FFIEC Released Two Statements on Compromised Credentials and Destructive Malware

The FFIEC provided two statements in order to notify financial institutions of the growing trend of cyber-attacks involving destructive malware and obtaining online credentials for theft, fraud or business disruption.

Sources: FFIEC Statement on Destructive Malware (PDF)

FFIEC Statement on Compromising Credentials (PDF)

What does this mean for Financial Institutions?

These statements do not contain any new regulatory expectations for financial institutions. They are intended to alert financial institutions of these specific growing threats and to ensure that financial institutions remain up-to-date on the below enhancements and the FFIEC's expanded focus on technology service providers' cybersecurity preparedness.

In accordance with FFIEC guidance, financial institutions should complete the following:

- Securely configure systems and services
- Review, update and test incident response and business continuity plans
- Conduct ongoing information security risk assessments
- Perform security monitoring, prevention and risk mitigation
- Protect against unauthorized access
- Implement and test controls around critical systems regularly
- Enhance information security awareness and training programs
- Participate in industry information-sharing forums, such as the Financial Services Information Sharing and Analysis Center

The FFIEC also included the below resources with additional information for strengthening user awareness of safe online practices.

- *Federal Trade Commission's On Guard Online*
- *National Cyber Security Alliance's Stay Safe Online*
- *US-Cert Security Tip (STI-003) "Handling Destructive Malware"*
- *Joint Security Awareness Report (JSAR-12-241-01B) "Shamoon/DstTrack Malware"*
- *National Institute of Standards and Technology "Cybersecurity Framework"*
- *US-CERT "Cyber Resilience Review"*
- *NSA/CSS Information Assurance Directorate (MIT-001R-2015) "Defensive Best Practices for Destructive Malware"*