Incident Response – Malware Play Cheat Sheet

Purpose:
The purpose of this document is to provide guidance to IT Custodians of individual Biological Sciences Division (BSD) Departments of the potential information required from IT Custodians to be given to Security Analysts upon a Potential Security Event realized as a **Malware Incident**.

Scope:
This cheat sheet describes the questions a Security Analyst will be requiring to answer based on a Potential Security Event turning into a Malware Incident and the potential actions a Security Analyst will require an IT Custodian to perform to contain, eradicate and remediate a Malware Incident.

Malware Types:

- Worm
- Virus
- Bot
- Ransomware
- Other

Roles:

Role	Description
IT Custodian	Responsible for managing IT systems assigned to them within their department. Typically, the first connect for end-user experiencing a potential incident.
BSD ISO Security Analyst	The BSD Information Security Office (ISO) provides information security services and security guidance to the BSD leadership and all members of the BSD research and academic enterprise. The Security Analysts within the BSD monitors events throughout the BSD departments and determine if potential incidents should be escalated to incidents. The BSD ISO works with end users, IT Custodians, and leadership within the BSD to ensure incidents are resolved in a timely manner.
System Owner	A System Owner is an employee of the BSD who is director level, faculty, or above who has the ultimate responsibility over a particular IT system. System Owners are responsible for ensuring their systems are maintained in a secure manner and working with IT Custodians and the BSD ISO to ensure security incidents are resolved in a timely manner.
Unit Leader (UL)	Unit leaders are senior leaders within each department. ULs are responsible for ensuring their departments operate within the BSD guidelines and policy, including security. ULs are the third level of

Incident Response – Malware Play Cheat Sheet

	escalation for security incidents and are typically only notified when all other means of resolving the security incident are exhausted.
BSD Chief Information Security Officer (CISO)	The BSD Chief Information Security Officer (CISO) is the lead of the BSD ISO. The CISO is responsible for developing, and maintaining security policies, standards, and procedures across all the BSD departments. The CISO facilitates the escalation of security incidents when initial attempts to correct the incident are exhausted and the security incident has not been resolved.

(MALWARE CATAGORY)

Upon notification that a Potential Security Event has been promoted to a Malware Incident, the Security Analyst is required to answer the following questions:

Questions	**Actions/Answers**
Can it be confirmed that the malware can be totally removed via anti-virus software?	IT Custodian attempts to use well-known techniques to remove the malware from the system. If the malware cannot be removed, the following actions and **information** might be required: If "yes": 1. **Date malware removed using AV** 2. **Type of Malware removed using AV Software** If "no": 1. Isolate the system from the network (pull the network wire) **– Date of system isolation from network** 2. Confiscate the system – **Data equipment was retrieved** 3. Provisioning of replacement equipment – **Data temporary replacement equipment was delivered to the user**
Can malware be removed manually using a verified process and without strenuous effort?	IT Custodian has exhausted all his/her well-known techniques to remove the malware, but there is an existing method to remove the malware from a 3rd party, then the following actions and **information** might be required: If "yes": 1. Using the 3rd party process, IT Custodian removes the malware – **Was malware manually removed successful?** If "yes": **a. Date malware was removed** **b. Infection Vector** If "no": a. **Does the System have a Known good backup available? (yes/no)** b. **Infection Vector**
Are credentials compromised due	IT Custodian has made the determination with the possible

Incident Response – Malware Play Cheat Sheet

to malware?	assistance from the Security Analyst that the System User's credentials have been compromised. The following **information** might be required: If "yes": 1. **Date of changed credentials of compromised account(s)**
Was the malware delivered as a result of a phishing campaign?	**Yes/No**
Did data breach occur as a result of this malware?	**Yes/No**

(MALWARE RANSOMWARE SUBCATAGORY)

In addition to the questions from above, if a Potential Security Event is promoted to a Malware Incident with type "Ransomware', then the following additional questions might be required:

Questions	**Actions/Answers**
Was Critical Data Lost?	IT Custodian determines that the malware on the system is malware and files have been observed to be encrypted, then the following **information** might be required: If "yes": **1. Was critical data lost? Yes/No** **2. What was lost – Type of Data** **3. Can data be restored from backup? Yes/No** **4. Cost of Ransom:** **5. Value of Data:** **6. Has Leadership determined to pay the ransom? Yes/No** If "yes": a. **Date Law Enforcement was contacted** b. **Police case #** c. **Police Point of Contact**