**PHISHING**

INCIDENT

RESPONSE

**RUNBOOK**

Contents

[SANS Framework 3](#_Toc136281782)

[Detection 3](#_Toc136281783)

[Analysis 4](#_Toc136281784)

[Containment 5](#_Toc136281785)

[Eradication 6](#_Toc136281786)

[Recovery 7](#_Toc136281787)

[Post incident activity 8](#_Toc136281788)

[Appendix A - Response report 9](#_Toc136281789)

[Appendix B - Evidence log and strategy 11](#_Toc136281790)

[Appendix C – Exercise evaluation 12](#_Toc136281791)

[RED TEAM Evaluation 12](#_Toc136281792)

[BLUE TEAM Evaluation 13](#_Toc136281793)

[Appendix D - Team minutes – Runbook pre-development discussion 14](#_Toc136281794)

[Appendix E - Team minutes – Post-exercise evaluation discussion 14](#_Toc136281795)

[Revision table 15](#_Toc136281796)

# SANS Framework

## Detection

A picture containing text, screenshot, diagram, design

Description automatically generated

## Analysis

A picture containing text, screenshot, diagram, design

Description automatically generated

## Containment

A picture containing text, screenshot, diagram, design

Description automatically generated

## Eradication

A picture containing text, screenshot, diagram, design

Description automatically generated

## Recovery

A picture containing text, screenshot, diagram, design

Description automatically generated

## Post incident activity

A picture containing text, screenshot, design, diagram

Description automatically generated

# Appendix A - Response report

**CYBER INCIDENT RESPONSE FORM**

|  |
| --- |
| **INCIDENT IDENTIFICATION INFORMATION** |

|  |  |
| --- | --- |
| **Date and Time of Notification:** Sunday, 28 May, 2023 | |
| **Incident Detector’s Information:** | |
| **Name:** Mark Byrne | **Date and Time Detected:** |
| **Title:** Threat intelligence analyst | **Location:** Melbourne, AUS |
| **Phone/Contact Info: 0400 000 798** | **System or Application:** Windows Server 2019 |

|  |  |
| --- | --- |
| **INCIDENT SUMMARY** | |
| **Type of Incident Detected:**  ☐ Denial of Service                    ☐ Malware                        ✓ Ransomware  ✓ Unauthorized Access              ✓ Phishing Attack            ☐ Malicious Code  ☐ Other: (Specify) | ☐ Unauthorized Use  ☐ Other |
| **Description of Incident:** Employee received suspect email requesting an Adobe license update and included an external link.  The employee accessed the link and subsequently downloaded some malware identified as DriverUpdate.exe (Trojan).  The Windows Defender identified this and the malware was quarantined and removed. | |
| **Names and Contact Information of Others Involved:** Shaun Heywood, Mark Byrne and Patrizia Constantini | |
| **INCIDENT NOTIFICATION – OTHERS** | |
| ✓ IS Leadership                                           ✓ System or Application Owner  ✓Security Incident Response Team        ☐ Public Relations Dept  ✓ Administration                                             ☐ Human Resources  ☐ Other: | ☐ System or Application Vendor         ☐ Legal Counsel |
| **ACTIONS** | |
| **Identification Measures (Incident Verified, Assessed, Options Evaluated):** | |
| The incident was verified by running a scan using Wireshark in order to verify the phishing attack and the remote connection. The downloaded file was also scanned using VirusTotal.com online services | |
| **Containment Measures:** | |
| * Configure firewall software to block the domain of phishing website. * Used antivirus scanner to detect any Malware installed as a result of successful phishing attack - if identified run Malware/Ransomware run book | |
| **Evidence Collected (Systems Logs, etc.):** | |
| * System logs * Emails * Malicious URL * Attachments | |
| **Eradication Measures:** | |
| * Malware removal running antivirus and antimalware scans | |
| **Recovery Measures:** | |
| * In this incident there was no data loss as the Malware was identified and removed, however any data loss would have been recovered from backups. * Users details were reviewed and checked if still working post the incident. | |
| **Other Mitigation Actions:** | |
| * Use email filtering and web protection in order to have a mechanism to block phishing emails and malicious files/attachments for example DriverUpdate.exe. * Install anti-phishing browser extensions | |
| **How Well Did Work Force Members Respond?** | |
| Since the attack was on Sunday the response took 2 hours between the employee notifying the phishing attack and the IT Team started the response for the attack. | |
| **Were the Documented Procedures Followed? Were They Adequate?** | |
| **Yes -** They were adequate and ready to follow the procedures indicated for OZ Casual. The IT Team followed and applied the procedures there were in the document. | |
| **What Information Was Needed Sooner?** | |
| * Users login credentials and server access details. * Remote desktop login details into the VM | |
| **Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?** | |
| There is no step that might inhibit the recovery. The actions and steps are clear in the procedures document. | |
| **What Could Work Force Members Do Differently the Next Time an Incident Occurs?** | |
| Report all emails like this as phishing and remember the training | |
| **What Corrective Actions Can Prevent Similar Incidents in the Future?** | |
| * Run antimalware services on daily bases * More training for employees on Phishing awareness | |
| **What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?** | |
| * Setup the use of SPLUNK in order to analyze the data traffic * Create “honeypots” in order to distract potential attackers | |
| **Other Conclusions or Recommendations:** | |
| As a company we have to see the possibility to use a cloud based mail server with malicious code and malware filtering. This will be helpful due to any attack that will be contained in the cloud before it reaches our physical servers or other devices. | |
| **FOLLOW-UP** | |
| **Reviewed By:**  ✓ IT Management                  ✓ Security Officer                           ☐ IS Department/Team  ☐ Privacy Officer                                   ☐ Other | |
| **Recommended Actions Carried Out:** | |
| Mauricio G. Guerra | |
| **Initial Report Completed By:** Mark Byrne | |
| **Follow-Up Completed By:** Mauricio G. Guerra | |

# Appendix B - Evidence log and strategy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATE, TIME AND LOCATION OF COLLECTION** | **COLLECTED BY** (name, title, contact and phone number) | **ITEM DETAILS** (quantity, serial #, model #, hostname, (MAC) address, and IP addresses) | **STORAGE LOCATION AND LABEL NUMBER** | **ACCESS –** date, time, person and rationale for access after collection |
| 28/05/23 - 2.15pm | **Name:**  Shaun Heywood  **Title:**  Incident Analyst  **Contact #:**  0400 000 789  **email:**  [shaun.heywood@live.vu.edu.au](mailto:shaun.heywood@live.vu.edu.au) | **Quantity** : 1  **Serial Number**:  22A9602F-3749-43E8-Af1C-26FEF4B3  **Model Number**:  00376-30715-20427-AA833  **Hostname**:  WIN-B2GHEVE7CC4  **MAC Address**:  00-15-5D-00-04-13  **IP Address**: 10.10.10.102 | Phishing email containing links to URL for Adobe update | 29/5/23 - 4pm  Access provided to respond to the cyber incident  **Mark Byrne** - Threat intelligence |
| Windows Defender blocking the file downloaded from the mail client by the user. | 29/5/23 - 4pm  Access provided to respond to the cyber incident  **Mark Byrne** - Threat intelligence |

# Appendix C – Exercise evaluation

## RED Team Evaluation

|  |
| --- |
| **Activity name and description**  **Name :** Phishing Attack  **Description:** The red team had successfully created a phishing email with a link to a backdoor trojan, that was sent to the blue team’s temporary email account. The blue team then clicked on the link, which opened a browser and downloaded the trojan. They then executed the file, disguised as a Driver Update program, opening a remote session to the red team’s attacking system |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities? If so, comment on its suitability. If not, provide details of what was missing.**  Yes.  It was a matter of selecting the right tools needed to get the remote connection open. |
| **Did you feel that there was an adequate level of training to support the attack? If, not provide details**  No. I believe that more time using the tools available to us, may have allowed us to develop more sophisticated methods of social engineering emails. The phishing email was a simplistic HTML format with text only, but with more training, it could have resembled a real looking email |
| **Was the structure of the exercise realistic? If not, provide details**  Yes.  In a real-world scenario, this type of attack happens on a daily basis. It's only the level of sophistication or spear phishing, that makes real world scenarios more dangerous. |
| **Please provide comments regarding what you believe worked and did not work during the exercise?**  All went as planned. With the blue team’s defenses down, the red team was able to remotely connect to the blue team’s system without being detected. However, once the Windows Defender was turned on, our payload was detected and quarantined before being able to execute the file. |
| **How can the red team’s actions be improved?**  By developing more realistic looking emails that could trick a recipient. Payloads that virus scanners will not detect before allow a remote connection to be established. |
| **How can the red team’s training be improved?**  By studying different tools that are used in more sophisticated attacks, we can further understand how much research and skill is required to easily trick a person into opening malicious emails. |
| **How appropriate was the pre-training to the exercise?**  In theory, the plan had merit. Of course, it was much different when putting our limited knowledge into action. Not knowing what tools would work best, meant experimenting with tools, before putting them to use. |
| **How could the pre-training be improved?**  It would be fair to say that more experience in using other tools, would allow us knowledge of what real world hackers do to get their malicious email across |

## BLUE TEAM Evaluation

|  |
| --- |
| **Activity name and description**  **Phishing attack with links to external website to download Ransomware**  The target will be sent a phishing email that contains a link to a cloned website.  The red team will attempt to deliver a backdoor trojan,  in the form of a file disguised as a driver update.  The victim will download the trojan, under the assumption it is a driver updater.  This will allow us remote access to upload and execute the ransomware |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities? If so, what information and resources were used? If not, provide details of what was included and what should have been included.**  No  We didn’t have an anti-phishing filter installed prior to the exercise and having this in place would have alerted us to the fact that a suspect phishing email was received |
| **Did you feel that there was an adequate level of training to support the response effort? If, not provide details**  More training could have been done on the exercise and use of anti-phishing email filters  We also could have had a review of blocking domains via the firewall to refresh the thinking |
| **Was the structure of the exercise realistic? If not, provide details**  Yes - This happens every day and users click through to malicious websites regularly.  The approach we took to emailing an employee was realistic |
| **Please provide comments regarding what you believe worked and did not work during the exercise?**  The installation of anti-phishing software could have been installed ahead of time and ready for execution. The selected cloud based solution wasn’t working straightaway. |
| **How can the blue team’s response be improved?**  Although in this instance it wouldn’t have helped, the Blue team could have taken an action to change the login credentials of the impacted users in case this was shared at any point. This would be good practice. In addition the Blue Team could have looked at other tools to decrypt the WannaCry with tools such as WannaKiwi tool. |
| **How can the blue team’s training be improved?**  We could have spent more time together as a blue team discussing the appropriate tools for phishing detection. We also could have spent time as a team reviewing the firewall domain blocking features to familiarize ourselves with this. |

# Appendix D - Team minutes – Runbook pre-development discussion

**27/05/2023 : Minutes of the Meeting**

**Giuseppe Raciti** - Manager / Team Lead

* The style of the framework was initially a step by step detailed guide, but eventually, it was decided that the SANS Incident Response format was preferred in a flowchart format.
* Using each runbook for the Ransomware and Phishing Incident response, each group member was able to allocate a task they wanted to perform during the functional exercise.
* The red team was originally going to breach the targeted system using a vulnerable exploit of the Windows 10 client. Unable to find a vulnerability that could be exploited, a unanimous vote was made to change the initial stage of the attack to a phishing email

**Mauricio Guerra** - Technology Watch

* **Detection step:** Implementing a cloud base security detection system, for example [IBM Security QRadar](https://www.ibm.com/qradar) Suit could be an opportunity to migrate to a predictive service that will analyze and anticipate potential Indicator Of Compromise (IOC) due to this system working with signature based, behavior based and machine learning methods.
* **Eradication step:** As a result of the ransomware and the possibility that there is no backup in place is critical to create a backup. At the same it is imperative to update policies, procedures, controls and technologies in place to build capacities for backups, physicals and in the cloud.
* **Post incident:** I would like to start this recommendation with a question: Is it reasonable to alert the enforcement authorities if the number of devices compromised is small? They might leak the information to the press and we will have a reputation loss when potentially just a few devices and little data is compromised. On the other hand if we have a lot of data lost, compromising our client’s personal information will be reasonable to alert the enforcement authorities in a discreet way. In this scenario the PR department will be essential.

