**RANSOMWARE**

INCIDENT

RESPONSE

**RUNBOOK**

Contents

[SANS Framework 2](#_Toc136218912)

[Detection 2](#_Toc136218913)

[Analysis 3](#_Toc136218914)

[Containment 4](#_Toc136218915)

[Eradication 5](#_Toc136218916)

[Recovery 6](#_Toc136218917)

[Post incident activity 7](#_Toc136218918)

[Incident Response Checklist 8](#_Toc136218919)

[Detect and Analyze 8](#_Toc136218920)

[Analysis 8](#_Toc136218921)

[Containment 8](#_Toc136218922)

[Eradicate 8](#_Toc136218923)

[Recovery 9](#_Toc136218924)

[Post Incident Review 9](#_Toc136218925)

[Appendix A - Response report 10](#_Toc136218926)

[Appendix B - Evidence Log and Strategy 13](#_Toc136218927)

[Appendix C – Exercise evaluation 16](#_Toc136218928)

[RED Team Evaluation 16](#_Toc136218929)

[BLUE Team Evaluation 17](#_Toc136218930)

[Appendix D - Team minutes - Runbook Pre-Development Discussion 17](#_Toc136218931)

[Appendix E – Team minutes – Post-exercise Evaluation Discussion 20](#_Toc136218932)

[Blue Team Mitigation Strategies: 20](#_Toc136218933)

[Methods of Lowering the Incident Resolution Time: 20](#_Toc136218934)

[Effectiveness of Pre-Training Activities 20](#_Toc136218935)

[Effectiveness of Red Team Activities 20](#_Toc136218936)

[Revision table 21](#_Toc136218937)

# SANS Framework

## Detection

START

**ALERTS**

**NOTIFICATIONS**

**Have risk factors been identified?**

No

Yes

**Collect and analyze data**

**Have threat indicators been identified?**

No

* Malware signature
* Unusual behavior
* Abnormal traffic
* User reported
* Anti-virus software
* Spam email with attachment
* Malware detection

Collect all evidence, such as:

* Emails containing malware
* System and device logs
* IDS/IPS event logs
* Screenshots of the Ransomware message
* Identify the scope of the incident
* The name of the malware
* What vulnerability allowed this to occur

**Categorize  
Attack**

Determine motive for attack

* Financial
* Exfiltrate sensitive data
* Data destruction

Assess potential impact:

* Financial damage
* Reputation sabotage
* Availability disruption

Determine scope

* Number of systems and devices the ransomware may have affected
* Can 3rd parties connected to network be impacted by the malware

Create an incident response report

**Triage  
Impact**

**Analysis  
Step**

Yes

## Analysis

Collect all evidence, such as:

* Examine affected systems for signs of encrypted files, ransom notes or messages with demands
* Take screenshots with a camera of the ransom note, with particular attention to the type of ransomware that identifies the attacker
* Conduct malware scans with up-to-date and reliable malware signatures to detect and confirm presence of malware
* Check whether files are encrypted, the file extensions typically found with ransomware encryption.

**Verify**

**Detection  
Step**

Update Incident Response Report and evidence logs

**Containment**

**Step**

**Update Scope**

Yes

**Data Collection**

**Have all the endpoints been identified?**

* Using reputable anti-virus or anti-malware software, perform thorough scans of the affected systems. Up to date software will be able to detect the latest signatures of malware.
* Update IDS / IPS Signatures and rules
* Analyze system logs, event logs, system and application errors or any other unusual or suspicious activities.
* Look for failed login attempts, or any other anomalies that would indicate system compromise
* Collect the ransomware not that could contain contact information, unique identifiers, or instructions by the attacker
* Analyze the network traffic logs and use traffic monitoring software to identify suspicious communication patterns or connections to malicious IP addresses or domains.
* Check modified files for metadata or timestamps to identify files that have been modified or encrypted
* Engage the Incident Response Team to react.

**Identify Indicators of Compromise (IOC)**

**Scan Organization**

No

Network based IOC

Host based IOC

Email based IOC

Behavioral IOC

## Containment

Shut down any communications the malware may be using to communicate with the attacker.

Any infected device or system still connected will have remote command-and-control channels and any new infected devices can still be quarantined without the ransomware being able to be executed once communications are restored

**Analysis**

**Step**

**Isolate affected systems**

Attempt to disconnect the affected systems from the rest of the network without shutting off the device, to prevent data loss

Devices must be disconnected from the network physically, or disable the wi-fi of affected systems and devices

**Eradication**

**Step**

**Collect and analyze data**

Update the detection software of all devices and network systems to detect the file and stop the possible spread

* Inform the IRT of the persistent threat the malware presents, and work to mitigate the scope of the attack.
* Scan all systems and devices that may or may not be affected
* Collect all logs that could identify the lateral movement of the malware and the extent of system compromise

Yes

**Can the executable file be blacklisted?**

No

To stop the spread of the malware, configure protection software to detect the file that contains the malicious malware

**Update Detection Software**

**Does the Ransomware variant spread itself?**

**Scan Endpoints**

Yes

No

**Block Remote Connections**

Preserve all evidence of scans or log files collected, because it’s important to preserve evidence for forensic analysis. This can be crucial in determining if it’s a targeted attack or if the attack is severe.

This can later be used as evidence that law enforcement can use.

Update Incident Response Report and evidence logs

**Update Scope**

## Eradication

**Block Additional Communication**

**Containment  
Step**

Update all security software

* Update all antivirus and anti-malware software with latest version and patches
* Update all device firmware
* Update firewall and IDS/IPS software, including latest patches

Yes

**Malicious process/service stopped successfully?**

**Patch & Mitigation**

**Remote Access**

If available, use remote tools to access infected systems, and kill services and processes to remove the malicious file.

If the executable is persistent, a remote connection can shut down persistent threats on infected hosts

No

No

Yes

* Scan all endpoint devices with updated software to remove files and any residual trace of the malware
* Delete any files that were infected or encrypted
* Check system processes and services on any affected devices. Looking for any unknown or high usage ones which could be related to the ransomware
* Perform registry scans, using caution not to alter or delete ones that are genuine
* Patch all software on the affected systems, removing any vulnerability the attacker used to exploit.

**Scan Organization & Patch Software**

**Containment**

**Step**

**Do Endpoints show IOC or lateral movement?**

**Collect and analyze data**

In some instances, attackers that use widely known ransomware, a Decrypter might be available. It can be used on files that were set aside, or where no backup was created.

Using backups stored off-site or on external media, restored the data that was encrypted

**Is a Decrypter available?**

**Is a backup available?**

No

Yes

Yes

**Restore encrypted files**

**Is the Ransomware variant known to steal data?**

No

**Initiate   
Data Loss / Theft Playbook**

Yes

Block any additional communication and channels that were discovered during the containment and eradication phases.

Update Incident Response Report and evidence logs

**Recovery**

**Step**

**Update Scope**

**Implement new detection rules**

**Send samples to vendors**

Implement custom detection rules into all security software, including IPS/IDS systems, SIEM, Virus and Anti-Malware software, Log Correlation, Analytics

Data Corrupted  
And Unrecoverable

## Recovery

**Post Incident**

**Step**

**Eradication**

**Step**

**Restore From Backups**

Yes

**Rebuild Compromised Systems**

Assess the extent of the damage caused by the ransomware attack. Identify the systems, applications and potential data affected or encrypted.

Prioritizing the importance of the data, use a reliable and up-to-date backup taken before the attack. It vital that the integrity of the backups is verified prior to the restoration, to ensure the malware didn’t infect backup data.

In cases where backups are deemed unreliable, compromised systems may need to rebuild from scratch. If firmware was affected, it could even mean the replacement of the hardware itself.

This would require reinstalling operating systems, applications, and security software. All the configurations would need to be configured as well as installing all necessary updates and patches

**Verify Data Integrity**

After the systems are restored from backups, data integrity and completeness should be verified.

Conducting thorough tests and validation on the restored data will ensure the restored data is accurate and functional

**Has the backup data been compromised?**

No

Data Corrupted  
And Unrecoverable

**Change Credentials**

**Harden Security Measures**

It can’t be assured that during the attack, credentials and other login details weren’t stolen. Therefore, it would be necessary to change the login credentials to all services, systems, and hardware, to prevent unauthorized access

Deploying and implementing endpoint security software, can be one of many ways to prevent a future attack. It could also be used to conduct regular audits, enhance network security, and improve employee awareness through training programs

## Post incident activity

A debriefing should be conducted that informs key stakeholder, including the Incident Response Team, IT personnel, senior management, vendors, and other relevant parties.

