Tech Training: Network Isolation

Taylor’s Network Access Control device (currently PacketFence) has the ability to identify and isolate devices running malicious and/or disallowed software. It does so by monitoring packets and comparing them to its list of allowed and disallowed programs. Of special interest to students are devices identified as running malware and/or peer-to-peer software. This tutorial covers the process of assisting students to eliminate the offending software and restore their internet access.

Background

On 9/3/15, 4040 started receiving emails directly from PacketFence when a client is placed into Isolation. TJ created an Exchange Rule to move these messages to 4040 > Inbox > zManagement > Sent Items – Keep > 2016-17 > Isolation.

If a student comes to us for help with Isolation, locate the email notification that was sent to them and read it to discover:

1. Why they were isolated (P2P, malware, TOR, etc.)
2. Which device caused the isolation
3. Steps the student needs to perform to get their internet access restored

Heads up… students may come to us with a device that is in Isolation due to P2P. But it may not be the device that actually has a P2P app installed. When any student device is caught for P2P, all of that student's devices are isolated.

Check the IP Addresses. If their device is in Isolation, their device will have a 10.9.xxx.xxx IP address. Then read the PacketFence email notification to clarify why the device is in Isolation and which device caused the trouble. Whether the device is in Isolation for P2P or malware, the email notification gives the student complete instructions for getting themselves out.

- **For malware Isolation, guide them through the Malware Removal Checklist.**
- **For P2P Isolation, send them to their hall director.**

Peer-To-Peer (P2P) Isolation

- Severity: High. This is a policy breach. Student cannot self-remediate. Student Development is involved.
- CS Role: Minor, if any. The most we can do is look through their list of installed applications and try to identify those that might use P2P technology. Make sure you’re working with the right device!
  - Validate - if they follow the steps, they will be removed from Isolation
  - Educate - find the appropriate PacketFence emails, read it to the student if necessary, explain the steps and that TUCAN Policies they agreed to state 'no P2P on campus'
  - Solve - guide them through identifying and uninstalling the offending apps if requested. Then point them to their hall director.
- Removal from Isolation:
  - Student speaks with hall director
  - Hall director responds to PacketFence email
  - IT removes student from Isolation

NOTE: CS cannot request removal from Isolation for P2P. Do not escalate a ticket to IT for P2P Isolation! Policy breaches are between the student, Student Development, and IT. The student must work through their hall director. Client Services plays no role.

Malware

- Severity: Mild. There is no policy breach. Student can self-remediate.
- CS Role: Involved, if requested. Make sure you're working with the right device!
    - Validate - if they follow the steps, they can get themselves out of Isolation.
    - Educate - find the appropriate PacketFence emails, read it to the student if necessary, explain the steps, 3 Enable Network opportunities (2 hours each).
    - Solve - guide them through the Malware Removal Checklist, **initial** the Check List as they complete steps, enter and resolve a ticket for the malware removal process, give completed Check List to TJ.
- Removal from Isolation – Enable Network Available:
    - Complete normal malware removal process
    - Student clicks Enable Network
        - PacketFence waits 2 hours to recheck the device for malware
    - One ticket:
        - Computer > Malware: Resolve the ticket with you as the Assigned Tech
- Removal from Isolation – Enable Network Unavailable:
    - Complete normal malware removal process
    - Enable Network option not available
    - Two tickets:
        - Computer > Malware: Resolve the ticket with you as the Assigned Tech
        - Network Access > Isolation – IT: IT will remove the device and resolve the ticket
            - Created only after malware is removed
            - PacketFence waits 2 hours to recheck the device for malware

Client Services no longer performs the malware removal process for students. We provide them instructions in the form of a tutorial and guidance if they have trouble. Sit them down, briefly walk them through the process (give them a printed copy of our Malware tutorial), and tell them to let us know if they have trouble. We will gladly guide them through the process. Most will want guidance with Add/Remove Programs. They'll also want to borrow our thumb drives with CCleaner and Malwarebytes on it. And yes, we still complete a Malware Checklist. Be sure to turn completed checklists in to TJ.