**Shaun Heywood** - Platform Specialist / Incident Analyst

* Accountable for overseeing the platforms and security infrastructure that the incident response team uses. This entails managing the installation, maintenance, and management of security solutions like firewalls, intrusion detection systems, and security information and event management (SIEM) systems.
* Analyze alerts or abnormalities while actively monitoring the security platforms for potential security problems, in order to investigate and prioritize warnings that may arise.   In order to find indicators of compromise (IOCs) or patterns of malicious activity, I will be examining network traffic, system logs, and other relevant information sources. Working together with other team members, I am able to analyze occurrences, pinpoint the underlying cause, and create containment and eradication plans.
* My role is to provide a coordinated and successful response to security incidents, working along with incident handlers, forensic analysts, and communication coordinators from the incident response team. During incident response I will offer guidance on actions like containment, eradication, and recovery.  In order to enhance future incident response skills, I can also be involved in creating incident response playbooks, documenting incident response protocols, and performing post-event analysis.

**Mark Byrne** - Threat intelligence analyst

* Phishing and ransomware is ever present and was a good selection from a practical perspective. We have all received phishing attempts and these are not going away.
* Communication is going to be important to ensure the team is aligned - An established Red Team / Blue team What’s App chat to share tools for the monitoring of any ransomware.
* Wireshark will be installed to monitor traffic on the network and to help detect unusual / abnormal outcomes. There was some discussion on the use of tools such as Splunk to set up alerts and monitor results.
* The windows firewall will be turned off and as a part of the exercise
* Anti-phishing email filters is another option to prevent the delivery of the ransomware and we will look into what we can install on the mail server to reduce the volume of phishing emails.
* The use of software such as Sophos Email can help prevent Phishing and imposter threats

# Appendix E - Team minutes – Post-exercise evaluation discussion

## Blue Team Mitigation Strategies:

The blue team was able to use a number of tactics to mitigate the threats that the phishing and ransomware cyber-attack posed. We were able to inform staff about the risks and attack methods used by the malicious actor (Red Team) by undertaking employee user awareness training.

The training was able to demonstrate the methods to identify and stop malicious emails and attachments by using email filtering, antivirus and malware tools, and anti-phishing methods.

Advanced endpoint protection solutions, routine software patches, and network segmentation are all strategies we were able to utilize in order to improve our ransomware defenses.  We made use of Wireshark, PFSense firewall with Snort, as well as CrowdStrike to detect, eradicate and recover from the attack.

The Blue Team was also able to implement data protection and recovery by using data backups that were performed on a regular basis.

## Methods of Lowering the Incident Resolution Time:

The OzCasual IRT should optimize their incident response strategies by routinely assessing and updating them, to reduce incident resolution time. This process guarantees that the plans are thorough, current, and in line with the changing security environment. By utilizing available security tools and technology, the IRT can minimize manual work by automating incident detection and response.

Security information and event management (SIEM) solutions can be implemented, creating a centralized log management that will enable effective detection of security incidents and analysis.  The SIEM is able to collect, correlate and analyze security events in real time.  OzCasual can reduce the amount of time needed to locate, contain, and lessen the impact of cyberattacks by putting these strategies into practice.

## Effectiveness of Pre-Training Activities

Pre-training exercises are essential for preparing OzCasual for cyberattacks. Their performance depends on providing staff with the knowledge and abilities needed to properly identify, prevent, and respond. This can be accomplished by educating staff members about phishing tactics and cybersecurity best practices through security awareness programmes.

Incident response plans provide staff with an understanding of their responsibilities as well as the ability to act rapidly in the event of an attack. Employees are able to improve their awareness through simulated exercises, where they can practice their response techniques in a realistic assault scenario.

## Effectiveness of Red Team Activities

The Red team’s activities are effective when they accurately simulate real-world cyber-attacks and identify vulnerabilities within an OzCasual’s defenses. Their success was measured by their ability to uncover weaknesses, expose vulnerabilities, and perform the pre desired attack, as well as provide actionable recommendations for improving security.

The Red team thoroughly assessed OzCasual’s infrastructure, processes, and human factors to uncover potential weaknesses that could be exploited by attackers.  By employing real-world attack techniques, phishing and ransomware, the red team was able to replicate the tactics used by malicious actors, allowing OzCasual to understand its vulnerabilities much better.

The red team's goal was to test the effectiveness of existing security controls, including firewalls, intrusion detection systems, and endpoint protection solutions, by attempting to bypass them and implement a ransomware attack via a phishing email.

The Red team was successful in its approach by utilizing a Kali Linux attacker machine and the Metasploit application.