Financial Sector Cyber Risks As Seen Through the Eyes of Central Bank CISOs

Survey responses from 21 Central Bank CISOs were used to develop a **working paper** on the main cyber concerns of central banks, their views of the threat landscape, and their overall assessment of cyber resiliency for the global financial sector. While responses varied based on whether the central bank was in an advanced economy vs. an emerging market economy, they had many views in common. Most have increased their cyber security-related investments by 5-10% since 2020, focusing on technical security controls and resiliency. Phishing, and social engineering are agreed to be the most common attack methods, while advanced persistent malware and ransomware are the costliest.

The blurring of defined perimeters to protect, by way of increased adoption of cloud services and move to remote work, has increased the risk and potential losses of a systemic cyber-attack on big tech providing critical cloud infrastructures. Furthermore, most agree that insurance markets are ill-prepared to effectively price and cover losses in the event of a cyber-attack. Central banks are increasingly focusing on risk management and resiliency efforts for the sector.

MSFT to Disable Exchange Online Basic Authentication

Microsoft has warned customers that it will **disable basic authentication** worldwide to improve Exchange Online security staring 1 October 2022. The announcement follows multiple reminders and warnings the company has issued over the last three years since it was decided back in September 2019.

Basic Authentication is an HTTP-based auth scheme application used for sending credentials in plain text to servers, endpoints, and other various online services. This method could allow threat actors to steal credentials using a man-in-the-middle style attack. They can steal the clear text credentials from apps using the basic auth via other tactics as well. Using basic auth makes it more complicated for firms to enable multi-factor authentication (MFA), dissuading firms from implementing MFA. Firms that still use Basic Authentication are encouraged to review notes and announcements made by Microsoft and apply new improved methods of authentication

SEC Sets Up New Office for Crypto Filings

Earlier this month the US Securities and Exchange Commission (SEC) announced a **new office to handle filings related to crypto assets**. The 'Office of Crypto Assets' will join several existing offices under the commission which handles corporate disclosure filings.

Credential Pharming Campaign Steals Thousands of Real Estate Credentials

People associated with real estate transactions, including realtors, real estate lawyers, title agents, buyers, and sellers, were targeted with phishing emails which, using familiar subject lines and templates from two mortgage and title companies, directed them to review new documents or messages on a secure server. The links brought them to fake log-in pages asking for their Microsoft 365 credentials. Each attempt returned an error and prompt to try again, allowing the criminals to collect thousands of possible credentials.

Researchers at Ironscales discovered these credentials while investigating vendor impersonation phishing campaigns. Furthermore, they noticed that Microsoft Defender features "Safe Links", which provides URL scanning and rewriting of inbound emails, and time-of-click verification of URLs and links in emails, did not function as intended. The initial phishing attack email URLs were not impacted by Safe Links, while subsequent iterations used Safe Link-compatible URLs, but still pointed to the original phishing URL.

Find two FS-ISAC alerts related to this activity: **FirstAm Credential Pharming** and **United Wholesale Mortgage Credential Pharming**.

Third-Party Breach Impacts Mortgage Customers

The Overby-Seawell Company (OSC), a provider of insurance services for lenders, mortgage servicers, and property investors, reported a data breach in August 2022 to the Attorney General in Maine and Montana on behalf of **Fulton Financial** and **KeyBank**. The personal information of their mortgage customers, including full names, Social Security numbers, addresses, account numbers, and mortgage loan information, was stolen.

An investigation by OSC concluded that an unauthorized party obtained access to their systems on 26 May 2022 and lasted until 5 July 2022 when OSC identified the threat. According to reports, KeyBank was informed of the breach on 4 August 2022, and it is unknown when Fulton Financial was notified. Both institutions have informed their impacted customers and offered free fraud monitoring services but face the possibility of a class action lawsuit as a result of the breach. The potential reputational and financial consequences stress the need for better third-party risk management.

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.