CIRT Playbook Battle Card: **GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Examine file shares for loose/open privileges
4. Maintain Antivirus/EDR application updates
5. Create network segmentation
6. Log traffic between network segments
7. Incorporate threat intelligence
8. Incorporate deception technology
9. Perform routine inspections of asset backups
10. Validate proper functionality
11. Confirm backups are free of malware
12. Establish ability to pay ransoms w/cryptocurrency
13. Obtain decryption keys for ransomware variants
14. Confirm cybersecurity insurance coverages
15. Conduct ransomware simulations
16. Conduct phishing simulations
17. Conduct user awareness training
18. Conduct response training (this PBC)

(I) Identification

1. Monitor for:
    a. Ransomware notes/messages
    b. Unusual file extensions or malicious extensions
    c. User reports of files being corrupt or not readable
    d. Emails with suspicious attachments
    e. Unusual DNS traffic
    f. High velocity renaming of files
    g. CPU spikes on file sharing systems
    h. Unusual userland executable binaries
    i. Anomalous network connections on hosts
    j. Firewall denies to well known file sharing ports
    k. Network connections to known C2 and exploit kit locations
    l. Use of TOR or I2P
2. Investigate and clear ALL alerts of possible ransomware
    a. IDS/IPS
    b. Antivirus/EDR
    c. Threat intelligence
    d. Deception technology

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Locate and isolate the assets responsible for encrypting files
5. Isolate impacted file sharing systems
6. Close the attack vector
7. Fortify non-impacted file sharing systems
8. Fortify non-impacted critical assets
9. Issue perimeter enforcement for known threat actor locations
10. Deploy EDR hunter/killer agents and terminate offending processes

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Re-image impacted assets
4. Inspect all assets for IOC consistent with the attack profile
5. Inspect user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery
7. Implement newly obtained threat signatures

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore from known clean backups
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Avoid opening email and attachments from unfamiliar senders
4. Avoid opening email attachments from senders that do not normally include attachments

Notes:

1. Report cybercrime: https://www.ic3.gov/default.aspx
2. Paying ransoms is discouraged but should be a contingency available to executives (SEE Preparation #12)

GUARDSIGHT