Wannacry

ATTEMPTS at REMEDIATION:

1) Identify ip/Mac of system being remediated and remove quarantine in TSC tools (https://utnetdb.gw.utexas.edu)

   IP Search

2) Firewall

Blocks inbound traffic on port 445, which should buy us enough time to patch the OS. This is being applied to all CNS OIT imaged workstations as of 2017/05/19.

   Script: https://utexas.box.com/s/o2xa0ssrz70vs2hgslceq2ne8fu6vc

   Block - Click ‘Yes’ when prompted

   Unblock - Click ‘No’ when prompted

3) Run updates on system

Windows Updates tool under Control Panel or Settings

or

Individual patches

\cns-srv-sccm.austin.utexas.edu\wannacry

VERIFICATION:

4) Run nmap Against it

https://www.tecklyfe.com/nmap-nse-script-detect-wannacry-ms17-010-vulnerability/

```
    sudo nmap -sC -Pn -p445 --script smb-vuln-ms17-010.nse x.x.x.x
```

5) Patch check

This does not patch the system, it only shows which hotfix(es) have been applied

Unknown Attachment

Collect Netcontact detail:(bold are examples)
location GEA 403
aco GEA0237
ip (128.83.90.20,)
name dhcp-128-83-90-20.he.utexas.edu
description Instrumentation controller/admin computer/deans staff computer/research station/etc
ut_tag 868354
serial 12345678
priority n (options: n=normal, i=important, c=critical)
category 3 (options: 1, 2, 3)
primary_user EID
contacts tech EID
contact_flags

**Alternative (UNTESTED) to pushing updates in the background:

These PowerShell commands need to be run with Admin rights.

Stop-Service -Name 'wuauserv' -Force
Remove-Item -Path 'C:\Windows\SoftwareDistribution' -Recurse -Force
sleep 10
Start-Service -Name 'wuauserv'

David Newsom
Computer Services
McCombs School of Business