Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Cyber Attacks Compromising Credentials

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members,[1] is issuing this statement to notify financial institutions of the growing trend of cyber attacks for the purpose of obtaining online credentials for theft, fraud, or business disruption and to recommend risk mitigation techniques. Financial institutions should address this threat by reviewing their risk management practices and controls over information technology (IT) networks and authentication, authorization, fraud detection, and response management systems and processes.

This statement does not contain any new regulatory expectations. It is intended to alert financial institutions of specific risk mitigation related to cyber attacks compromising credentials. Financial institutions should refer to the appropriate *FFIEC Information Technology (IT) Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

Recent reports indicate an ongoing and increasing trend of attacks by cyber criminals to obtain large volumes of credentials. These attacks include theft of users' credentials—such as passwords, usernames, e-mail addresses—and other forms of identification used by customers, employees, and third parties to authenticate themselves to systems as well as theft of system credentials, such as certificates.

User credentials can be stolen in many ways, including phishing and spear-phishing,[2] malvertising,[3] watering holes,[4] and web-based attacks.[5] Stolen credentials are often sold in

[1] The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

[2] Conducting attacks using social engineering by sending e-mails disguised as legitimate messages; tricking users into disclosing names and passwords, payment card information; or clicking on links or attachments that deliver malware to their computers.

[3] Injecting malware into legitimate online advertising and downloading the malware to the computer of any person who visits the Web site containing the advertisement.

[4] Injecting malware into a vulnerable Web site frequented or commonly visited by targeted victims. The compromised site facilitates the downloading of malware to the computer of any person who visits the Web site.

cyber-criminal forums and then used to commit fraud through account takeovers and identity theft. Users may significantly increase exposure by creating usernames and passwords that are easy to guess or using the same usernames and passwords to access accounts on multiple Web sites.

The theft of each type of user credential presents distinct risks. Stolen customer credentials may give an attacker access to customers' account information to commit fraud and identity theft. Stolen employee and third-party credentials may provide initial access to trusted internal systems that may be used to leverage system administrator level access to obtain confidential business and customer information, modify and disrupt information systems, and destroy or corrupt data. System credentials may be targeted directly through vulnerabilities in authentication systems (e.g., OpenSSL "Heartbleed")[6] or indirectly by compromising the credentials of trusted third parties (e.g., fraudulent certificates). Stolen system credentials may also be used to gain access to internal systems and data to further distribute malware or impersonate the financial institution to facilitate fraud such as accessing payment processing systems for automated clearing house transactions.

RISKS

Compromised credentials may expose financial institutions to a range of risks that include loss of the confidentiality and integrity of sensitive data, such as customer information and confidential business information. Further, compromised credentials enable cyber attackers to disrupt and degrade systems or process fraudulent financial transactions that may not be recovered by the institutions.

RISK MITIGATION

Financial institutions should design multiple layers of security controls to establish several lines of defense and ensure that their risk management processes also address the risk posed by compromised credentials, consistent with the risk management guidance contained in the *FFIEC IT Examination Handbook*,[7] specifically the "Information Security,"[8] "Outsourcing Technology Services,"[9] and the "Retail Payment Systems"[10] booklets.

---

[5] Targeting systems and services that contain customer credentials using "brute force" or other methods to gain access to the information through direct penetration of the targeted network.

[6] http://www.ffiec.gov/press/PDF/OpenSSLAlert041014.pdf

[7] http://ithandbook.ffiec.gov/

[8] http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[9] http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

[10] http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx

To mitigate the potential risks to customer information, financial institutions must follow the standards outlined in the *Interagency Guidelines Establishing Information Security Standards*[11]and the related *Guidance and Supplement on Authentication in an Internet Banking Environment.*[12] The guidance requires, among other things, security measures to reliably authenticate customers accessing their financial institutions' Internet-based services.

In accordance with regulatory requirements and FFIEC guidance, a financial institution should consider taking the following steps.

- **Conduct ongoing information security risk assessments.** Maintain an ongoing information security risk assessment program that considers new and evolving threats to online accounts and adjust customer authentication, layered security, and other controls in response to identified risks. Identify, prioritize, and assess the risk to critical systems, including threats to applications that control various system parameters and other security and fraud prevention measures. In addition, ensure that third-party service providers
    - Perform effective risk management and implement controls.
    - Properly maintain and conduct regular testing of their security controls simulating potential risk scenarios.
    - Are contractually obligated to provide security incident reports when issues arise that may affect the institution.

- **Perform security monitoring, prevention, and risk mitigation.** Ensure protection and detection systems, such as intrusion detection systems and antivirus protection, are up-to-date and firewall rules are configured properly and reviewed periodically. Establish a baseline environment to enable the ability to detect anomalous behavior. Monitor system alerts to identify, prevent, and contain attack attempts from all sources. In addition,
    - Follow software assurance industry practices for internally-developed applications.
    - Conduct due diligence of third-party software and services.
    - Conduct penetration testing and vulnerability scans, as necessary.
    - Promptly manage vulnerabilities, based on risk, and track mitigation progress, including implementing patches for all applications, services, and systems.
    - Review reports generated from monitoring systems and third parties for unusual behavior.

- **Protect against unauthorized access.** Limit the number of credentials with elevated privileges across the institution, especially administrator accounts, and the ability to easily assign elevated privileges to access critical systems. Review access rights periodically to reconfirm approvals are still appropriate to the job function. Establish stringent expiration

[11] 12 CFR Part 30, Appendix B (Office of the Comptroller of the Currency); 12 CFR Part 208, Appendix D-2, and Part 225, Appendix F (Federal Reserve); 12 CFR Part 364, Appendix B (Federal Deposit Insurance Corporation); 12 CFR Part 748, Appendix A and B (National Credit Union Administration).

[12] http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf

periods for unused credentials, monitor logs for use of old credentials, and promptly terminate unused or unwarranted credentials. Establish authentication rules, such as time-of-day and geolocation controls, or implement multifactor authentication protocols for web-based control panels. In addition,

- Conduct regular audits to review the access and permission levels to critical systems for employees and contractors. Implement least privileges access policies[13] across the entire enterprise. In particular, do not allow users to have local administrator rights on workstations.
- Change default password and settings for system-based credentials.
- Prevent unpatched systems, such as home computers and personal mobile devices from connecting to internal-facing systems.
- Implement monitoring controls to detect unauthorized devices connected to internal networks.
- Use secure connections when remotely accessing systems and services (e.g., virtual private networks).

- **Implement and test controls around critical systems regularly.** Ensure appropriate controls, such as access control, segregation of duties, audit, and fraud detection and monitoring systems, are implemented for systems based on risk. Limit the number of sign-on attempts for critical systems and lock accounts once such thresholds are exceeded. Implement alert systems to notify employees when baseline controls are changed on critical systems. Test the effectiveness and adequacy of controls periodically. Report test results to senior management and, if appropriate, to the board of directors or a committee of the board of directors. Include in the report recommended risk mitigation strategies and progress to remediate findings. In addition,
  - Encrypt sensitive data on internal- and external-facing systems in transit and, where appropriate, at rest.
  - Implement an adequate password policy.
  - Review the business processes around password recovery.
  - Regularly test security controls, such as web application firewalls.
  - Implement procedures for the destruction and disposal of media containing sensitive information based on risk relative to the sensitivity of the information and the type of media used to store the information.
  - Filter Internet access through Web site whitelisting[14] where appropriate to limit employees access to only those Web sites necessary to perform their job functions.
  - Conduct incremental and full backups of important files and store the backed-up data offline.

[13] Principles of least privilege refers to the security objective of granting users only the access needed to perform official duties.

[14] A computer administration practice used to permit users the ability to access only authorized Web sites.

- **Enhance information security awareness and training programs.** Conduct regular, mandatory information security awareness training across the financial institution, including how to identify and prevent successful phishing attempts. Ensure training reflects the functions performed by employees.

- **Participate in industry information-sharing forums.** Incorporate information sharing with other financial institutions and service providers into risk mitigation strategies to identify, respond to, and mitigate cybersecurity threats and incidents. Since threats and tactics can change rapidly, participating in information-sharing organizations, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), can improve an institution's ability to identify attack tactics and to successfully mitigate cyber attacks involving destructive malware on its systems. In addition to the FS-ISAC, there are government resources such as the U.S. Computer Emergency Readiness Team (US-CERT) that provide information on vulnerabilities. The US-CERT portal may be found at www.us-cert.gov.

ADDITIONAL RESOURCES

The following resources provide practical information for strengthening user awareness and highlight the need for customers to maintain strong passwords and safe online practices.

- Federal Trade Commission's On Guard Online at www.onguardonline.gov
- National Cyber Security Alliance's Stay Safe Online at www.staysafeonline.org

REFERENCES

FFIEC Information Technology Examination Handbook booklet "Business Continuity Planning"
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

FFIEC Information Technology Examination Handbook booklet "Information Security"
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

US-CERT Alert, "Phishing Campaign Linked with 'Dyre' Banking Malware" https://www.us-cert.gov/ncas/alerts/TA14-300A