Recent Cyber Attacks in Louisiana

- 7 School Systems - July 2019
- Parish Governments – August 2019 – January 2020
- Law Enforcement Agencies – August 2019 – January 2020
- Institute of Higher Education – August 2019
- State of Louisiana – November 2019
- Baton Rouge Community College – December 2019
- City of New Orleans – December 2019
- New Orleans Convention Center – January 2020
- ITI Technical College in Baton Rouge – February 2020
15 Emergency Support Functions (ESF)

1. Transportation
   Department of Transportation

2. Communications
   National Communications System

3. Public Works and Engineering
   U.S. Army Corps of Engineers

4. Firefighting
   Department of Agriculture/Forest Service

5. Emergency Management
   Federal Emergency Management Agency

6. Mass Care, Housing, Human Services
   Department of Homeland Security
   American Red Cross

7. Resource Support
   General Services Administration

8. Public Health and Medical Services
   Department of Health and Human Services

9. Urban Search and Rescue
   Federal Emergency Management Agency

10. Oil and Hazardous Materials Response
    Environmental Protection Agency

11. Agriculture and Natural Resource
    US Department of Agriculture/Department of the Interior

12. Energy
    Department of Energy

13. Public Safety and Security
    Department of Homeland Security/Justice

14. Community Recovery, Mitigation, and Economic Stabilization
    U.S. Small Business Administration

15. External Communications
    Federal Emergency Management Agency
Cyber Event Notification

Cyber Event
L5 (Emergency) – Poses an imminent threat to the provision of wide-scale CI services, state gov’t stability, or the lives of LA citizens
L4 (Severe) – Likely to result in a significant impact to public health or safety
L3 (High) – Likely to result in a demonstrable impact to public health or safety
L2 (Medium) – May impact public health or safety

First Notified
L3 | L4 CE
First Notified
L2 | L5 CE

Parish OHSEP Office
Fusion Center Via: DPS Hotline
Assess: Triage Event

No Assistance Required
(File for Intel Value / Trend Analysis)

Assistance Required
1) LE Only
2) Off Site Consultation
3) On-Site Consultation
4) Resource Request

Notify OHSEP OMs With Recommended Action
ReadyOP
Notify ESF-17 for S.A. (Actions 1 – 4)

Local OHSEP

Cyber Response Assets
1. LSP – Evidence Team / Critical Infrastructure
2. LANG – Incident Response Teams (CPT, DCO-E, C-DIRT)
3. OTS – Incident Response Teams

GOHSEP Operations
WebEOC
Cyber Quick Response Team (CQRT)
LSP OTS LANG
Resolved Not Resolved
AAR AAR
Resolved Not Resolved
ESF-17 CIOCC MS-ISAC
State Incident Response Teams
DHS | CIOCC | US-ICS | US-CERT | FBI | NORTHCOM
EMAC

Fusion Center Notify CIOCC / MS-ISAC regarding all L4 and L5 incidents and any L2 or L3 event with extenuating circumstances based on public impact
## Recovery Planning Considerations

<table>
<thead>
<tr>
<th>Category</th>
<th>Self Assessed Current Profile</th>
<th>Assessed Current Profile</th>
<th>Target Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management (ID.AM)</td>
<td>Tier 1</td>
<td>Tier 1.3</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Business Environment (ID.BE)</td>
<td>Tier 2</td>
<td>Tier 2.2</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Governance (ID.GV)</td>
<td>Tier 1</td>
<td>Tier 1.4</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Risk Assessment (ID.RA)</td>
<td>Tier 1</td>
<td>Tier 1.3</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Risk Management Strategy (ID.RM)</td>
<td>Tier 1</td>
<td>Tier 1.2</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Supply Chain Risk Management (ID.SC)</td>
<td>Tier 1</td>
<td>Tier 1.5</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Identity Management, Authentication and Access Control (PR.AC)</td>
<td>Tier 3</td>
<td>Tier 2.4</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Awareness and Training (PR.AT)</td>
<td>Tier 2</td>
<td>Tier 1.9</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Data Security (PR.DS)</td>
<td>Tier 1</td>
<td>Tier 1.2</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Information Protection Processes and Procedures (PR.IP)</td>
<td>Tier 2</td>
<td>Tier 1.9</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Maintenance (PR.MA)</td>
<td>Tier 2</td>
<td>Tier 1.7</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Protective Technology (PR.PT)</td>
<td>Tier 2</td>
<td>Tier 1.9</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Anomalies and Events (DE.AE)</td>
<td>Tier 1</td>
<td>Tier 1.7</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Security Continuous Monitoring (DE.CM)</td>
<td>Tier 2</td>
<td>Tier 1.9</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Detection Processes (DE.DP)</td>
<td>Tier 1</td>
<td>Tier 1.6</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Response Planning (RS.RP)</td>
<td>Tier 1</td>
<td>Tier 2.0</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Communications (RS.CO)</td>
<td>Tier 1</td>
<td>Tier 1.2</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Response Analysis (RS.AN)</td>
<td>Tier 2</td>
<td>Tier 1.7</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Mitigation (RS.MI)</td>
<td>Tier 2</td>
<td>Tier 1.9</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Improvements (RS.IM)</td>
<td>Tier 1</td>
<td>Tier 1.8</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Recovery Planning (RC.SP)</td>
<td>Tier 2</td>
<td>Tier 2.0</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Improvements (RC.IM)</td>
<td>Tier 2</td>
<td>Tier 2.0</td>
<td>Tier 3</td>
</tr>
<tr>
<td>Communications (RC.CO)</td>
<td>Tier 1</td>
<td>Tier 2.1</td>
<td>Tier 3</td>
</tr>
</tbody>
</table>
Recovery Planning Consideration

- Identify Work Functions that Require IT
- Identify Criticality of Each Function
- Identify Maximum Tolerable Downtime
Ryuk Ransomware After Action Report

Findings by Major Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>7</td>
</tr>
<tr>
<td>Operations</td>
<td>23</td>
</tr>
<tr>
<td>Outreach / Protective Measures</td>
<td>2</td>
</tr>
<tr>
<td>Situational Awareness / Reporting</td>
<td>8</td>
</tr>
<tr>
<td>Forensics</td>
<td>6</td>
</tr>
<tr>
<td>Public Affairs</td>
<td>10</td>
</tr>
<tr>
<td>Legal</td>
<td>5</td>
</tr>
<tr>
<td>Local Restoration and Remediation</td>
<td>11</td>
</tr>
</tbody>
</table>
Ryuk Ransomeware Lessons Learned

- You need to have a plan
- Machines that were compromised had Local Admin privileges
- Do not re-image an impacted machine until forensics can be captured
  - Live Memory
  - Allows remediation course of action development
- Backups were not segregated from the network
- Test your ability to recover your data
  - Legacy Systems
Ryuk Ransomware Lessons Learned

• Establish short-term and long-term recovery goals
  • Prioritize systems

• Provide your employees with cyber awareness training

• Your Public Affairs personnel need to have a base knowledge on cybersecurity

• Develop a reporting format to keep senior management informed

• Need to remove the stigma of being a victim of a cyber attack
What You Can Do

• Develop, Update and Test Your Recovery Plan
• Identify Critical IT Functions and Establish Priorities of Effort
• Know What Resources are Available to You
  • State
  • Federal
• Get Involved
  • InfraGard
• Make Cybersecurity Part of the Organizations Culture