Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – June 2022

Corporate Employees Focusing on M&A Being Pursued by Hackers

Employees focusing on mergers and acquisitions (M&A) and large corporate transactions are **being targeted** by a fairly new suspected espionage threat actor. The cybersecurity company Mandiant has been tracking this person or group believed to be called UNC3524, which is mirroring attack techniques used by different Russian-based hacks like APT28 and APT29. UNC3524's attacks involved the deployment of either a backdoor called QUIETEXIT, which allowed the attacker remote access, or a web shell as a means of alternate access, should the first backdoor stop functioning. Once inside a system, the attacker would retrieve information from emails of executives in a firm that worked on corporate development projects.

SEC Crypto Team Adds 20 Officials

The US Securities and Exchange Commission (SEC) is adding **20 additional officials** to a team dedicated to policing crypto markets in a move to crack down on digital tokens that violate the commission's rules. The focus on the group will include virtual currency, decentralized finance and trading platforms and stable coins.

Companies Seek to Alter Cyber Rules

After the US Securities and Exchange Commission (SEC) announced proposed rules, many companies are now looking to **change the proposed rules**. In comments to the SEC, companies have urged the agency to harmonize its deadline to four business days to disclose security incidents with similar rules with other agencies. In public interviews, security professionals from firms have said they are supportive of a SEC reporting regime and provisions to the proposed rules to support and fortify cybersecurity risk management.

CISA Removes Windows Vulnerability from Its Must-Patch List, Temporarily

The US **Cybersecurity and Infrastructure Agency** (CISA) temporarily removed a bug (**CVE-2022-26925**) from its catalog of vulnerabilities that are known to be exploited, a move that strays away from their norm. There is a possible risk of authentication failures if an admin applies Microsoft's 10 May 2022 roll up security fixes to Windows Servers that are used as domain controllers. While this issue is with regards to Windows Servers used as domain controllers, CISA is strongly advising admins to apply the May Windows updates on client Windows devices and non-domain controller Windows Servers.

Crypto Survey Highlights Regulatory Concern

A survey was held during a crypto conference in late April of this year. The **survey** gathered the views and key themes from attendees. Participants of the survey represented both decentralized finance (DeFi) and traditional finance (TradFi) organizations. Survey results showed that 60% of participants say clarity around regulatory framework will have the most positive impact on institutional crypto adoption. Another 55% also say that regulatory uncertainty is most likely to hinder adoption. The survey showed that most participants plan to increase their exposure to crypto through the end of this year.