This would include a detailed and comprehensive recollection of the incident, the response actions taken, and any lessons learned

Gather all the evidence taken during the incident, to understand the attack vector, identify the scope of the compromise, and evaluate the extent of the damage.

Analysis of the evidence can help to understand the attacker’s methodology, the level of skill and knowledge required, how the vulnerabilities were found and exploited, and understanding how to bolster the organizations security posture

Review and enhance backup procedures using insights gained through the incident. If more frequent backups are required, documentation and systems can be changed to backup data systems on a more frequent basis, reducing the chance of data corruption or loss.

Review employee training documentation, to reinforce to security awareness, and provide addition training to employees.

The incident can be used to educate the company’s employees about the recent attack, emphasizing the need to be aware of phishing scams, and being alert when opening any file.

Employees can also be reminded about the importance of good cyber hygiene practice and maintaining complex passwords to secure themselves.

Conduct a thorough review of the organizations current security posture, by reviewing policies, procedures, controls, and technologies.

This process will allow the team to identify areas that require review, and necessary changes and improvements required.

Review the Incident Response Plan based on the insights gained from the ransomware attack. Implement any lessons learned that would allow the implementation of preventative measures and response procedures that would improve the response capabilities in a future attack

Using lessons learned, implement security technologies that would prevent a future incident. This could include implementing security controls and monitoring mechanisms within the company network.

This may also include new intrusion detection and prevention systems, advanced endpoint protection, Security Information and Event Management (SIEM) technologies, and maintaining a regular security audit.

Continuously monitor the systems and network, for any signs of re-infection or suspicious activity or connections.

**Recovery**

**Step**

**Incident Review**

**Document debriefing**

**Forensic Analysis**

**Review Company Documentation**

**Implement Security Controls and Monitoring**

**Ongoing Incident Response Readiness**

**END**

# Incident Response Checklist

## Detect and Analyze

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | Received report of ransomware on user’s device | Done |
| 2 | Inspect user’s device to determine threat indicators   * Event logs or alerts of malware detections * Anti-virus or Anti-malware event / alerts * Ransomware message demanding funds | Done |
| 3 | Determine if the phishing email containing malware was a targeted attacked, or random email | Done |
| 4 | Determine the ransomware scope – application, workstation, network devices, or servers | Done |
| 5 | Begin an Incident Response Report form and retain all evidence and logs | Done |

## Analysis

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | Confirm the presence of malware   * Ransomware message on the screen of the affected device * Document the evidence, taking photos of the ransomware message with a phone * Scan the affected system to determine if the anti-virus/malware detects the ransomware | Done |
| 2 | Identify whether there are Indicators of Compromise   * Collect all the information about the ransomware and determine the motive for attack (ie financial) * Analyze network traffic and attempt to detect known malicious IP addresses or domains * Check files for metadata that could provide further information * Engage the Incident Response Team | Done |
| 3 | Collect IOC data from emails, behavioral IOC, host based and network-based IOC | Done |
| 4 | Have all affected endpoints been identified? | Done |

## Containment

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | Isolate affected systems, disable wi-fi, disconnect ethernet, but attempt to leave device on | Done |
| 2 | Attempt to contain the spread of the malware by blacklisting the file on the network | Done |
| 3 | * Scan all endpoints and determine if the malware is self-replicating to prevent lateral spread * Update all detection software and firewalls to stop the file spreading | Done |
| 4 | * Block remote connections to malicious IP addresses and domains * Collect evidence of logs, alerts, ransomware variant and information, take photos | Done |
| 5 | * Collect all evidence for forensic analysis port incident * Update the information in the Incident Response Report form | Done |

## Eradicate

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | * Attempt remote access to affect systems and kill related services and processes of the ransomware. * If the attempt fails, return to beginning of analysis until successful | Done |
| 2 | * Patch all firmware, including applications, operation systems, and security software * Run company wide scan of all systems, to remove residual trace of ransomware | Done |
| 3 | Scan all endpoints for possible lateral spread. Collect all evidence of logs and events | Done |
| 4 | * Attempt to restore the data that was encrypted, is there a decrypter available for the ransomware. * Determine the malware variant, to expose the motive for the attack (financial, data exfiltration) * Refer to Data Loss / Theft playbook, if required * Block any network communication channels discovered in the containment and eradication phases | Done |
| 5 | * Update scope in the Incident Response Report form * Send samples of the malware to vendors of software who are likely vulnerable * Implement new detection rules in IDS/IPS, SIEM, Anti-malware and anti-virus software | Done |

