Group 2: SITREP #1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Incident Report / SITREP #2017-Month-Report#** | | | | | | | | |
| **Incident Detector’s Information** | | | | | | | | |
| **Date/Time of Report** | 11/13/2020 | | | | | | | |
| **First Name** | Group | | | | | | | |
| **Last Name** | 2 | | | | | | | |
| **OPDIV** | IT Department | | | | | | | |
| **Title/Position** | Digital Forensic Examiner and Incident Response Professional | | | | | | | |
| **Work Email Address** | N/a | | | | | | | |
| **Contact Phone Numbers** | *Work N/A* | | | *Government Mobile N/A* | | *Government Pager N/A* | | *Other N/A* |
| **Reported Incident Information** | | | | | | | | |
| **Initial Report Filed With (Name, Organization)** | IT Department | | | | | | | |
| **Start Date/Time** | 11/13/2020 | | | | | | | |
| **Incident Location** | Raveton Ransomware Infection | | | | | | | |
| **Incident Point of Contact (if different than above)** | Group 2 – Team Australia | | | | | | | |
| **Priority** | Level 1 | | | | | | | |
| **Possible Violation of ISO/IEC 27002:2013** | YES. Security controls were not implemented | | | | | | | |
| **Privacy Information - ISO 27000 (Country Privacy Act Law)** | * The incident was a violation of ISO 27000 * Targets suffered an adverse effect * The ransomware attack was intentional by the hackers. * PII - personally identifiable information was not used maliciously | | | | | | | |
| **Incident Type** | * A ransomware attack. * The incident created denial of service (DoS) and delays. * Caused some exposure of information * Increased notoriety for the attackers. * There is the theft of information technology resources. * Some financial resources lost | | | | | | | |
| **US-CERT Category** | * DoS * Unauthorized Access * Ransomware attack | | | | | | | |
| **CERT Submission Number, where it exists** | All relevant documents submitted to management | | | | | | | |
| **Description** | Attendees were denied access into their computers | | | | | | | |
| **Additional Support Action Requested** |  | | | | | | | |
| **Method Detected** | User Notification and IDS | | | | | | | |
| **Number of Hosts Affected** | Attendees and HR machines | | | | | | | |
| **OPDIV / Department Impact** | IT department – HR department | | | | | | | |
| **Information Sharing** | US-CERT collaborates with federal agencies, private sectors, research community, state and local government, and international entities. | | | | | | | |
| **System** | Summit Computers | | | | | | | |
| **Status** | Resolved | | | | | | | |
| **Attacking Computer(s) Information** | | | | | | | | |
| **IP Address / Range** | | **Host Name** | **Operating System** | | **Ports Targeted** | | **System Purpose** | |
| **192.168.10.112** | |  | HTTPS | | 1835 | | Ransomware | |
|  | |  |  | |  | |  | |
| **Victim's Computer(s) Information** | | | | | | | | |
| **IP Address / Range** | | **Host Name** | **Operating System** | | **Ports Targeted** | | **System Purpose** | |
| **192.168.10.201** | | SSDP | HTTPS | | 80 | | HR Department | |
|  | |  |  | |  | |  | |
| **Action Plan** | | | | | | | | |
| **Action Description** | Company shared folders were encrypted by hackers with a ransomware | | | | | | | |
| **Requestor** | Upper management | | | | | | | |
| **Assignee** | Group 2 – team Australia | | | | | | | |
| **Time Frame** |  | | | | | | | |
| **Status** | Impacted computers are being examined | | | | | | | |
| **Conclusion / Summary** | | | | | | | | |
| **Entities Notified** | Upper management | | | | | | | |
| **Resolution** | The affected computers were examined. Encrypted folders were decrypted. The infected files were decrypted when the IT team cracked the password which resulted into no ransom being paid. | | | | | | | |