Version: 1.03
Published: 12/23/19
Updated: --

Emergency Support Function 17
Statewide Cyber Incident Management

Cyber Attack Prevention

Critical Task List for All Government Entities

This document is solely for the purposes of providing urgent assistance to all Government Entities (GE) within the State of Louisiana. The specific tasks defined below were crafted with the specific goal of addressing the current risks facing GEs across the state. These tasks are intentionally specific, tactical in nature, and should not be considered the only actions required to protect data or prevent unauthorized access to technical resources. However, completing these critical tasks in an urgent manner will greatly improve the chances of preventing a potential cyberattack and ensuring organization can continue critical government functions.

Critical Note: In the event of a suspected Cyber Attack – **DO NOT POWER OFF** from any server or workstation, as this causes more harm than good. You should however; remove network connectivity from any devices you suspect is infected with malware as soon as possible and reset any user's password that was using the infected device.

Phase One: Critical Security Readiness

There is a very high likelihood malicious events may be happening in your environment already. Any indication of the following events should be treated very seriously as a precursor to a larger attack.

❖ Diligently review the following systems as described below:

☐ **Intrusion Prevention System** (IPS)

- All GEs should have an IPS deployed at the edge of the network, behind the firewall.
- *** More importantly *** - The IPS should be properly configured to:
  - ☐ automatically download content and signature updates on a daily basis;
  - ☐ block all critical and high severity threats; and
  - ☐ Generate alert notification (emails) for any detections of critical, high, or medium severity threats.
- *** Additionally *** - Your prior IPS logs should be reviewed to ensure no matches for following malware :
  - ☐ Trickbot, Emotet, or Lokibot

☐ **Firewall**

- All GEs should have a firewall at the edge of the network.
- *** More importantly *** - The firewall should be properly configured to:
  - ☐ send connection logs to a syslog server (minimum 90 days retention);
  - ☐ deny any external connections to internal systems over TCP 3389, 22, & 445;
  - ☐ allow internal systems to only communicate with internet resources over the specific ports required.
- *** Additionally *** - Your prior firewall logs should be reviewed to ensure no matches for following:
  - ☐ Attempted outbound traffic over ports 445, 447, 449, 2869, 5435 5985, 5986, 8082, 8335, 47001

☐ **Domain Controllers**

- **Extremely important** that all GEs properly configure and protect the Microsoft Domain Controllers
  - ☐ **All GE Domain Controllers** should have "Next Gen" Antivirus installed and configured
    - CarbonBlack, CrowdStrike, SentinelOne, Cisco AMP, Palo Alto Traps, or Cylance
    - ☐ Properly configured to take action on malicious events and generate notification on detection.
  - ☐ **All GE Domain Controllers** should be single purpose and ***not*** be used for DHCP, Web Servers, File Servers, Print Servers or FTP Servers.
  - ☐ All GEs should limit Domain Admin accounts to the absolute minimum amount of staff needed to perform admin duties.
  - ☐ All GEs ***should not*** grant Domain Admin to any service accounts.

☐ **Internet Content Filters**

- **Important Note**: "Secure DNS" solutions, similar to "OpenDNS" or Cisco's Umbrella Service do add value to an environment but do not remove the critical need to have proper filtering for outbound internet connections.
- All GEs should have a solution to preform inline inspection and filtering of outbound connections to the internet.
- *** Most importantly *** - block outbound connections to:
  - ☐ Unregistered Web Sites
  - ☐ "Malicious content", "Proxy Avoidance", and "Hacker tools"
  - ☐ Traffic to "pastbin.com" from any servers
  - ☐ LogMeIn, Bomgar, or TeamViewer
  - ☐ **Take particular care in reviewing traffic sourcing from any windows domain controllers, as any identified events sourcing from a domain controller should be considered a critical alarm requiring additional follow up.**

Phase Two: Review Your Environment for These Events

There is a very high likelihood malicious events are happening in your environment already. Any indication of the following events should be treated very seriously as a precursor to a larger attack.

- Any recent events matching the following description:
  - Unauthorized use of PowerShell scripts on domain controllers.
  - Unauthorized modifications to Microsoft Domain Group Policy Objects (GPO)s
  - Unexpected users found in the "Domain Admins" user group membership list.
  - Consistent Administrative user lockouts.
  - Anti-Virus Services paused/stopped or outdated signature updates
  - Installed services with unusual names/created scheduled tasks with unexpected names or paths
  - Creation of new user accounts with broad privileges
  - Any of the following usernames: RepatriateQuery, Menthol.Notary5001, Anisati2918, Reform63435, Pharmacist 1690, Mistaking 5570, Overshadow 4957, Restock 5814, Resist 386
  - Ensure systems are patched in reference to CVE-2014-0324, CVE-2017-8759, & CVE-2017-11882.

❖ Once all above actions in Phase Two have been completed:

- ○ **If any events defined above have been found in your environment – you are likely at critical risk.**
  - **YOU ARE STRONGLY ENCOURAGED TO REPORT FINDINGS TO THE STATE'S FUSION CENTER (number below)**
    - **NOTE**: The State will not release any information about your institution related to reporting this, or cause of current posture. We will diligently work with you and we feel confident that if engaged at this stage we can prevent the potentially imminent attack on your organization.

❖ If you did not identify and events defined above please proceed to Phase Three.

Contact Information:

If you believe you have already become a victim of a cyber-attack, the following steps are vital to minimizing service interruption and ensuring the proper evidence collection process is followed:

❖ **DO NOT** Power Off Clients or Servers

❖ **DO** modify firewall to prevent outbound traffic

❖ **DO** disconnect physical network connections (if needed)

❖ Contact Louisiana State Police Fusion Center:
- ○ **1-800-434-8007**
- ○ **LaFusion.Center@la.gov**

Phase Three: Additional Cyber Hygiene

- Ensure account password policy is configured to enforce password change at a minimum every 90 days.

- Ensure you have configured proper configuration to the following systems to ensure logs are being generated and retain for at least 90 days

    - Firewalls, Intrusion Detection Systems, Domain Controller Windows Events, and public facing web applications.

    - Additional guidance for Audit Logging technical requirements can be found in the State's Information Security Policy located here: https://www.doa.la.gov/OTS/InformationSecurity/LA-InfoSecPolicy-v1.01.pdf

- Ensure your staff users are not running local as local administrators while also connecting to the internet or reading email.

    - Understanding that this may be a difficult transition for many different reasons, there are few things more effective from preventing malware gaining the initial foothold required to launch a cyber-attack.

- Use VPNs for any and all remote network connections (especially as it relates to private vendor \ partner connections)