PREPARE TO MAKE YOUR OWN LUCK

MODERATOR: John Felker
Director, Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)

PANELISTS: Bradley Nix
NCCIC Senior Advisor

Jermaine Roebuck
Deputy Division Director, NCCIC
Hunt and Incident Response Team
**RSAC**

**Malware Execution**
- **Malware executes**
- **Installs as service** (to maintain presence)

**ATTEMPTS CONNECTION TO KILL SWITCH DOMAIN**
- **Attempts connection to kill switch domain**
- **Successful?**
  - **Yes**
    - Malware exits, no infection
  - **No**
    - **Installs as service** (to maintain presence)

**Scan for Devices that use SMB**
- **Scan for devices that use SMB**
- **Found?**
  - **Yes**
    - **Attempt SMBv1 exploit**
    - **Successful?**
      - **Yes**
        - **Upload & execute dropper**
      - **No**
        - **Extract ransomware component**
  - **No**
    - Continue scanning

**Extract Ransomware Tor or Bitcoin config**
- **Extract ransomware Tor or bitcoin config**
- **Setup encryption process**
- **Begin encrypting user data**
- **Add .WNCRT/1 extension**

**Connect to CZ via Tor**
- **Connect to CZ via Tor**
- **Delete shadow volumes (backup)**
- **Delete shadow volumes**

**Display Ransom note as wallpaper**
- **Display ransom note as wallpaper**

**Additional notes:**
- `b. wncrt - desktop wncrt`
- `c. wncrt - tor config`
- `d. wncrt - AES key for decrypting DLL`
- `f. wncrt - ?`
- `g. wncrt - Ransomnote`
For more information:
www.us-cert.gov/ransomware

Questions?
Email: nccicccustomerservice@hq.dhs.gov
Phone: 888-282-0870