Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – August 2022

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.

CISA Orders Agencies to Patch Zero-Day Vulnerabilities

The United States Cybersecurity and Infrastructure Agency (CISA) **has ordered agencies** to patch new Windows zero-day used in attacks by 2 August 2022. The severity flaw (**CVE-2022-22047**) impacts both Windows server and clients, including the latest desktop and servers. Microsoft has already released a patch to this vulnerability, which they say was discovered internally by the Microsoft Threat Intelligence Center and Microsoft Security Response Center.

HavanaCrypt Ransomware Delivered via Fake Google Update

A new ransomware is being delivered via the disguise of a **Google update**. Researchers states that the HavanaCrypt ransomware contains features meant to defy reverse engineering and speed up file encryption before the **malicious actor** collects the victim's money. The malware encrypts the file with the '.Havana' file extension and at the start of its execution on a host machine checks to see if it is being run on a virtual machine, if so it shuts down the VM. Whoever is behind HavanaCrypt sought to ensure the software moves quickly by invoking thread pooling, a software design technique for concurrent execution by the operating system.