## Recovery

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | * If the off-site or cloud backup has not been compromised, attempt to restore systems * If data has been corrupted, this could result in a full rebuild from scratch | Done |
| 2 | Verify the integrity of the restored data, confirming its complete and functional | Done |
| 3 | Change credentials of all systems, devices, workstations, and users, in case of compromise | Done |

## Post Incident Review

|  |  |  |
| --- | --- | --- |
| # | Action | Completed |
| 1 | Assemble relevant staff, ICT, stakeholders, management, and vendors for debriefing of incident | Done |
| 2 | Collaborate the evidence to understand the attack vector, scope of the compromise, and the damage extent  Analyze the data to understand the attacker methodology, difficulty to breach, and vulnerabilities exploited | Done |
| 3 | * Review company security posture by auditing policies, procedure, controls, and technologies * Review company backup procedures and make improvements when needed * Improve employee awareness of cyber hygiene and threats related to the recent attack * Run additional training of staff who may require training or are a higher risk of becoming a victim | Done |
| 4 | Review the lessons learnt, and implement new detection technologies, such as newer IDS/IPS systems, better developed SIEM systems or artificial intelligence behavioral technologies | Done |
| 5 | Continuously monitor network systems and traffic for the immediate future for signs of re-infection | Done |

# Appendix A - Response report

**INCIDENT RESPONSE REPORT FORM**

|  |  |  |
| --- | --- | --- |
| **INCIDENT IDENTIFICATION INFORMATION** | | |
| **Date and Time of Notification:** Sunday, 28 May, 2023 | | |
| **Incident Detector’s Information:** | | |
| **Name:** Shaun Heywood | | **Date and Time Detected:** 28 May 2023. 11:00 AM |
| **Title:** Incident Analyst | | **Location:** Melbourne, AUS |
| **Phone/Contact Info:** 0400 000 789 | | **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 identified with the number 58964 in this company opened an email with a malicious link which he opened. After this incident happened a trojan identified as DriverUpdate.exe was downloaded and executed remotely.  After 30 minutes a malicious individual got unauthorized access and ran the ransomware WannaCry. The files of the sales department are encrypted. The employee was creating a marketing campaign in order to generate more revenue for the winter season. He was working extra hours on Sunday and had ready the marketing campaign for the following week. | | |
| **Names and Contact Information of Others Involved:** Mark Byrne | | |
| **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. Also we verified the connection between a malicious device and Windows Server. | | |
| **Containment Measures:** | | |
| * Disconnect ethernet cables and turn off the Wi-Fi. The devices still are running in order to allow forensic analysis. * Isolate the sales department computers * Create an DMZ in order to isolate the sales department   Run antivirus scans for the rest of the departments connected to the same network | | |
| **Evidence Collected (Systems Logs, etc.):** | | |
| * System logs * Logins attempts * Emails * Malicious URL   Attachments | | |
| **Eradication Measures:** | | |
| * Malware removal running antivirus and antimalware scans * Patching and vulnerability management * Password resets   Update patches for the OS and antivirus | | |
| **Recovery Measures:** | | |
| Due to OZ Casual being a company that has suffered many cyber attacks, they already have recovery measures in place. One member of the IT department, after eradicating the malware and ransomware (if possible), will check if there is any data lost.  If there is data lost it will recover the server and computers with the data that is keeped encrypted in the cloud. | | |
| **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. | | |
| **How Well Did Work Force Members Respond?** | | |
| Due to the fact that 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?** | | |
| 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?** | | |
| * Sales during May * Sizes and products to be refilled   Database with clients that have access to our membership | | |
| **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?** | | |
| The principal recommendation will be: “won’t open suspicious links”. | | |
| **What Corrective Actions Can Prevent Similar Incidents in the Future?** | | |
| * Run antimalware services on daily bases * If the employee is a recurrent offender could be an option to let him go by the management.   Separate the different departments by an DMZ | | |
| **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:** Shaun Heywood | | |
| **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**)** |
| 28/05/2023  3:00  pm | **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 | This screenshot shows the victim receiving an email with a link to a website.  The URL provided  asks the user to download a Driver Update file called **DriverUpdate.exe** | **29/5/23 - 5pm**  Access provided to respond to the cyber incident  **Patrizia Costantini**  - Vulnerability Handlers  **Mark Byrne**  - Threat intelligence analyst |
|  |
|  |
| 28/05/2023  3:01  pm | This screenshot shows the malicious URL being discovered by Wireshark, blocked by Windows Defender and sent to quarantine, and not being able to be executed by the user. | **29/5/23 - 5pm**  Access provided to respond to the cyber incident  **Mark Byrne** - Threat intelligence analyst |  |
| 28/05/2023  3:25  pm | **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 | Wireshark captures the GET request for malicious file | **29/5/23 - 5pm**  Access provided to respond to the cyber incident  **Mark Byrne**  - Threat intelligence analyst |  |
| 28/05/2023  3:59  pm | Windows defender was turned on and stopped infected file **WannaCry.exe** downloading | **29/5/23 - 4pm**  Access provided to respond to the cyber incident  **Mark Byrne**  - Threat intelligence analyst |  |
| 28/05/2023  3:37  pm | **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 | Windows defender detects malware being opened and quarantines the file | **29/5/23 - 4pm**  Access provided to respond to the cyber incident  **Mark Byrne**  - Threat intelligence analyst |  |
| 28/05/2023  4:25  pm | Red team executed ransomware WannaCry, decrypter could be found, or full restore from backup | **29/5/23 - 4pm**  Access provided to respond to the cyber incident  **Mark Byrne**  - Threat intelligence analyst |  |

