelligence or political advantages against adversaries and allies alike. In common with nation-state actors, cyber-criminals do not want to be detected and so employ the same techniques: however their goal is financial gain.

Passive assessment

Once these cyber-criminals have finished gathering data they create a massive digital footprint of the potential target. Typically this is achieved through vast correlation of public data using mathematical algorithms on companies that are stock market listed, have patents pending, active lawsuits, legal approvals, upcoming IPOs or those considered to be likely acquisition targets.

The insider traders intelligently comb through the data for the best targets, which would be expected to yield the highest returns and once identified, the active targeting of the victim begins. Usually it starts with collecting a digital footprint of the target’s employees and their family relations, organisational structure, public data, software versions, supply chains, third-party vendors and contractors. All of this can be obtained without touching the company’s security perimeter and is a technique known as passive assessment. When the weakest security link has been identified, which is typically either an employee or third-party vendor, and with enough knowledge of personal details, email formats, invoice templates and existing security controls, the cyber-criminals can easily start the technique to gain access.

Human factors

If we look at why many of the breaches in the past year have occurred, it comes down to three major factors – a: human factors, b: identities and credentials and c: vulnerabilities. In the digital age, most people are sharing more information via social media, ultimately causing themselves to be much more exposed to social engineering and targeted spear-phishing attacks. The ultimate goal is to compromise systems to commit financial fraud or to steal identities in order to access the company that the target was entrusted to protect. When identities are stolen, it provides the attacker with the means to bypass the traditional security perimeter undetected and if that identity has access to privileged accounts, he or she can easily carry out insider trading.

Email and social media continue to be the weapon of choice. Simply targeting a secondary victim – the unsuspecting employee who receives an authentic looking email from a third-party supplier – only requires that employee to click once on a hyperlink and it is game over for that endpoint. The employee has handed over his or her secret password and digital identity for the cyber-criminal to use and bypass security controls and pose as a trusted employee.

The cyber-criminal then spends time learning about the behaviour of the employee and any other predictable schedules and operations of the victim. He know when the victim logs on and off, what applications he executes and what is installed.

1. www.technologyreview.com/innovation/2017/05/01/insider-threat/
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات