# BEST PRACTICES FOR US FINANCIAL INSTITUTIONS

## Reducing Risks Associated with Destructive Malware

**November 23, 2015**

## Executive Summary

Destructive Malware (DM) is a unique threat in that it is both infrequent and yet potentially catastrophic. It presents a significant threat to an organization's daily operations and business continuity; it impacts confidentiality, integrity and availability of data, and can thwart an organization's ability to recover from an attack. Two recent cyber-attacks against the Las Vegas Sands and SONY Entertainment illustrate how DM can compromise an organization's data integrity, disrupt business operations, and harm brand reputation.

The National Institute of Standards and Technology (NIST) defines malware as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." [1]

Financial institutions are under increasing threat from cyber-attacks involving DM[2]. In light of this, an interagency working group (WG) comprised of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the National Security Agency (NSA), and the Securities Industry and Financial Markets Association (SIFMA) recently published a whitepaper and resource guide that map currently available resources for financial institutions, providing an accessible instrument that organizations can use to identify and assess vulnerabilities, and implement holistic security processes.

In addition, the members of this WG provide recommendations in the context of the NIST Cybersecurity Framework to defend against DM and have consolidated industry best controls and processes based upon a five-part risk management framework, which consists of twenty processes and controls recommended for reducing the risks associated with DM. As this threat applies to both enterprise systems as well as Industrial Control Systems (ICS), additional guidance for ICS DM mitigations is included in each section.

A more detailed paper is available for financial institutions in the FS-ISAC portal and on the Financial Services Sector Coordinating Council website. This detailed paper may also be useful for non-financial institutions that are deemed to be part of the nation's "critical infrastructure."

Financial institutions of all sizes should review their existing strategies to protect critical assets from DM and adjust countermeasures where necessary to address this evolving operational risk. Fundamentally, a financial institution should implement processes and controls centered on five core elements:

[1] Malware is an umbrella term that can include viruses, worms, Trojans, ransomware, spyware, adware, scareware, wiper software and other malicious, hostile or intrusive software. It can be used to spy or designed to cause harm, destroying or sabotaging systems or data. The recommendations in this paper are concerned with malware that destroys the confidentiality, integrity and availability of data.

[2] https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

***Identify* –** Gain situational awareness by identifying critical data, backup processes and systems in the organization that is necessary for critical business functions, where it comes from, where located, and where used. Having a thorough knowledge of solution components, training, vectors, detection technology, ongoing risk assessments, monitoring, information sharing and incident response keeps the enterprise in a continuous state of alert and prepares an organization to take action promptly.

***Protect* –** From network and endpoint security to system redundancy and backup, to reputation management, a variety of controls are necessary for a comprehensive and robust security framework to protect corporate data and personally identifiable information.

***Detect* -** Speed is essential in detecting malware when it enters a key environment, understanding the context, determining whether it is destructive in nature and quickly assessing the full potential impact.

***Respond* -** In the event of unauthorized access, the financial institution's computer systems could potentially fail, and confidential information could be compromised. Management must decide how to properly protect information systems and confidential data while also maintaining business continuity.

***Recover* –** Organizations need to adjust their cyber incident response processes and playbooks to prepare for a destructive malware scenario where there is the potential of catastrophic business impact. Organizations need to update mitigation strategies and align multiple parts of the organization - including the executive team, communications teams, customer-facing departments and business partners.

## Primary Recommendations

| | Rec 1 | Rec 2 | Rec 3 | Rec 4 | Rec 5 |
|---|---|---|---|---|---|
| Identify | Build a strong security awareness training program and crisis response to destructive malware threats and potential attacks | Identify all potential attack vectors for destructive malware and create programs promoting awareness and defense | Note all systems with enterprise-wide reach | Perform consistent and ongoing security monitoring, prevention and risk mitigation | Participate in industry information-sharing forums |
| Protect | Operationalize preventive controls, segmenting networks and making it as hard as possible for adversaries to move within a system, using encryption to transmit and store data safely, and establishing baselines from which to monitor all future activity | Implement detective controls such as multifactor authentication, event correlation, session timeouts and restricting access to help identify harmful attacks as they occur | Use corrective controls as a first response, suspending accounts or access based on policy violations and increasing time intervals between unsuccessful logins | Enhance both strategic and tactical controls in line with an organizations high risk assets and threat vectors | Use multiple backup solutions including offline backups, snapshots, and replication, on a regularly timed schedule altered to reflect the risk associated with the data |

