Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – February 2022

Zloader Malware Spreads to 100+ Countries

Researchers have warned of a **new malware campaign** that has already stolen passwords and user information from over 2000 victims in over 100 countries worldwide. The banking Trojan named Zloader uses web injections to steal cookies, passwords, and sensitive information from its victims. It has been linked to the delivery of the Ryuk and **Conti** ransomware variants. In the past, Zloader has been deployed using both traditional phishing email campaigns and abuse of online advertising platforms where attackers purchase ads pointing to **legitimate looking websites** hosting the malware. This new campaign Begins with the installation of legitimate remote management program from ATERA **pretending to be a Java installation**. The installation of the ATERA software provides attacker access to the infected system allowing them to access files, and run scripts, such as one to exploit a firm's digital signature verification method. Researchers do not know how this campaign has been disseminated, but the largest groups of victims are located in the United States, followed by Canada and India. Users are advised to not install programs from unknown sources and not to click on links or open attachments in unsolicited messages.

FS-ISAC Launches Critical Providers Program

On 19 January, FS-ISAC announced the launch of a new member benefit, the Critical Providers Program to bolster the financial sector's supply chain security. This comes as critical service providers increasingly host, connect, and protect a substantial percentage of financial institutions' digital infrastructure. Critical providers are defined as non-financial organizations providing network infrastructure and services that, if impacted by an incident, would interrupt a significant amount of core financial services across the sector. *Connect* users were automatically added to the new Critical Provider (CP) team in *Connect*. In the CP team, they will have access to a dedicated channel for each critical provider. In the event of a large-scale incident, these dedicated *Connect* channels will function as the official conduits of timely, accurate, and necessary information. Additionally, they will be used to communicate during large-scale security upgrades, technical outages, cyber-based vulnerabilities, software and hardware misconfigurations, and/or changes that could impact multiple members. A FAQ document is on the FS-ISAC website **here**.

GDPR Fines Increase Sevenfold

According to new research, **fines for the European Union privacy law** have increased to a total of $1.25 billion over breaches of the bloc's General Data Protection Regulation (GDPR) since 21 January 2021, up from $180 million the year prior. Notifications of data breaches from firms to regulators climbed by 8% to 356 notifications a day on average.

Since 2018, GDPR has been in use and the regulation is aimed at giving consumers in Europe more control over their information. Companies are required to demonstrate a clear legal basis to collect and process user's data. The rule states that firms must notify authorities about any data breach within 72 hours of first being aware of a breach. If a firm fails to comply it can result in large fines including up to 4% of a company's annual revenue.

CISA Urges Preparedness for US Organizations

The Cybersecurity and Infrastructure Security Agency (CISA) is imploring US organizations to **bolster their cybersecurity defenses** against data-wiping attacks. The urgency from CISA was prompted by the recent news coming from the Ukrainian government who recently suffered a coordinated cyberattack where websites were vandalized, and data was corrupted. CISA has provided steps to be taken by organizations to defend themselves against similar attacks.