Joint Statement

Cyber-attacks on Financial Institutions' ATM and Card Authorization Systems

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members[1] ("members") are issuing this statement to notify financial institutions of a type of large dollar value automatic teller machine (ATM) cash-out fraud characterized as Unlimited Operations by the U.S. Secret Service. The members are aware of a recent increase in cyber-attacks launched in connection with this fraud, to gain access to, and alter the settings on, ATM web-based control panels used by small- to medium-size financial institutions.

Unlimited Operations may cause financial institutions to incur large dollar losses. Therefore, the members expect financial institutions to take steps to address this threat by reviewing the adequacy of their controls over their information technology networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes.

BACKGROUND

Unlimited Operations are a category of ATM cash-out fraud where criminals are able to withdraw funds beyond the cash balance in customer accounts or beyond other control limits typically applied to ATM withdrawals. Criminals perpetrate the fraud by initiating cyber-attacks to gain access to web-based ATM control panels, which enables them to withdraw customer funds from ATMs using stolen customer debit, prepaid, or ATM card account information. A recent Unlimited Operations attack netted over $40 million in fraud using only 12 debit card accounts.

Criminals may begin the attack by sending phishing emails to employees of financial institutions as a means to install malicious software (malware) onto the institution's network. Once installed, criminals use the malware to monitor the institution's network to determine how the institution accesses ATM control panels and obtain employee login credentials. These control panels, often web-based, manage the amount of money customers may withdraw within a set time frame, the geographic limitations of withdrawals, the types and frequency of fraud reports

---

[1] The FFIEC is comprised of 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.

that its service provider sends to the financial institution, the designated employee that receives these reports, and other management functions related to card security and internal controls. When criminals obtain this information, they may use an employee's login credentials to gain access to the control panel and change the settings to permit greater or unlimited cash disbursements at ATM machines, and to change other fraud and security related controls.

Following an attack on an institution's ATM control panels, criminals use fraudulent debit, prepaid, or ATM cards they create with account information and personal identification numbers (PINs) stolen through separate attacks to withdraw funds from ATMs. Card account information and PINs typically are stolen in a number of ways including through point-of-sale (POS) malware or skimming, ATM malware or skimming, or compromise of the issuer's card operations. The cash-out phase of the attack involves criminals organizing simultaneous withdrawals of large amounts of cash from multiple ATMs over a short time period, usually four hours to two days. Criminals may conduct their operations during holidays and weekends to take advantage of increased cash levels in ATMs and limited monitoring by financial institutions during non-work hours.

RISKS

Financial institutions that issue debit, prepaid, or ATM cards may face a variety of risks from Unlimited Operations including operational risks, fraud losses, liquidity and capital risks, depending on the size of the institution and the losses incurred, and reputation risks. Financial institutions that outsource their card issuing function to a card processor may initially be liable for losses even if the compromise occurs at the processor.

RISK MITIGATION

Financial institutions should ensure that their risk management processes address the risk from these types of cyber-attacks consistent with the risk management guidance contained in the *FFIEC Information Technology (IT) Examination Handbook* [2] and specifically the *Information Security*,[3] *Outsourcing Technology Services*,[4] and the *Retail Payment Systems*[5] booklets.

Financial institutions and processors that create PINs for cardholders should follow the Payment Card Industry Data Security Standards (PCI-DSS) on *PIN Security Requirements*,[6] September 2011, and *Hardware Security Module (HSM) Security Requirements*,[7] May 2012, to address key management practices and the use of HSMs for encrypting PINs.

---

[2] http://ithandbook.ffiec.gov/
[3] http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
[4] http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
[5] http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx
[6] https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements.pdf
[7] https://www.pcisecuritystandards.org/documents/PCI_HSM_Security_Requirements_v2.pdf

In accordance with regulatory requirements[8] and FFIEC guidance, the members expect financial institutions to take the following steps, as appropriate:

- ***Conduct ongoing information security risk assessments.*** Maintain an ongoing information security risk assessment program that identifies, prioritizes and assesses the risk to critical systems, including threats to applications that control ATM parameters and other security and fraud prevention systems.

- ***Perform security monitoring, prevention, and risk mitigation.*** Ensure intrusion detection systems and antivirus protection are up-to-date, and firewall rules are configured properly. Monitor system reports to identify when attacks are attempted or are occurring, when data may be inappropriately leaving the network, and when anomalous behavior patterns occur inside the institution's network (i.e., attempted simultaneous logins to control panels or login attempts during non-business hours). Monitor third-party processers as well as ATM transaction activity for unusual behavior or attempts to go beyond normal daily limits.

- ***Protect against unauthorized access.*** Limit the number of elevated privileges across the institution, including administrator accounts, and the ability to assign elevated privileges to critical systems such as the systems to manage the institution's card issuer authorization and ATM management systems. Consider updating all credentials and monitoring logs for use of old credentials. Consider establishing authentication rules, such as time-of-day controls, or implementing multifactor authentication protocols for web-based control panels.

- ***Implement and test controls around critical systems regularly.*** Ensure appropriate controls are implemented for systems based on risk. Ensure that sign-on attempts for critical systems are limited and result in locking the account once limits are exceeded. Implement alerts to notify multiple employees when controls are changed on critical systems. Test the effectiveness of controls periodically. Report test results along with recommended risk mitigation strategies and progress to remediate findings to senior management or a committee of the board of directors.

- ***Conduct information security awareness and training programs.*** Conduct regular information security awareness training across the financial institution, including how to identify and prevent successful phishing attempts.

- ***Test incident response plans.*** Test the effectiveness of incident response plans at the financial institution and with third-party processors to ensure that all employees

---

[8] 12 C.F.R. Part 30, Appendix B (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, Appendix D-2, and Part 225, Appendix F (Federal Reserve); 12 C.F.R. Part 364, Appendix B (Federal Deposit Insurance Corporation); 12 C.F.R. Part 748, Appendix A and B (National Credit Union Administration).

understand their respective responsibilities and protocols, including individuals responsible for managing liquidity and reputation risk, information security, vendor management, fraud detection, and customer inquiries. Consider conducting an exercise at the financial institution that simulates this type of attack.

- *Participate in industry information sharing forums.* Incorporate information sharing with other financial institutions and service providers into risk mitigation strategies. 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 facilitate more efficient information sharing. The FS-ISAC and the United States Computer Emergency Readiness Team (US-CERT) are good sources of information on the methods used to conduct attacks and on risk mitigation tactics to minimize their impact.