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

(I) Identification

1. Monitor for:
   a. Ransomware notes/messages
   b. Unusual file extensions or maliciousextensions
   c. User reports of files being corrupt or notreadable
   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 sharingports
   k. Network connections to known C2 andexploit 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

References:

1. MITRE ATT&CK Technique T1486: https://attack.mitre.org/techniques/T1486/
2. Paying ransoms is discouraged, but it should be a contingency available to executives (SEE Preparation #4 and #6).

Resources:

➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT