Threat Image

Entering June, we will look at some Advanced Persistent Threat (APT) actors, starting with Iran. Iranian state actors use Cyber-Enabled IO or psychological operations (PSYOPS) to influence other nations. According to Microsoft, Israel and the USA are highly targeted. Iranian State Actors used SMS messaging in conjunction with the impersonation of high-value organizations and figures to amplify their PSYOPS efforts. (1)

Leading Russian anti-malware vendor Kaspersky revealed the discovery of an APT actor launching zero-click iMessage exploits on iOS devices within its corporate network. On the same day, the Russian Federal Security Service (FSB) separately accused US intelligence agencies of conducting a continuous espionage campaign, targeting numerous iOS devices belonging to domestic subscribers and foreign diplomatic missions. (2)

In a collaborative effort, the National Security Agency (NSA) has partnered with several organizations to enhance awareness regarding the Democratic People's Republic of Korea's (DPRK) strategic use of social engineering and malware tactics. DPRK has strategically targeted sectors such as think tanks, academia, and news media sectors. (3)
North Korea's cyber program provides the regime with broad intelligence collection and espionage capabilities. The Governments of the United States and the Republic of Korea (South Korea) have observed sustained information-gathering efforts originating from these North Korean cyber actors. The Reconnaissance General Bureau (RGB), North Korea's main military intelligence organization, is primarily responsible for this network of actors and activities. To help protect against these DPRK cyber-attacks, the NSA and its partners have publicly released the Cybersecurity Advisory (CSA) titled "North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media." (4)

The hacker group known as "Anonymous Sudan" has recently made an unexpected demand of $3 million from Scandinavian Airlines (SAS) to halt their distributed denial-of-service attacks (DDoS) that have been targeting the airline's websites since February. Despite initially presenting themselves as politically motivated hacktivists, the group appears to be resorting to using extortion tactics for financial gain. (5)

Latest Cyberthreats and Advisories (6)

- China State-Sponsored Actor Infiltrates U.S. Critical Infrastructure
- The Meteoric Rise of LockBit Ransomware
- Over 1 Million Customer Records Leaked in SimpleTire Database Error Debacle
- U.S. City of Augusta Reportedly Hit with Ransomware Attack
- Personal Data Swindled from Nearly 9 Million Patients in MCNA Dental Breach

(1) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW13D48
(2) https://www.securityweek.com/russia-blames-us-intelligence-for-ios-zero-click-attacks/
(3) https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-rok-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/
(4) https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF
(5) https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas
(6) https://blog.isc2.org/isc2_blog/2023/06/latest-cyberthreats-and-advisories-june-2-2023.html