Compromised Machine Notifications

What is a compromised machine?
A compromised machine is any device that is showing signs of being infected with a virus or other malicious software. This kind of software may be relatively benign in its behavior, such as popping up annoying advertisements on your screen, or it may be incredibly dangerous and capable of stealing your financial information, attacking other devices on the network, or worse.

What are compromised machine notifications?
The EITS Office of Information Security has an automated system that incorporates security feeds from a multitude of sources. When our system detects certain network traffic patterns or host-based logs that we are confident indicate a compromised machine, the system will automatically issue a notification to the Designated Network Liaison (DNL) responsible for the IP address linked to that activity. In case of student traffic, the notices are sent to Student Technology Services (STS). Notifications for users who are employees on the wireless network will have notices sent to the DNL associated with the user's department. If patterns are detected that don't meet a confidence threshold but still may indicate a compromise, those notices are sent to the Security Operations Center, which may then forward the notices to the appropriate IT support office after further analysis.

What should I do if the machine is a system that handles sensitive information?
If you receive a notification for a machine that contains or processes sensitive information as defined by University policy, do NOT attempt to investigate or remediate, but instead contact the Office of Information Security through the EITS Help Desk at 706-542-3106.

What should I do if I get a compromised machine notice for a user that isn't in the department I work for? What if I'm not getting notifications for my subnet?
The DNL of a wired network IP is based upon BlueCat Proteus permissions - the DNLS that have control over the IP's subnet there will receive these notifications. If you are not the DNL of the IP range for which you are getting notifications, or you are not getting notifications for a subnet over which you are a DNL, please open a ticket with the EITS Help Desk to have yourself removed or added as appropriate.

What should I do if I get a compromised machine notice for a machine that isn't owned by the University?
Some notifications will involve devices that are owned by employees and not the University, especially wireless user devices. Regardless of who owns them, actively compromised machines cannot be allowed continued access to the network. The IT support for the affected employee's department is the only support available through the University in these situations. If a DNL does not wish to help a user with a personal device, the only option left is to simply block the user's device from getting on the network until such time that the device is cleaned some other way. If you do not wish to assist a user in this situation, please reply to the notification and let us know we need to block the user.

What security feeds cause notifications to be sent?
This information, and other questions, can now be found here:

https://eits.uga.edu/access_and_security/infosec/compromised_machine/

Note: You will need to use your MyID username and password to access this page.

External Links
- Office of Information Security Homepage