|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Incident Report / SITREP #2020-November-Report#2** | | | | | | | | |
| **Incident Detector’s Information** | | | | | | | | |
| **Date/Time of Report** | 11/19/2020 | | | | | | | |
| **First Name** | Group 2 | | | | | | | |
| **Last Name** | Australia | | | | | | | |
| **OPDIV** | IT Department | | | | | | | |
| **Title/Position** | Cybersecurity Incident Response Professional | | | | | | | |
| **Work Email Address** | Group2\_Ausi@fvey.com | | | | | | | |
| **Contact Phone Numbers** | Work: 555-123-4567 | | | Gov Mobile:  555-456-7890 | | Government Pager: n/a | | Other: n/a |
| **Reported Incident Information** | | | | | | | | |
| **Initial Report Filed With (Name, Organization)** | HR Manager / CISO | | | | | | | |
| **Start Date/Time** | 11/19/2020 | | | | | | | |
| **Incident Location** | FVEY Global Economic Summit | | | | | | | |
| **Incident Point of Contact (if different than above)** | Group 2 – Team Australia | | | | | | | |
| **Priority** | Level 1 | | | | | | | |
| **Possible Violation of ISO/IEC 27002:2013** | YES  12.0 – Operations Security  12.2 – Protection from Malware  12.5 – Control of Operational Software | | | | | | | |
| **Privacy Information - ISO 27000 (Country Privacy Act Law)** | Was the incident a violation of ISO 27000? ***Yes***  Did the target suffer an adverse effect? ***Yes***  As a result, was the OPDIV the direct or proximate cause of the adverse effect? ***Direct***  Was the violation intentional or willful? ***Intentional***  Was the personally identifiable information used maliciously? ***Yes***  INCLUDE PRIVACY IMPACT BELOW:  ***Privacy Act 1988 - Applies to all government and private sector entities and defines how personal and sensitive information can be collected, processed and/or transferred to other entities.*** | | | | | | | |
| **Incident Type** | Reveton Ransomware Attack (bitcoin), Malware Attack, alter or destroy information | | | | | | | |
| **US-CERT Category** | Denial of Service (DoS) – the attacker maliciously intended to interrupt authorized user access to the computer network.  Unauthorized Access – the attacker gained unauthorized access to the computer network to alter/destroy information and is now requesting ransom in the form of bitcoin  Malicious Code - Ransomware | | | | | | | |
| **CERT Submission Number, where it exists** | CERT Australia – the national computer emergency response team provides advice and support or cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest. | | | | | | | |
| **Description** | Malware was used to launch a ransomware attack in an attempt to ransom crypto currency (bitcoin) from members of the FVEY nations. | | | | | | | |
| **Additional Support Action Requested** | n/a | | | | | | | |
| **Method Detected** | IDS and User Notification – The US reported that data exfiltration was detected in their intrusion detection system. | | | | | | | |
| **Number of Hosts Affected** | 2 – Summit Attendees and HR Benefits Coordinator | | | | | | | |
| **OPDIV / Department Impact** | National Security / Information Security | | | | | | | |
| **Information Sharing** | Entities within Five Eyes (FVEY) Alliance can share incident data. | | | | | | | |
| **System** | Australia’s Global Economic Summit Secure Comms Server | | | | | | | |
| **Status** | Ongoing | | | | | | | |
| **Attacking Computer(s) Information** | | | | | | | | |
| **IP Address / Range** | | **Host Name** | **Operating System** | | **Ports Targeted** | | **System Purpose** | |
| 192.168.10.112 | |  | HTTP | | 1835 | | Ransomware – store/transfer ransomware via attack script | |
| 23.23.99.139 | |  | HTTP | |  | | Malicious Infrastructure | |
| **Victim's Computer(s) Information** | | | | | | | | |
| **IP Address / Range** | | **Host Name** | **Operating System** | | **Ports Targeted** | | **System Purpose** | |
| 192.68.10.201 | |  | HTTP | | 80 | | HR Department – process Australia’s HR data Secure Network | |
| 84.200.69.80 | |  | HTTP | | 80 | | Secure Network | |
| **Action Plan** | | | | | | | | |
| **Action Description** | Team Australia will not comply with the bitcoin ransom demand of the attacker. The malware signature will be added to the IDS/IPS. Impacted files will be restored from a good backup. Antivirus software and firewalls will be installed along with scanning and filtering of email servers. Ensure that all systems and software are up to date with applicable patches. Using VirusTotal and AlienVault tools, we reviewed the hash from the indicator report (see below). | | | | | | | |
| **Requestor** | CISO | | | | | | | |
| **Assignee** | Group 2 – Team Australia – Cybersecurity Incident Response Professionals | | | | | | | |
| **Time Frame** | 11/19/2020 | | | | | | | |
| **Status** | Ongoing | | | | | | | |
| **Conclusion / Summary** | | | | | | | | |
| **Entities Notified** | CISO | | | | | | | |
| **Resolution** | Cryptocurrency not paid. Server recovered from backups and malware isolated and blocked using SNORT. | | | | | | | |

References

ISO (2013). ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls. Retrieved from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>

Kaspersky Lab (2020). What is Malicious Code? Retrieved from <https://www.kaspersky.com/resource-center/definitions/malicious-code>