# Appendix C – Exercise evaluation

## RED Team Evaluation

|  |
| --- |
| **Activity name and description**  **Ransomware attack using WannaCry malware**  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, comment on its suitability. If not, provide details of what was missing.**  Yes.  Kali contains all the tools needed to create a phishing email and clones a website using the Social Engineering Tool (SET).  Kali also contains the tools in Metasploit, to create the backdoor trojan needed to gain remote access  The WannaCry malware was available to download from the Dark web |
| **Did you feel that there was an adequate level of training to support the attack? If, not provide details**  No,  It required some out of the box thinking, as well as resources that required study to know how to use. |
| **Was the structure of the exercise realistic? If not, provide details**  Yes.  In a 3 phase attack, the email is sent with the backdoor. Once opened, we gain remote access. Deploy and execute the ransomware, encrypting the victims device |
| **Please provide comments regarding what you believe worked and did not work during the exercise?**  The target was tricked into opening the phishing email, where they then downloaded the file which opened the backdoor for the Red team to upload and run the ransomware |
| **How can the red team’s actions be improved?**  If the red team was able to install and run a rootkit, the backdoor wouldn't rely on waiting for the user to execute the backdoor trojan again, if the red team wanted access after a system reboot. |
| **How can the red team’s training be improved?**  Training ourselves on the use of other pen-testing tools to create different types of attacks, would allow us to deploy more sophisticated techniques, such as brute force entry into the target system, without the need of a trojan. |
| **How appropriate was the pre-training to the exercise?**  It was difficult in the aspect of having to find the tools needed, and learning how to use them. Having no prior experience using the tools, meant learning how the program is used, how to deploy the exploit, etc |
| **How could the pre-training be improved?**  Having an experienced person who has used the software and tools needed, could have saved time, but also allowed others to benefit from the experience a trained professional has. |

## BLUE Team Evaluation

|  |
| --- |
| Activity name and description  **Ransomware attack using WannaCry malware**  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 a antivirus software / malware removal software installed prior to the exercise and having this in place would have alerted us to the fact that a ransomware was installed |
| 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 antivirus software  We also could have had a review of blocking domains via the firewall to refresh our familiarization of firewall config. We also should have taken a backup of the servers to support in recovery. |
| 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 antivirus 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?  Getting to know the antiviruses and malware detections being used in the exercise and the procedures taken once installed and in action. |
| 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 malware 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 analyse and anticipate potential Indicator Of Compromise (IOC) due to this system working with signature based, behaviour 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.
* Analyse 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 analyse 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.  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 defences.  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 analyse 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 defences. 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.

# Revision table

Given the outcome of blue and red team discussions about the exercise, the runbook is to be modified for improvements and the changes noted in the revision table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Modification** | **New revision number** | **Modifiers name** |
| 28/05/2023 | This is revision 1.2 | V1.2 | Giuseppe Raciti |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |