LA-SAFE CYBER DIGEST

June 28, 2022

MALWARE | SOCIAL ENGINEERING | RANSOMWARE

Cyberattack Forces Iran Steel Company to Halt Production **-SecurityWeek– 06.27.2022**
One of Iran's major steel companies said on Monday it was forced to halt production after being hit by a cyberattack, apparently marking one of the biggest such assaults on the country's strategic industrial sector in recent times. The company's CEO, Amin Ebrahimi, claimed that Khuzestan Steel managed to thwart the cyberattack and prevent structural damage to production lines that would impact supply chains and customers. The company did not blame any specific group for the assault, which constitutes just the latest example of an attack targeting the country's services that has embarrassed authorities in recent weeks.

Analyst Note:
A supply chain attack is a highly effective way of breaching security by injecting malicious libraries or components into a product without the developer, manufacturer, or customer's knowledge. The supply chain is not a single uniform group of suppliers, as there are often several layers. These layers can include vendors, customers, and manufacturers. Many large organizations have security controls that make infiltration difficult. Illicit actors use the relations between suppliers or vendors and attack the targets at the weakest points (small business who is a customer or vendor). It is important that all businesses stay vigilant and protect their networks. Even though a business may not be the direct target, they may be a link in the chain of attack.

CYBER POLICY| CYBER INFRASTRUCTURE | CYBER INITIATIVE

Japanese Man Loses USB Stick with Entire City's Personal Details **-BBCNews-06.24.2022**
The unnamed individual who works for a company tasked with providing benefits to tax exempt households losing a memory stick during an evening of drinking. The USB contained the personal information of the entire city's residents. City officials said the memory stick included the names, birth dates, and addresses of all the city's residents. It also included more sensitive information, including tax details, bank account numbers and information on families receiving social security. Luckily, city officials said the data on the drive is encrypted, locked with a password, and there had been no signs of unlawful access.

Analyst Note:
This is a great illustration of practices that should be a part of any company cybersecurity policy. The agency likely required the employee to have a password encrypted drive that stored such valuable information. Unfortunately, the policy may not have included regulations on where the device could be stored once utilized for company purposes. Personal time turned into an alarming incident when the USB disappeared. Administrator's regulatory policy needs to include where and how information should be stored and utilized. The policy should also include detailed information about which devices are acceptable and who should keep these devices in their possession.

CYBER CRIME | CYBER DEFENSE | SECURITY BREACH

Fancy Bear Uses Nuke Threat Lure to Exploit One-Click Bug **-ThreatPost-06.23.2022**

Advanced persistent threat group *Fancy Bear* is behind a phishing campaign that uses the specter of nuclear war to exploit a known one-click Microsoft flaw. The goal is to deliver malware that can steal credentials from the Chrome, Firefox and Edge browsers. Fancy Bear is pushing malicious documents weaponized with the exploit for Follina (CVE-2022-30190). Follina is associated with the Microsoft Support Diagnostic Tool (MSDT) and uses the ms-msdt protocol to load malicious code from Word or other Office documents when they're opened. Microsoft recently patched Follina in its June Patch Tuesday release but it remains under active exploit by threat actors, including known APTs.

Analyst Note:

Follina affects the Microsoft Support Diagnostic Tool (MSDT) in Windows. An attacker can exploit this vulnerability and take control of an affected system. Security issues are regularly identified in various parts of any operating system, including the main platform. To further help protect systems, software patching is key. Software patching is the process of repairing system vulnerabilities that are discovered after the infrastructure components have been released on the market. Administrators should make sure all systems are constantly updated and any patches issued should be install so that systems can remain protected from publicized vulnerabilities.