|  |  |
| --- | --- |
| **Incident Report Information** **Incident Ticket Number:** #IS214-310597 **Category:** System **Sub-category:** Google Slide **Priority:** High **Status**: Closed | **Contact Information for this Incident** **Name:** Kenny Kwek  **Title:**  IT Operations Manager & Support Manager  **Mobile Phone:**  9620 1737  **Email address:** kenny.kwek.2017@sis.smu.edu.sg |

# **Description of the incident:**

On 17 March 2019, at approximately 8.17am, the team received an incident ticket via IS214 ESM Ticketing system that there is a ransomware attack on the SCP’s Google Slide 2. The team conducted a verification check on SCP and find it to be genuine. The team has conducted a temporary fix to the situation by replacing the ransomware slides with a spare google slide which the team has backed up. This is to protect the company's brand and reputation. The incident was believed to have happened at approximately 12.00am on 17 March 2019. News that the previous version of URL is classified as malicious on 18 March 9.02a.m. A new version of replacement was given by Product Manager on 19 March 12.29pm. Tier 3 immediately execute the replacement.

The team will continue investigating this incident and would require the assistance of Fantasma Web Services.

# **Impact to business agreed service levels:**

High. Incident has escalated into a problem as it has affected many users. Google Slide is temporarily replaced with a new version which was sent by Product Manager. No data was involved during this incident

(Refer to the “*Systems affected by Incident”* section for technical analysis of incident.)

|  |  |
| --- | --- |
| **Scope of Incident** | |
| **Number of sites affected by the incident:** | 3 |
| **Approximate number of systems affected by the incident:** | 1 |
| **Approximate number of users affected by the incident:** | > 50 |
| **Are business partners affected by the incident?**  **(If Yes, please describe)** | No |
| ***Additional information:*** As the affected web server is for the sole purpose of displaying the web page on the latest launch updates of the Smart Contract Product, no user accounts or administrative accounts were affected. | |

# 

# **Additional Personnel notified of Incident**

Loc Hguyen Huynh Chief Operating Officer

Wendy Tan & Michelle Kan Product Manager

Ong De Lin Quality Assurance

Lee Jia Ern, Janell Tier 1 - Communication

Tan Rong Jian Mark Tier 2 - Business Analyst

Lau Jun Rong Tier 3 - Dev and Infrastructure & Security

|  |  |
| --- | --- |
| **Systems affected by Incident** | |
| **Attack Sources (e.g., IP Address, Port):** | Internal File, .trojan file |
| **Attack Destinations *(e.g., IP address, Port)*:** | Google Slide 2 |
| **IP Addresses of Affected Systems:** | <http://3.1.118.42:8000>, <http://3.1.118.42:8001>, <http://3.1.118.42:8002> |
| **Domain Name(s) of Affected Systems:** | [esmscp.tk:8000](http://www.esmscp.tk:8000) |
| **Primary Functions of Affected Systems:**  ***(e.g., Web Server, Domain Controller)*** | Web Server |
| **Operating Systems of Affected Systems:**  ***(e.g., Version, Service Pack, Configuration)*** | Amazon Linux, Linux Kernel 4.14. |
| **Patch Level of Affected Systems:**  ***(e.g., Latest Patches Loaded, Hotfixes)*** | Latest Patches Loaded |
| **Security Software Loaded on Affected Systems:**  ***(e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)*** | NIL |
| **Physical Location of Affected Systems:**  ***(e.g., State, City, Building, Room, Desk)*** | AWS Cloud |

|  |  |
| --- | --- |
| **Users Affected by Incident** | |
| **Names and Job Titles of Affected Users:** | VIPs & users |
| **System Access Levels or Rights of Affected Users: (e.g., regular User, Domain Administrator, Root)** | Regular user |
| ***Additional information:***  Regular user’s readability access right has been violated due to ransomware attack on SCP’s Google Slide 2 | |

|  |  |
| --- | --- |
| **Timeline of Incident** | |
| **Date and Time When Agency First Detected, Discovered, or Was Notified About the Incident:** | 17 March 2019, 8.17 P.M. |
| **Date and Time When the Actual Incident Occurred:**  ***(Estimate If Exact Date and Time Unknown)*** | 17 March 2019, 12.00 A.M. |
| **Date and Time When The Incident Was Contained or When All Affected Systems or Functions Were Restored:**  ***(Use Latest Date and Time)*** | 17 March 2019, 10.55 A.M. |
| **Elapsed Time Between the Incident and Discovery:**  ***(e.g., Difference Between a. and b. Above)*** | 8 hours 17 minutes (497 minutes) |
| **Elapsed Time Between the Discovery and Restoration:**  ***(e.g., Difference Between a. and c. Above)*** | 2 hours 38 minutes (158 minutes) |
| **Resolution Time (Elapsed Time Between the Incident and Restoration:** | 10 hours 55 minutes (655 minutes) |
|  | |

# 

# **Ishikawa Fishbone Diagram with the 5 Whys Analysis**

# **Incident Management**

**Action(s) Taken to Identify Affected Resources**

1. Receive incident ticket via IS214 Ticketing System
2. Access SCP to check if ticket is genuine

**Action(s) Taken to Remediate Incident**

1. Temporary replacement of ransomware slides with a new version sent from Product Manager

|  |  |  |
| --- | --- | --- |
| **Walkthrough of Incident Timeline** | | |
| **Tier 1 - Communications** | | |
| **Steps** | **Description** | **Comment** |
| 1 | Receive notification of incident ticket & access IS214 Ticketing System | Check ticket’s information via IS214 ESM Ticketing System |
| 2 | Verify if incident is genuine by accessing ‘esmscp.tk’ | Google Slide 2 was attacked by ransomware as what was described in ticket |
| 3 | Inform Tier 2 of Incident | Update Tier 2 of Incident |
| **Tier 2 - Business Analyst** | | |
| **Steps** | **Description** | **Comment** |
| 4 | Access IS214 Ticketing System | Check status and information of incident |
| 5 | Verify if incident is genuine by accessing ‘esmscp.tk’ | Google Slide 2 was attacked by ransomware as what was described in ticket |
| 6 | Inform IT Operations Manager and Tier 3 | Immediately update relevant stakeholders that port 8000 is down |
| **Tier 3 - Dev and Infrastructure & Security** | | |
| **Steps** | **Description** | **Comment** |
| 7 | Access IS214 Ticketing System | Check status and information of incident |
| 8 | Verify if incident is genuine by accessing ‘esmscp.tk’ | Google Slide 2 was attacked by ransomware as what was described in ticket |
| 9 | Access the directory of application’s startup file ‘cd /home/ec2-user/Django\_Application/virtual\_env/ICA-1/ICA/bin’ | Get to the directory to start the startup file |
| 10 | Temporarily replaced embedded google slide to “<https://docs.google.com/presentation/d/e/2PACX-1vRh_WpvKQ7K1CpV3LRSvwEOtYUXfqqlBYAFxIIij3sSZ-xbzlwLANUtaL6mgfccZWMvl_-aieKJQL4q/embed?start=true&loop=False&delayms=3000&slide=id.p>" | Check if google slide was replaced successfully |
| 11 | Replaced embedded google slide to url from Fantasama Web Services | Check if google slide was replaced successfully |

# 

# **Post-Incident Follow up**

Actions Planned to Prevent Similar Incidents:

|  |  |  |
| --- | --- | --- |
| **Steps** | **Description** | **Comment** |
| 1 | Request for Fantasma Web Services to secure their servers. | Assist Fantsma in any steps to trace the source and nature of attack. |
| 2 | Follow up with Fantasma Web Services on appropriate troubleshooting steps in the event of a similar incident. | Take details of steps to recover the incident and who to follow-up report to. |
| 3 | Warm standby of a deployed application to take over when such incidents happen. | Deploy app to a standby instance, ready to take over in the event of an incident. |
| 4 | Implemented visual monitoring app called VisualPing | Helps to monitor any changes done on the visual or web level |

**Additional Remediation Details:**

|  |  |  |
| --- | --- | --- |
| **S/N** | **Action** | **Details** |
| 1 | Implement ITIL Change Management | Ensure all staff are informed and trained on the necessary corrective steps to take in an incident |
| 2 | Improve software release processes | Ensure all staff are informed and trained on the necessary corrective steps to take in an incident. |
| 3 | Proactively identify incident trends | Beside from port monitoring, Tier 1 & 2 will monitor the website periodically to ensure correct output is displayed to the end user. |
| 4 | Identify recurring incidents ‘on the go’ | Incidents are recorded and easily accessible at the incident log. This is to ensures that similar incidents in the future will be easy to troubleshoot and categorize. |
| 5 | Prevent the recurrence of major incidents | Root cause analysis to be performed and sent to all stakeholders. Rectification steps must be made (change in process or improvement in environment) to ensure that similar incidents will have a lesser chance of recurring. |

#### 