



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE

Version 1.0

16 January 2015

MIT-001R-2015



# DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE



Once a malicious actor achieves privileged control of an organization's network, the actor has the ability to steal or destroy all the data that is on the network. While there may be some tools that can, in limited circumstances, prevent the wholesale destruction of data at that point, the better defense for both industry and government networks is to proactively prevent the actor from gaining that much control over the organization's network. In practice, this can be difficult to do, but there are several cost effective mitigations that make it much more difficult for a malicious actor to achieve that level of control over an organization's network undetected. The earlier that network defenders can detect and contain an intrusion, the less damage the intruder can possibly cause. In addition to trying to contain an intrusion as early as possible, planning for the possibility of a significant intrusion and potential wide scale destruction of data and systems will be well worth the effort in the event that they are needed. Preparing through offline backups and exercised incident response and recovery plans can make the organization more resilient, enabling quick reconstitution and the resumption of normal business functions as soon as possible.

This report reiterates many strategies from the NSA/CSS Information Assurance Directorate's (IAD) previously published "**Information Assurance Mitigation Strategies**" (available at [http://www.nsa.gov/ia/mitigation\\_guidance](http://www.nsa.gov/ia/mitigation_guidance)), as well as additional guidance. Presented below are the mitigations and best practices that prevent, detect, and contain an adversary who seeks to penetrate and disrupt an organization's systems.

## Prevent, Detect, and Contain

The best practices to protect information systems and networks from a destructive malware attack include:

- Segregate network systems in such a way that an attacker who accesses one enclave is restricted from accessing other areas of the network
  - For more information, please see the IAD Publication, [Segregating Networks and Functions](http://www.nsa.gov/ia/files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf), at:  
[http://www.nsa.gov/ia/files/factsheets/I43V\\_Slick\\_Sheets/Slicksheet\\_SegregatingNetworksAndFunctions\\_Web.pdf](http://www.nsa.gov/ia/files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf)
- Protect and restrict administrative privileges, especially for high-level administrator accounts, from discovery and use by the adversary to gain control over the entire network
  - For more information, please see the IAD Publication, [Control Administrative Privileges](http://www.nsa.gov/ia/files/factsheets/I43V_Slick_Sheets/Slicksheet_ControlAdministrativePrivileges_web.pdf), at:  
[http://www.nsa.gov/ia/files/factsheets/I43V\\_Slick\\_Sheets/Slicksheet\\_ControlAdministrativePrivileges\\_web.pdf](http://www.nsa.gov/ia/files/factsheets/I43V_Slick_Sheets/Slicksheet_ControlAdministrativePrivileges_web.pdf)
- Deploy, configure, and monitor application whitelisting to prevent unauthorized or malicious software from executing



# DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE



- For more information, please see the following IAD Publications:
  - IAD's Application Whitelisting Slick Sheet:  
<http://www.nsa.gov/ia/ files/factsheets/I43V Slick Sheets/Slicksheet Application Whitelisting Standard.pdf>
  - Application Whitelisting Trifold:  
<http://www.nsa.gov/ia/ files/factsheets/Application Whitelisting Trifold.pdf>
  - Application Whitelisting Using SRP:  
<http://www.nsa.gov/ia/ files/os/win2k/Application Whitelisting Using SRP.pdf>
  - Application Whitelisting using Host Based Security System (HBSS):  
<http://www.nsa.gov/ia/ files/factsheets/HBSS HIPS Application Whitelisting Technical Implementation Guide 20130211.pdf>
  - Application Whitelisting using Microsoft AppLocker<sup>®1</sup>: visit [www.iad.gov](http://www.iad.gov) (login required) and search for AppLocker.
- Limit workstation-to-workstation communications to reduce the attack surface that an adversary can use to spread and hide within a network
  - For more information, please see the IAD Publication, Limit Workstation to Workstation Communications, at:  
<http://www.nsa.gov/ia/ files/factsheets/I43V Slicksheets/Slicksheet LimitingWtWCommunication Web.pdf>
- Implement robust network boundary defensive capabilities such as perimeter firewalls, application firewalls, forward proxies, sandboxing, and/or dynamic analysis filters to catch malware as it enters the network
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions to detect anomalous or malicious activity as soon as possible, enabling containment and response actions before significant damage is done
  - For more information, please see the IAD Publication, Spotting the Adversary with Event Log Monitoring, at:  
<http://www.nsa.gov/ia/ files/app/Spotting the Adversary with Event Log Monitoring.pdf>
- Implement Pass-the-Hash (PtH) mitigations to reduce the risk of credential theft and reuse
  - For more information, please see the IAD Publication, Reducing the Effectiveness of Pass-the-Hash, at:

---

<sup>1</sup> AppLocker<sup>®</sup> is a registered trademark of Microsoft Corporation in the United States and/or other countries.



# DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE



- <http://www.nsa.gov/ia/ files/app/Reducing the Effectiveness of Pass-the-Hash.pdf>

  - Also see the Microsoft<sup>2</sup> publication on PtH, Mitigating Pass-the-Hash (PtH) and Other Credential Theft Techniques, at:  
<http://www.microsoft.com/en-us/download/details.aspx?id=36036>
- Deploy Microsoft Enhanced Mitigation Experience Toolkit (EMET) or other anti-exploitation capability (for non-Windows<sup>3</sup> operating systems) to prevent numerous initial exploits from being successful
  - For more information, please see the following IAD Publications:
    - Anti-Exploitation Features:  
<http://www.nsa.gov/ia/ files/factsheets/I43V Slick Sheets/Slicksheet AntiExploitationFeatures Web.pdf>
    - Microsoft's Enhanced Mitigation Experience Toolkit:  
<https://www.nsa.gov/ia/ files/os/Win EMET/I43V EMET Rationale v3.4.pdf>
    - Understanding the Enhanced Mitigation Experience Toolkit  
<https://www.nsa.gov/ia/ files/os/Win EMET/EMET FAQ v3.1.pdf>
- In addition to anti-virus services, employ anti-virus file reputation services to gain full benefit from industry knowledge of known malware sooner than normal anti-virus signatures can be deployed
  - For more information, please see the IAD Publication, Anti-Virus File Reputation Services, at:  
<http://www.nsa.gov/ia/ files/factsheets/I43V Slick Sheets/Slicksheet AntivirusFileReputationServices.pdf>
- Implement and tune Host Intrusion Prevention Systems (HIPS) to detect and prevent numerous attack behaviors
  - For more information, please see the IAD Publication, Host Intrusion Prevention Systems, at:  
<http://www.nsa.gov/ia/ files/factsheets/I43V Slick Sheets/Slicksheet HostIntrusionPreventionSystems.pdf>
- Update and patch software in a timely manner so known vulnerabilities cannot be exploited
  - For more information, please see the IAD Publication, Take Advantage of Software Improvements, at:

<sup>2</sup> Microsoft<sup>®</sup> is a registered trademark of Microsoft Corporation in the United States and/or other countries.

<sup>3</sup> Windows<sup>®</sup> is a registered trademark of Microsoft Corporation in the United States and/or other countries.



# DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE



[http://www.nsa.gov/ia/files/factsheets/I43V\\_Slick\\_Sheets/Slicksheet\\_SoftwareImprovements\\_Print.pdf](http://www.nsa.gov/ia/files/factsheets/I43V_Slick_Sheets/Slicksheet_SoftwareImprovements_Print.pdf)

## Prepare for Incident Response and Recovery

Hardening a network and defending its systems is more than just implementing mitigations and best practices. To more fully defend a network and its resources, an organization should prepare for a worst case scenario that requires an incident response. Incident response plans should be tested on a regular basis, to ensure the plans are viable, reflexive, and account for new personnel and technology. The NSA/CSS recommends the following actions in preparation for a similar event:

- Implement a robust backup solution for all critical systems and data
  - The backup solution should include out-of-band or offsite backups to prevent an adversary from fully destroying critical data
  - These backups should be regularly tested
- Establish an incident response plan that addresses communication (normal and out-of-band), roles and responsibilities, data recovery/reconstitution procedures, eviction strategies, and reporting processes that can be put into action quickly upon detection of a significant intrusion event
- At the conclusion of an incident, ensure that lessons learned are collected, assessed and necessary adjustments are made across the enterprise in order to reduce the likelihood of a future exploit using the same tactic, technique or procedure.

### Disclaimer of Endorsement:

The guidance in this document is provided "as is." In no event shall the United States Government be liable for any damages, regardless of the nature or theory of liability, arising in any way out of the use of or reliance on this guidance. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.