Quarantining Practices

Version 1.0

Author

IT Security Office (ITSO)

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Introduction

The University IT Security Office (ITSO) monitors Duke’s network and systems for security issues and vulnerabilities. Consistent with Duke’s Vulnerability Management Policy and in order to maintain network and system security, timely patching of systems is required on an ongoing basis.

Scope

Under certain circumstances--including even when timely patching is practiced but when severe vulnerabilities arise--the ITSO may need to remove vulnerable, infected or compromised machines from Duke’s network. This occurs in cases where the systems are known to pose a security threat to the rest of the Duke community. The practices associated include:
Computers, servers and other devices not patched in a timely fashion

The ITSO scans the Duke network on a regular basis to identify security vulnerabilities on servers, computers, and other devices (e.g. printers). According to Duke’s vulnerability management policy, system administrators or owners are responsible for applying security updates in a timely fashion:

1. Systems containing Sensitive data should be patched within 2 weeks of a security update addressing a Critical or High vulnerability becoming available.
2. Systems containing Restricted or Public data should be patched within 4 weeks of a security update addressing a Critical or High vulnerability becoming available.

If a vulnerable system is not patched according to the schedule above, the IT Security Office will notify the system administrator or owner and may quarantine the system within 48 hours of initial notification if the vulnerability is not addressed.

Computers, servers and other devices infected with malware or otherwise compromised

Through monitoring of Duke’s network, antivirus notifications, and system logs, the ITSO may identify systems that are infected with malware or have been compromised by an attacker. In these situations, the ITSO will take one of two actions.

1. High or Critical Security Issues

Immediately remove the system from the network and contact the system owner, and additionally for Duke owned machines, IT support for the system owner.

In this scenario, the ITSO will quarantine or remove the system from the network immediately so that the system cannot attack or harm other systems. The ITSO will then contact the system owner and IT contact. Lastly, the campus IPS will redirect attempts to access the Internet with a web browser to a quarantine page, which will provide the affected user contact details. This scenario is reserved for more severe threats including:

(a) System has been compromised by an external attacker who is actively using the system to attack other Duke systems, adversely affect Duke’s network, attack computers on the Internet, collect usernames and passwords, or is attempting to exfiltrate data from the system.
(b) System is infected with malware that has been reported by Duke’s Intrusion Prevention System as actively communicating with known attackers (e.g. participating in a Botnet), or is attempting to spread malware to other Duke machines.

2. Low to Moderate Security Issues

Contact the system owner and IT support with details of the issue, and give the system owner 48 hours from notification to address the issue before removing the system from the network.
In this scenario, the ITSO will contact the affected party first before quarantining the system. This scenario is used in less severe cases such as:

(a) Low and moderate risk security issues (e.g. spyware infections)
(b) Times when it would be unduly onerous to quarantine a machine (e.g. students during exam week).
(c) When quarantining the system would impact Duke business in a negative fashion (e.g. web presence).

The ITSO will work with the affected party to attempt to identify a mutually satisfactory remediation plan within 48 hours. If the issue cannot be addressed in the stated time frame, the ITSO may at their discretion, quarantine the machine until the issue can be resolved.

**Compromised Accounts**

Through monitoring of Duke's system mail, and authentication logs, the ITSO and OIT may identify accounts that have been compromised and are being used by attackers to log into systems. In these situations, the ITSO and OIT will take one of two actions.

1. **Manual Locking**
   In cases where the ITSO or OIT have identified a compromised account based on a reported incident or analysis of system and authentication logs, the questionable account will be referred to the OIT Service Desk.
   The Service Desk will:

   (a) Attempt to contact the affected individual.
   (b) Lock the account.
   (c) Assist the customer in resetting their password and updating CRV questions when they call the Service Desk.

   If the account is a faculty or staff account, the ITSO will also contact the appropriate IT contact in the school or department to let them know about the incident.

   In some cases, if the account is involved in an active security incident, or is part of a large security incident involving a larger number of accounts, the ITSO and Service Desk will immediately lock the account and then attempt to contact the affected party and IT contact for the affected party. The Service Desk will help the user reset their password and update CRV questions when they contact the Service Desk for assistance.

   When contacted, the affected parties will be asked if they have access to systems with Sensitive data so that access to those systems can be checked for inappropriate access.

2. **Automated Locking**
   In cases where a compromised account is being used to send spam or phishing messages from the Duke mail system, an automated task may detect the misuse and immediately quarantine the account. In these cases, the affected user will need to contact the Service
Desk who can assist with resetting their password and updating CRV questions.

1In this case a “threat” is posed to the broader community if the infected or vulnerable, unpatched system could create a foothold for an attacker to access other systems on the Duke network through the vulnerable system, or if the attacker could adversely impact the performance of Duke’s network more generally through Denial of Service attacks or other methods.