Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – April 2022

New Target for Ransomware Attackers: Company Acquistions

Two months after a **midsized manufacturer** was purchased by a private-equity firm, the manufacturer had to pay a ransomware group that had locked up its systems. The cost of the ransom was about $1.2 million and was paid to a group suspected of links to the Russian ransomware group REvil. This attack fits a familiar pattern, as ransomware groups are turning their attention to midmarket acquisition targets, presenting a risk for private equity, venture capital and other deal makers that often invest in these businesses as the new company has access to more funds and less robust cybersecurity. While midsize companies represent a small number of all companies attacked, their average payouts exceed over one million dollars. Attackers see them as a stable source of payments without any geopolitical risk that comes with attacking a globally-based company.

A Joint Advisory from CISA and the FBI

On Saturday, 26 February, the US Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a **joint advisory** that pointed to Ukrainian organizations becoming a target to Russian state-sponsored activity utilizing WhisperGate and HermeticWiper malware. The **advisory** presents actions that organizations can start to take today as WhisperGate and HermeticWiper are designed to erase Windows devices and corrupt the master boot record of a hard drive. While the advisory does contain detailed guidance, organizations are encouraged to increase vigilance and evaluate their capabilities to include planning, preparation, detection, and response.

Applying Security During Software Development

According to a report from **Checkmarx**, vulnerable applications were shown to be a direct result of at least two security breaches in 45% of responding organizations. This report highlights the biggest security challenges that application security (AppSec) managers and software developers are facing. While the survey featured factors that contributed to breaches – Software supply chain attack, cloud application misconfiguration, and malicious third-party packages, there was some positive news to share. A great deal was learned from the breaches with an insightful take-away for implementing greater application security, and overall security, that can be achieved in the coming year with having clearer defined roles and responsibilities for AppSec managers and developers, along with better integration of application security testing.

New SEC Proposal on Reporting Requirements

On 9 March, the Securities and Exchange Commission proposed a new cybersecurity risk management and disclosure rule for publicly traded companies, where companies have to report a **cybersecurity incident within 4 hours**. The proposed rule would also require publicly traded companies periodically disclose their policies for managing cybersecurity risks, the company's management team's role in managing cybersecurity and the company's board of directors' oversight role and cybersecurity expertise.

FINRA Alerts Broker Dealers to Russian Sanctions

Since 25 February, the Financial Industry Regulatory Authority (FINRA) has issued two sanction alerts pertaining to Russian sanctions. The regulator is urging broker dealers (BDs) to **review the various sanctions** issued against Russian financial institutions, debt and equity offerings and leaders. The notices also suggests BDs monitor the Treasury Department's Office of Foreign Asset Control (**OFAC**) website for more developments.