## 

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Incident Report / SITREP #2020-November-Report#2** | | | | | | | | |
| **Incident Detector’s Information** | | | | | | | | |
| **Date/Time of Report** | 11/25/2020 | | | | | | | |
| **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)** | CISO/Cos | | | | | | | |
| **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 | |
| **Fact Finding** | | | | | | | | |
| **Findings Description** | * 1 web developer is still unaccounted for, for more than five days. * 1 member of the Server Operations team is still unaccounted for, for more than five days. * Server team discovered a thumb drive laying inside the rear panel of a hardware encloser. * What appears to be passwords were found on a sticky note stuck to the inside of a laptop known to be used by Ms. Grascholtz and others. * The thumb drive was found to have 4 partitions with only one containing data. * A word document claiming to be a resignation letter from Ms. Grascholtz was on one of the partitions of the thumb drive. * Four thumb drives matching the one found in the back of the server were located at a workstation known to be used by Ms. Grascholtz and others. | | | | | | | |
| **Requestor** | CISO | | | | | | | |
| **Assignee** | Group 2 – Team Australia – Cybersecurity Incident Response Professionals | | | | | | | |
| **Time Frame** | 11/19/2020 | | | | | | | |
| **Status** | Ongoing | | | | | | | |
| **Thumb Drive Document** | | | | | | | | |
| **Entities Notified** | CISO | | | | | | | |
| **Content** | The resignation letter claiming to be from Ms. Grascholtz states that there was an extortion attempt made against her to infect the computers on the network. After this interaction it is claimed that Ms. Grascholtz attempted to contact management to report the incident and she was denied help resolving the issue. | | | | | | | |
| **Conclusion** | This document can not be trusted at this time as being the true intentions of Ms. Grascholtz. Just because Ms. Grascholtz’s name appears on the document it alone does not prove she wrote the document.  The thumb drive was not located in her workstation as would be expected if she intended to send the document herself. | | | | | | | |
| **Actions** | Direct managers need to be interviewed to try and validate the statements made concerning reporting the extortion attempt.  Meta Data should be examined to find data/time of creation, last edits, and owner of the document.  Previous documents and emails sent by Ms. Grascholtz should be examined to identify how Ms. Grascholtz sings her documents. Found document ends with Penelope Anne rather than Penelope Grascholtz. | | | | | | | |
|  | **Thumb Drives at Workstation** | | | | | | | |
| **Entities Notified** | CISO | | | | | | | |
| **Thumb Drive found at workstation conclusion** | Findings of the same type of thumb drives at the workstation that was used by multiple users and no statements claiming to see Ms. Grascholtz’s in possession of any thumb drives. | | | | | | | |
| **Actions** | System logs need to be checked to see if at any time Ms. Grascholtz’s account mounted a thumb drive. | | | | | | | |
|  | **Passwords Found** | | | | | | | |
| **Significance** | The passwords found on the workstation contained the password (Fast246) to decrypt the document (resignation letter) discovered on the thumb drive in the back of the server.  Two of the other passwords were mentioned in the resignation letter as the passwords needed to decrypt the file encrypted by the ransomware. | | | | | | | |
| **Assumptions** | The password Fast246 does not fit the other passwords due to its simplicity.  This simplicity may have been to ensure that it could be decrypted easily. | | | | | | | |
|  | **Thumb Drive Partitions** | | | | | | | |
| **Significance** | The partitioning of the thumb drive would lead one to believe that concealment of data would have been the purposes behind the action.  Windows 10 does not recognize the partitions on a thumb drive thus leading one to believe the creator knew Linux or another OS other than Windows. | | | | | | | |
|  | **Ms. Grascholtz’s Browser History** | | | | | | | |
| **Significance** | The list of websites visited by Ms. Grascholtz’s would indicate a person who was seeking information on ransomware and how to report it. There was an instance of going to Facebook in the browsing history but not to any persons’ page. The other pages were about Corona virus testing and travel. | | | | | | | |
| **Assumptions** | The visiting of Corona virus testing and travel pages may indicate someone gathering information to plan to travel. This in conjunction with the sites for reporting of extortion could be the actions of someone who is fearful and planning on traveling to get away from someone. | | | | | | | |
|  | **Reventon Malware link to Ms. Grascholtz’s** | | | | | | | |
| **Assumptions** | Currently there is not sufficient evidence to link Ms. Grascholtz to the introduction of the Reventon malware. There were no witnesses placing the thumb drives in possession of Ms. Grascholtz. There is no digital forensics proving that Ms. Grascholtz was the one who partitioned the thumb drives or wrote the resignation letter found on it. | | | | | | | |
|  | **Other Insider Suspect** | | | | | | | |
| **Assumptions** | There is reason to not discount the possibility of another insider besides Ms. Grascholtz. There are two individuals that are still unaccounted for that held positions that would allow access to the systems need to infect the network as well as place information that would point to Ms. Grascholtz. | | | | | | | |
|  | **Next Actions** | | | | | | | |
| **Actions** | * The two missing employees need to be found. * The accounts of both missing employs need to be locked to prevent any further logins. * Any unauthorized accounts that are found need to be locked and forensics will investigate them. * The thumb drives should be digitally investigated to find out what they have been used for and by who. * The system logs should be checked to find any instances of the found thumb drives being mounted to the system. * Look into the labeling of the thumb drives and if they are logged out by users. * The meta data from the resignation data will need to reviewed for information. * Ms. Grascholtzs’ managers need to be interviewed to verify claims she came to them to report the extortion attempt. * The persons next to the workstation where the passwords were found need to be interviewed to get a timeline of Ms. Grascholtz use of the workstation. | | | | | | | |

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>