Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – July 2021

High Tech Cybercrime is Here to Stay

Cyber-attacks are now happening more frequently with the **stakes getting higher** each time. According to Brad Gow, Global Cyber Product Leader from Sompro International, cyber-attacks will continue to grow until the money flow stops. Ransom requests of $30, $40 or $50 million are becoming more the norm, which has put immense pressure on organizations to strengthen their defenses as well as insurers who are sometimes unable to write policies on these organizations.

Over 8 Billion Passwords Leaked

Last week, over 8 billion passwords had been posted on a popular hacker forum. A forum user posted a 100GB text file containing the **8 billion plus passwords**; it is presumed that the list had been a combination of previous data leaks and breaches. The compilation itself has been dubbed 'RockYou2021', in reference to the **RockYou data breach** in 2009.

By combining all of these password variations with other breach compilations, threat actors can use the list of passwords in the Rockyou2021 file to gain access to accounts or systems by credential stuffing and password spraying attacks.

Microsoft Patches Six Zero-Day Security Holes

On 8 June 2021, Microsoft released security updates for their Windows operating systems and other software products including **fixes for six zero-day bugs** that malicious hackers already are exploiting in active attacks. Some details of the zero-days are:

- **CVE-2021-33742** - a remote code execution bug in a Windows HTML component.
- **CVE-2021-31955** - an information disclosure bug in the Windows Kernel
- **CVE-2021-31956** - an elevation of privilege flaw in Windows NTFS
- **CVE-2021-33739** - an elevation of privilege flaw in the Microsoft Desktop Window Manager
- **CVE-2021-31201** - an elevation of privilege flaw in the Microsoft Enhanced Cryptographic Provider
- **CVE-2021-31199** - an elevation of privilege flaw in the Microsoft Enhanced Cryptographic Provider

Microsoft states that the elevation of privilege flaws are just as valuable to attackers as remote code execution bugs. Once an attacker has gained access, they can move laterally across the network and uncover further ways to escalate to system or domain-level access.