Cyber Section

Department Reminds Firms to Contact Regulators with Issues Related to SolarWinds Breach

DoBS is reminding financial service registrants, state-registered investment advisers and intrastate broker-dealers, to report any known issues or concerns related to the SolarWinds cybersecurity incident to their primary securities regulator.

In December 2020, the federal government reported that SolarWinds, a vendor that provides updating and monitoring software to numerous government agencies and private companies, was the victim of a breach that caused SolarWinds Orion Network Management Products to transmit malware to many of its clients, including federal, state, and local governments, as well as other private sector entities.

The U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has issued an alert that describes the threat and provides guidance on how to address it. Any firm with known malicious versions of the SolarWinds Orion software should contact its primary regulator. State-registered investment advisers and intrastate broker-dealers in Pennsylvania should contact the department at RA-BNSECURITIESLIC1@pa.gov.

CISA: CHIRP IOC Detection Tool

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA has announced its CISA Hunt and Incident Response Program (CHIRP) tool. The tool helps network defenders detect activity related to the supply chain compromises affecting SolarWinds and Active Directory/Microsoft 365. CHIRP is freely available on the CISA GitHub Repository. Organizations can use CHIRP to:

- Examine Windows event logs for artifacts associated with this activity;
- Examine Windows Registry for evidence of intrusion;
- Query Windows network artifacts; and
- Apply YARA rules to detect malware, backdoors, or implants.

Ransomware Self-Assessment Tool

The Bankers Electronic Crimes Taskforce (BECTF), State Bank Regulators and the United States Secret Service has developed a Ransomware Self-Assessment Tool. The tool was developed to help financial institutions assess their efforts to mitigate risks associated with ransomware and identify gaps for increasing security. This tool provides executive management and the board of directors with an overview of the institution's preparedness towards identifying, protecting, detecting, responding, and recovering from a ransomware attack.

Microsoft Exchange Cyber Attack

On March 2, Microsoft announced hackers had gained access to email accounts through vulnerabilities in its Exchange Server email and calendar software.

Microsoft has issued security patches for the vulnerabilities dating back 10 years, with attackers exploiting those vulnerabilities since January.

According to the Wall Street Journal, tens of thousands of businesses, government offices and schools are potentially impacted.

CISA has issued an alert on mitigating the Microsoft Exchange Server vulnerabilities.