Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – July 2022

New Cybersecurity Regulations to Assist the Financial Sector

The European Union (EU), in a move to lessen the cyber threat risk to financial institutions, is **imposing tougher cybersecurity standards**, according to Moody's Investors Services. While this new legislation will lead to increased costs, the upside will bring improved cyber defense standards and a more cohesive framework for overseeing cybersecurity risk. With more organizations moving to the cloud, this legislation will emphasize reliance and utilization on third-party providers and vendors.

CISA Warns of Active Exploitation

The United States Cybersecurity and Infrastructure Agency (CISA) added a Linux vulnerability named PwnKit to its known exploited vulnerabilities **catalog**. The vulnerability was first **discovered** in the beginning of this year detailing concerns of a local privilege escalation in polkit's **pkexec** utility, which allows an authorized user to execute commands as another user. Successful exploitation of the flaw could allow the pkexec utility to execute arbitrary code, granting access administrative rights to a malicious actor.

Ukraine Arrest Cybergroup Operating 400+ Phishing Sites

The Ukraine police have arrested nine members of a criminal group that operated over 400 phishing websites designed to appear like EU portals offering financial assistance to Ukrainians. These malicious actors used forms on the site to steal visitors' payment card information and online banking account credentials and perform fraudulent, unauthorized transactions like moving funds to accounts they controlled. The arrested individuals may face up to 15 years in prison for multiple violations of the Ukraine's Criminal Code.

Unpatched Email Servers Used to Deploy Ransomware

Microsoft has announced that an affiliate of the **BlackCat ransomware group** is attacking unpatched Microsoft Exchange Servers. Security experts from the software maker stated that in one instance the attackers slowly moved through the victim's network, stealing credentials and exfiltrating information used for double extortion. After a few weeks, the unpatched Exchange server was used as an entry point, and the threat actors deployed the BlackCat ransomware payloads. Although the Exchange vulnerability used for initial access was not named, Microsoft refers to a **security advisory** from March of last year.

Rise of Ransomware Against Governments

Researchers have the observed a **rise in ransomware attacks** in the second quarter of 2022. Various attacks would severely impact the victims, such as the 12 April attack on the Costa Rican government, which caused a nationwide crisis. Experts have warned of the attacks against government organizations, and have observed a total of 48 government organizations from 21 countries that were hit by attacks in 2022. Small states and governments seem to be an easy target for these attackers because of the low level of security of their critical infrastructure due to low budgets protecting them. Experts highlighted the importance of these smaller states and governments to improve their cyberdefense to quickly respond to any attacks.