Risk Alert: Cybersecurity: Safeguarding Client Accounts Against Credential Compromise

September 29, 2020

On September 15, 2020, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert warning financial firms of an increase in "credential stuffing" cyber-attacks. Credential stuffing is an automated attack on a client account or direct network using compromised login account credentials purchased from the dark web. Recent SEC examinations have revealed an increase in these automated attacks, some of which have resulted in the loss of customer assets and unauthorized access to customer information. In an effort to reduce successful attacks, the OCIE staff shared best practices of firms that have implemented policies and procedures to help protect client accounts from credential stuffing attacks.

Credential stuffing can be a more effective and efficient way for attackers to gain unauthorized access to customer accounts and firm systems than traditional brute force password attacks. Cyber attackers obtain lists of usernames, e-mail addresses, and corresponding passwords from the dark web and then use those lists to attempt to log in and gain unauthorized access to client accounts. If successful, cyber attackers can then use this access to steal assets from client accounts, access confidential information, sell the credentials to other cyber attackers on the dark web, or gain access to a firm's network and system resources.

Internet-facing websites, such as a firm's information system, are targets for credential stuffing because they can be used by attackers to initiate

transactions or transfer funds from a compromised client account. This includes systems hosted by third-party vendors. If an attacker is successful in obtaining a client's personal information, this may open the door for the attacker to take over a client account or attack accounts held by the client at other institutions. This is especially risky if clients use the same password across accounts or use login usernames that are easily guessed, such as e-mail addresses or full names.

To help mitigate this risk, the OCIE staff has recommended that firms periodically review cybersecurity policies and controls with a focus on the following practices:

- Review, and if necessary, update the firm's Regulation S-P and Regulation S-ID policies and programs to address the emerging risk of credential stuffing;
- Incorporate minimum password requirements (length, character types, change frequency) to ensure adequate complexity;
- Employ and properly implement Multi-Factor Authentication ("MFA") to authenticate the person seeking to log into an account;
- Deploy a "Completely Automated Public Turing test to tell Computers and Humans Apart" ("CAPTCHA") to combat automated scripts or bots used in such attacks. (CAPTCHA usually requires users to identify particular objects within a grid of pictures, a sequence of letters and numbers perceptible in a distorted image, or words spoken against a background of other noise);
- Consider whether the firm's customers and staff are properly informed on how they can better secure their account through strong passwords and MFA, including the use of mobile phones prompts to verify users; and
- Implement client account monitoring controls to detect and prevent attacks such as:
    - monitoring for a higher-than-usual number of login attempts over a given time period, or a higher-than-usual number of failed logins over a given time period;
    - using a Web Application Firewall ("WAF");
    - using tools to collect information about user devices and creating a "fingerprint" for each incoming session; and
    - monitoring the dark web for lists of leaked user IDs and passwords and performing tests to evaluate whether current client accounts are susceptible to credential stuffing attacks.

OCIE staff notes that even with MFA, it is still possible for attackers to identify valid user accounts, which may be sold on the dark web to other attackers. These attackers may attempt to gain access through social engineering, phishing e-mails, and online research. Furthermore, while mobile devices are commonly used as a verification method for MFA, mobile devices can pose a risk if the phone (and SIM card) are not properly destroyed.

It is important that firms understand the current and emerging cyber threats, such as credential stuffing so that they can adopt appropriate policies and controls to mitigate those threats. A strong cybersecurity program will include structures to proactively identify, test, monitor, and adapt to such emerging threats.

Foreside has partnered with BlueVoyant to offer cost-effective, tailor-made cybersecurity consulting and managed security services specifically designed to meet the needs of Foreside's clients.

Austin Berglas, BlueVoyant Global Head of Professional Services and former head of the FBI Cyber Branch in New York notes, "Unfortunately your risks from credential stuffing extend well beyond your business perimeter. In addition to implementing MFA and enforcing solid password hygiene as recommended by OCIE, organizations need to be concerned with the exploitation of trust. A compromise of the account of a trusted vendor or business partner can serve as a vector of attack through carefully crafted phishing e-mails, aimed at obtaining sensitive information from your employees or gaining a foothold inside of your organization."

Foreside and BlueVoyant are prepared to help you combat credential stuffing and other forms of cybercrime. Click **here** to learn more about our cybersecurity offerings.

Home