| | | | | | |
|---|---|---|---|---|---|
| | Risk-based detection should be based on organizations, countries, or actors that pose a threat to the organization | Signature-based detection should monitor for known malware on networks and endpoints and should be shared through information sharing groups with the industry | Behavior-based detection will rely on an organization's baseline to notify teams of any change to the environment and to abnormal activity, lateral movement, and privilege escalation | Ensure you have a strong and well known reporting procedure for social engineering attacks | Use application based controls requiring active verification as a control against data integrity attacks, which can often go unnoticed |
| Respond | Develop an Incident Response Plan and test annually, integrating with the Business Continuity Plan | Contain any attack the moment it is detected to minimize damage through immediate reporting and engagement of those assigned responsibility to respond during an attack | Isolate all compromised systems, search for additional compromises, validate the integrity of data downstream, communicate with affected parties and preserve all evidence | Focus intrusion response on technologies and people, formalizing both aspects in an Incident Response Plan is key to an effect response | Engage the Computer Security Incident Response Team or equivalent security team and integrate this teams activity into other crisis response teams within the organization |
| Recover | Using evidence preserved during the response, categorize IT assets by criticality and use well document recovery plans to being the process or restoring systems and networks | Utilize multiple backups that have been maintained separately and restore data to alternate systems | Use snapshots of storage to minimize data loss and plan for other ways to record transactions that have occurred during the incident so you can account for those transactions once systems have resumed | Consider a Bare Metal Rebuild BMR in the event of a catastrophic event, which works separately from conventional backup tape processes, as BMR is faster and eliminates some human error | Document all procedures, maintaining forensics in order to share threat indicators with industry and government partners and immediately incorporate any lessons learned from the event |

## Participating Organizations

The Destructive Malware - Data Integrity Task Force (DMDITF) consisted of 85 experts from 36 companies and associations as well as 7 government agencies and partners including the following:

**Financial Services – Information Sharing and Analysis Center (FS-ISAC):**

Launched in 1999 by the financial services sector in response to 1998's Presidential Directive 63 which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the US critical infrastructure. The FS-ISAC is uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information, including analysis and recommended solutions from industry experts. The Treasury and Department of Homeland Security rely on the FS-ISAC to disseminate critical information to the financial services sector in times of crisis.

**National Institute of Standards and Technology (NIST):**

Founded in 1901 and now part of the US Department of Commerce, NIST and the National Cybersecurity Center of Excellence (NCCoE) is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major handicap to US industrial competitiveness at the time - a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of 4 human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks. The National Cybersecurity Center of Excellence (NCCoE) at NIST was established in 2012 to provide businesses with real-world cybersecurity solutions based on commercially available technologies.

**Department of Homeland Security (DHS):** The DHS has a vital mission to secure the nation from the many threats we face. DHS duties are wide-ranging, and its goal is clear - keeping America safe. DHS works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems and to reduce the vulnerability of critical infrastructure and key resources, and of essential leadership. It also warns of major events, such as terrorist attacks. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical national infrastructures – including assets, networks, and systems – that are vital to public confidence and the nation’s safety, prosperity, and well-being.

**National Security Agency (NSA):** The NSA has provided timely information to US decision makers and military leaders for more than half a century. NSA is unique among US defense agencies because of its government-wide responsibilities, providing products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners. The Agency's Information Assurance Directorate (IAD) is responsible for NSA's defensive mission and is widely acknowledged for leading innovative security solutions. Partnering extensively with government, industry, and academia ensures appropriate security solutions are in place to protect and defend information systems, as well as our nation's critical infrastructure.

**Securities Industry and Financial Markets Association (SIFMA)**: SIFMA is the voice of the US securities industry, representing the broker-dealers, banks and asset managers with access to the capital markets, raising over $2.4 trillion for businesses and municipalities in the US, serving clients with over $16 trillion in assets and managing more than $62 trillion in assets for individual and institutional clients including mutual funds and retirement plans.

## Questions (Contact):

Member Services, 877.612.2622 – prompt 1

# # #