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

Destructive Malware

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members,[1] is issuing this statement to notify financial institutions of the increasing threat of cyber attacks involving destructive malware. Financial institutions and technology service providers should enhance their information security programs to ensure they are able to identify, mitigate, and respond to this type of attack. In addition, business continuity planning and testing activities should incorporate response and recovery capabilities and test resilience against cyber attacks involving destructive malware.

This statement does not contain any new regulatory expectations. It is intended to alert financial institutions to specific risk mitigation related to the threats associated with destructive malware. 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

Over the past two years, cyber attacks on businesses have increased in frequency and severity. In some cases, destructive malware used in these attacks successfully compromised large quantities of data and rendered supporting systems inoperable. Malware can be introduced into systems through a variety of mechanisms, including through employees downloading attachments in phishing or spear-phishing emails, connecting external devices (e.g., USB drives), or visiting compromised Web sites, or through unauthorized parties using stolen employee or third-party credentials to install malware directly on systems. Once introduced, destructive malware may be further distributed through compromised enterprise system management technologies.

Historically, business continuity plans have focused on restoring operations after physical events, such as a natural disaster or other geographically centered infrastructure disruptions. In today's rapidly evolving cyber threat landscape, however, comprehensive resilience depends on the ability to identify and contain damage, recover data, and restore operations from a broader set of scenarios that include cyber attacks involving destructive malware on critical information systems or the institution's underlying infrastructure. To ensure that critical backup data are not

[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.

destroyed or corrupted by destructive malware, financial institutions and their technology service providers should ensure that recovery strategies address the potential for simultaneous cyber attacks on backup data centers (e.g., mirrored sites[2]) or the potential for corrupted data to replicate to backup systems.

RISKS

Financial institutions face a variety of risks from cyber attacks involving destructive malware, including liquidity, capital, operational, and reputation risks, due to such events as fraud, data loss, and disruption of customer service.

RISK MITIGATION

Financial institutions should ensure that their risk management processes and business continuity planning address the risk from this type of cyber attack consistent with the risk management guidance contained in the *FFIEC IT Examination Handbook*, specifically the booklets on "Business Continuity Planning" and "Information Security" and their appendixes, such as Appendix J, Strengthening the Resilience of Outsourced Technology Services.

An institution's management is expected to maintain sufficient business continuity planning processes to ensure the rapid recovery, resumption, and maintenance of the institution's operations after a cyber attack involving destructive malware. A financial institution should develop appropriate processes that enable recovery of data and business operations and that address rebuilding network capabilities and restoring data if the institution or its critical service providers fall victim to this type of cyber attack. This should include the ability to protect offline data backups from destructive malware.

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

- **Securely configure systems and services.** Protections such as logical network segmentation, hard backups, air gapping,[3] maintaining an inventory of authorized devices and software, physical segmentation of critical systems, and other controls may mitigate the impact of a cyber attack involving destructive malware. Consistency in system configuration promotes the implementation and maintenance of a secure network. Essential components of a secure configuration include the removal or disabling of unused applications, functions, or components.

- **Review, update, and test incident response and business continuity plans.** Test the effectiveness of incident response plans at the financial institution and with third-party processors to ensure that all employees, including individuals responsible for managing

[2] Data mirroring is the replication of data to alternate processing sites or storage systems at regular intervals defined by recovery time periods of an organization.

[3] An air gap is a security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically.

liquidity and reputation risk, information security, vendor management, fraud detection, and customer inquiries, understand their respective responsibilities and their institution's protocols. Conduct an exercise at the financial institution that simulates a cyber attack involving destructive malware.

- **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 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[4] across the

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

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[5] 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.

- **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

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

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 government resources provide assistance to institutions for mitigating destructive malware.

US-CERT Security Tip (ST13-003) “Handling Destructive Malware” https://www.us-cert.gov/ncas/tips/ST13-003

Joint Security Awareness Report (JSAR-12-241-01B) “Shamoon/DstTrack Malware” https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B

National Institute of Standards and Technology “Cybersecurity Framework” http://www.nist.gov/cyberframework/

US-CERT “Cyber Resilience Review” https://www.us-cert.gov/ccubedvp/self-service-crr

NSA/CWW Information Assurance Directorate (MIT-001R-2015) “Defensive Best Practices for Destructive Malware”
https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf

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

FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement
http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf