1. **NotPetya Response Process**
   1. **Preparation**

Planning and preparation are the keys to promptly responding to incidents and reducing their impact to a minimum. The defence of a system will be greatly improved if a well-trained team is present and provided with up-to-date documentation. All documentation (i.e., CIRP; workflows; inventory documentation; system/network logs; network and separate system configuration standards; contact information of the entities responsible for resolving the incidents) must be easily accessible and stored in a centralised location. Additionally, the following actions should be carried out to ensure the effective functioning of the Cyber Incident Response Team.

The organisation is also advised to create specific prerequisites to monitor the state of its network as this will help with quicker responses to possible incidents. Such actions can be (but are not limited to):

* Automated alerts when suspicious actions are identified (implementing IDS);
* Create baselines for various activities which cover the network, server, storage, and different applications;
* Daily review of IDS event logs;
* System backups;
* Clock synchronisation with trusted time sources (Network Time Protocol);
* Vulnerability management programs;
* Develop and maintain relationships/partnerships with governmental and third-party organisations (Law Enforcement, Insurance, Threat Intelligence, Digital Forensics, and Incident Response services). They can be used for additional support or even taking down adversaries (phishing websites, infected servers, etc.);
* Review personnel permissions based on their position.
  + 1. **Threat Intelligence**

Gathering Threat Intelligence will allow the team to understand the infrastructure of the organisation and its risks, who the potential adversaries may be, as well as their motivations and delivery methods. The information can be obtained from various sources – Cyber Defence departments of the government, Law Enforcement, and OSINT (open-source intelligence) such as security vendors and newsfeeds.

Furthermore, creating security architecture review routines and reviewing the policies for the organisation’s departments (HR, Management, etc.) will be beneficial and will ensure that a defensive structure can be thoroughly planned.

* + 1. **Training and Awareness**

Properly trained personnel are also vital for the safety of the organisation’s data and network. For this reason, awareness and training events are highly recommended for both regular employees and the CIRT. Annual recertification/training will ensure that the CIRT is well-informed about new and ongoing threats and ways to mitigate them or counter any infections. They should also be required to learn specific guidelines such as MITRE ATT&CK to become more familiar with how cyberattacks and intrusions occur. Regular staff should be informed regarding phishing campaigns and common social engineering techniques and flags (fearmongering, spearphishing, sense of urgency, poor grammar, fake email addresses) as many attackers obtain access to systems after employees provide them with login credentials or run suspicious files.

**<Organisation Name>**‘s Human Resources department must maintain a strict record of the staff’s security training to ensure that all personnel are properly instructed.

Together with the training and exercises, **<Organisation Name>** should carry out appropriate testing programs on their systems to sustain and refine their capacity to deal with incidents. One recommended program is **NIST Special Publication 800-84 Guide to Test, Training and Exercise Programs for IT Plans and Capabilities** but others may be used to better suit the organisation. Based on the beforementioned program, the testing should include annual penetration and Red Team tests, insider threat assessment and usage of simulated scenarios to examine **<Organisation Name>**‘s incident response plan capabilities (Ransomware, DDoS, Phishing, Data theft, Lateral Movement detection, etc).

* 1. **Identification**

It is important that the staff can properly identify the type of incident as reporting a false type would potentially result in more damages while the CIRT is attempting to mitigate and analyse the wrongly reported attack. Possible incident types for NotPetya infections are provided in Table 4.2.1 below this paragraph.

|  |  |  |
| --- | --- | --- |
| № | Incident Type Name | Incident Description |
| 1 | Phishing | Phishing can have two different incidents. The first type covers personnel from the organisation who receive suspicious emails from someone who claims to be a specific individual/organisation. The second type covers third-party individuals who receive an email from someone who claims to work in **<Organisation Name>** without being a part of the organisation. |
| 2 | Social Engineering | Attempts to gain access to the **<Organisation Name>**‘s data or systems by deceiving or extorting users – customers, staff, or external contractors. |
| 3 | Installation and/or execution of unknown software. | Any attempts or actual execution of unknown software on **<Organisation Name>**‘s devices. This covers both detections from anti-virus software and/or whitelisting software. |
| 4 | Loss, theft, or damage of company assets. | Any cases of loss, theft and/or damage of **<Organisation Name>**‘s data and devices. This includes removable media (external drives, USBs, etc.) and work devices (computers, IoT devices, etc.) |
| 5 | Impersonation | Any cases of account compromise/hijacking. It covers attacks on the **<Organisation Name>**‘s authentication capabilities, password sharing, suspicious login cases, accounts without a verifiable owner (zombie accounts), etc. |
| 6 | Network intrusion and enumeration | Any cases of network intrusion and probing – alerts generated by security equipment such as IDS/IPS (reconnaissance, a connection from outside devices, etc). |
| 7 | Privilege escalation | Any cases of users being moved to a group with more privileges or gaining excessive privileges through exploits or account switching. |
| 8 | Questionable use of legitimate privileges | Any case of a user abusing their privileges (accessing large amounts of data, sending data to unknown recipients, moving data to removable devices or inappropriate locations on the network). |

***Table 4.2.1*** *– Example Incident Types*

The sample was delivered before through an infected patch for a specific accounting software application as a “**.dll**” file. It is, however, also possible to be executed without owning the software through a CMD command. For this reason, Phishing, Social Engineering, Impersonation, and Installation/Execution remain. The malware also contains sophisticated propagation mechanisms, allowing it to enumerate the network, send copies of itself to uninfected hosts and even escalate privileges.

* 1. **Incident Reporting**

The successfully identified incident type and affected information should be reported to the appropriate entities. It is important that the staff can collect data to the greatest of their extent as it will set the priority of the incident and identify whether it should be reported to the authorities and if **<Organisation Name>** will require coordination with law enforcement or other third-party organisations. Some of the most valuable information about incidents is – the contact information of the individual/s reporting the incident, the type of the incident, hostnames and IP addresses of suspected systems, the type of affected data with its potential impact on other businesses/the country and a description of the activity with evidence (IDS logs, suspicious activity, phishing emails, etc.)

When the above information is obtained and forwarded, the **<Organisation Name>** can assign a priority to the cyber incident and then decide whether it is a cyberattack even which should be referred to the **CIRT** and any other affected entities.

In countries complying with the GDPR (Article 13), the appropriate entity (ICO for the United Kingdom) must be informed within 72 hours of the discovery of an incident which creates a “risk to the rights and freedoms of the involved parties”. The **<CIRT/Responsible staff member>** will determine if there is any data breach which requires it to be reported to a Data Protection Regulation organisation. If a decision to report the incident has been made, the following data must be provided:

* Contact data of the responsible staff member if more information is required;
* Description of the nature of the incident and an approximate number of affected individuals, as well as implications of the data breach;
* Description of any countermeasures and mitigation of adverse effects.

If the incident meets the requirements of local authorities, law enforcement and the appropriate governmental Cybersecurity department will be informed and offer any support where appropriate. The decision will be taken by the responsible staff member and can be reported even if the requirements are not met but a severe risk still exists.

* 1. **Analysis and Assessment**

In the event of a received alert for a NotPetya infection, the Core IT CIRT must research the incident and perform a rapid analysis of the situation. Those actions aim to acquire more information about which systems were affected, how was the infection delivered, and the severity based on the number and type of compromised systems. The first entity to receive the alert (the first Incident Responder) should conduct this investigation and provide the information to the incident manager. If the responder considers it appropriate, they can request additional help from other members of the CIRT. It is crucial to quickly identify whether the infection is real or if it’s a false positive alert due to the severity of the malicious software – false cases must be properly documented based on the incident-tracking procedures of the organisation. Due to the criticality of the infection, the severity score for NotPetya is **Critical**, and the incident must be escalated to the extended CIRT and possibly the government/law enforcement if required.

* + 1. **Severity Assessment**

One of the best ways to identify the criticality of an incident and its implications is by using a risk matrix. To create the matrix, this CIRP will use threat levels (types of threat in hierarchical order based on severity) and criticality levels (importance of systems/information in hierarchical order). Both can be found in descending order in Table 4.4.1 and Table 4.4.2 respectively. The tables are based on the examples in the Scottish Cyber Incident Response Plan Template.

|  |  |
| --- | --- |
| Threat Levels | Description |
| Threat 1 | Full compromise controlled by a human:   * External personnel without appropriate authorisation (cyber intrusion). * External stakeholders with inappropriate authority. * Internal staff exceeding intended authority.   Close-Access Breach (physical penetration of a site)   * Fake Wi-Fi network. * Router pivoting (redirection of traffic). |
| Threat 2 | Partial compromise controlled by a human:   * External personnel without appropriate authorisation (cyber intrusion). * External stakeholders with inappropriate authority. * Internal staff exceeding intended authority. |
| Threat 3 | Automated full compromise controlled by malware |
| Threat 4 | Automated partial compromise controlled by malware |
| Threat 5 | DoS (Denial of Service, affecting connectivity) |
| Threat 6 | Directed Scanning (vulnerability and open port identification) or malware not controlled by a command-and-control server. |

***Table 4.4.1*** *– Threat types converted to levels based on the Scottish CIRP Template.*

|  |  |
| --- | --- |
| Criticality Levels | Description |
| Criticality 1 | Enterprise-Wide Resources (Vital Services, Network Devices, DNS, Firewall. etc.). |
| Criticality 2 | Critical Data – Confidential Data (Intellectual Property, Blueprints, etc.). |
| Criticality 3 | Critical Systems (AD Servers, Web Services, etc.). |
| Criticality 4 | Sensitive Data – Restricted Data (Corporate Information, Financial Documentation, User Data, etc.). |
| Criticality 5 | Non-Critical Systems (File Servers and other systems that are not vital for the organisation’s workflow). |
| Criticality 6 | Regular Data and Separate Systems. |

***Table 4.4.2*** *– Criticality levels based on the Scottish CIRP Template.*

NotPetya is a type of malicious software that not only actively attempts to leverage improperly set-up user privileges, but also uses password-stealing mechanisms (Mimikatz) to obtain credentials and access the machines of those users. Additionally, it interrogates the infected network (both hosts and servers, including DHCP servers) and checks whether a specific file exists or not. This allows it to identify machines which were already infected. Furthermore, if it is unable to retrieve user passwords, the malware utilises the EternalBlue vulnerability to exploit vulnerable machines and gain access to them. For this reason, the type of threat is set to level 3, while the criticality level is set to 1.

The malicious software actively attempts to infect not only the host network but also spread to different organisations and any IP address it identifies. The process is automated and is possible to reach root-level privileges (threat level 3) while affecting all network-wide resources and assets owned by the organisation. This places it as a critical type of incident.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Criticality Level | Threat Level | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Critical | Critical | Critical | High | High | Medium |
| 2 | Critical | Critical | High | High | Medium | Medium |
| 3 | Critical | High | High | Medium | Medium | Medium |
| 4 | High | High | Medium | Medium | Medium | Low |
| 5 | High | Medium | Medium | Medium | Low | Low |
| 6 | Medium | Medium | Medium | Low | Low | Low |

***Table 4.4.3*** *– Risk Matrix based on the Scottish CIRP Template.*

* + 1. **Severity Guidance**

Based on the capabilities of the malware and the fashion it operates in, it can affect the entire corporate network of the organisation, as well as third-party organisations which may not even be related to **<Organisation Name>**. Based on the scale of the damage (on both local and external levels), multiple media outlets may be involved, and the organisation’s executives may require multiple levels of frequent reporting. In terms of the damage, it is possible to significantly disrupt the operations of unprepared organisations, destroy many assets and/or critical data, as well as pose life-threatening risks if the infection spread to medical equipment. Due to the Critical Severity Level of the incident, the organisation should assign the response duty to the entire CIRT and, if required, external entities such as Cyber Defence Departments (and equivalents) and/or law enforcement.

|  |  |  |  |
| --- | --- | --- | --- |
| Severity Level | Impacts | | IR Characteristics |
| Critical | | Highest level of severity. The impact can potentially be catastrophic for the company and its employees, including loss of business, public trust and/or impact on its operations. The following implications are indicators of this degree of severity:   * Threat to life or physical safety of customers, public or personnel. * Significant destruction of IT assets (hardware and software). * Significant disruption of business operations for a long period. * Significant damage to **<Organisation Name>**‘s reputation. * Significant destruction of corporate capabilities. * Risks of considerable financial loss. * Loss/Leakage of confidential information. | Due to the nature of this severity level, immediate and continual action from the CIRT is required. Such incidents have the highest impacts on the organisation and involve extensive and persistent operations, which often use complex attacks that are hard to counter. This severity level will trigger the policies of the Cyber Defence Departments of the country where **<Organisation Name>** is based. Possible indicators for such incidents are:   * Potentially involving law enforcement. * Potentially involving multiple media outlets and support from multiple organisations. * **<Organisation Name>**‘s executives will have an immediate and continual interest in the incident and its development. Possible requirement for multiple levels of reporting (regulatory and/or compliance). |

***Table 4.4.4*** *– NotPetya Severity Level*

The following entities must be contacted if the incident causes significant damage or spread to other networks (**Table 4.4.5**):

|  |  |
| --- | --- |
| Contact | Contact Details |
| <Local Cyber Defence Department> | Email:  Phone:  Address:  Comments: i.e., ask for specific staff title” |
| <Local Police Department> | Email:  Phone:  Address:  Comments: i.e., ask for specific staff title” |
|  |  |
|  |  |

***Table 4.4.5*** *– Entity Contact Details.*

* + 1. **Malware Identification**

It is important to use the initial triage to obtain additional intel regarding the malware and its appropriate artefacts. This includes a few subcategories – delivery, execution, and symptoms.

As previously mentioned, the malware was initially delivered with a software update for an accounting application, but the dynamic-link library file can be executed without owning the software. The DLL file can be delivered after an attacker obtains access to a host or through phishing and social engineering. If it is provided through the latter method, the adversary can provide instructions on how to execute it, together with other techniques such as soliciting a sense of urgency or fearmongering. All evidence (network and IDS/IPS logs, emails, unexpected connections) must be thoroughly documented as it can be used to identify how it was delivered from where and where it has propagated in the organisation or other networks. The identified suspicious files must have the following hashes - db349b97c37d22f5ea1d1841e3c89eb4 (MD5) and 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c (SHA256)

In terms of execution, as previously mentioned, the DLL requires a specific command to execute. It may be provided by the attacker or a new strain with easier execution may be released. To find the execution method, the symptoms can be analysed – altered files/registries and deleted local system logs. Some symptoms may also not be obvious, and they can be identified through basic static malware analysis – human-readable strings, implemented libraries and system functions. They will show additional information regarding its capabilities.

* + 1. **Evidence Preservation**

It is advised to not stop the machines as this will not only alter the evidence but also fully trigger NotPetya’s capabilities. The encryption process starts after the host is rebooted and a fake repair message is displayed. If images of infected machines are taken, the process should be done with a write-blocker to ensure the data is not altered. The permissions for the created image should also be changed to read-only.

* + 1. **Malware Analysis**

If more intel regarding the infection is required, the malware can be analysed to further prove its capabilities and nature. The analysis section can be split into basic and advanced phases. Each phase has two separate categories – static and dynamic.

The basic static analysis shows the functionalities of NotPetya without executing the malicious software. The hashes, human-readable strings, and blacklisted libraries/functions. The hashes can be used to easily identify common malicious applications on websites like **VirusTotal**. The strings and blacklisted libraries can show the functionalities of the malware, as well as other strings such as emails, ransom messages, names of embedded executables, etc. Examples of useful software are **Floss** (string extraction) and **PEStudio** (complete analysis of binary files)

The basic dynamic analysis executes the malware in a safe environment to see how it affects both the host and the network. Software such as **TCPView** (open connection monitoring), **Procmon** (process monitor for all actions executed on the system) and **Wireshark/Inetsim** (internet connection simulation and traffic monitoring) can be used to test the detonation conditions, as well as the behaviour of the sample.

The advanced analysis takes a more in-depth look at the malware by analysing its code and its exact functionalities, encryption algorithms and embedded files. The dynamic side of it aims to alter or prevent the execution of the files. One such method is the temporary kill-switch vaccine (create a file called **perfc** in “**C:/Windows/**”) may prevent the execution as the malware will consider the system as infected if the file is present. However, that name will change based on the name of the DLL file used to infect the system – i.e., if the file is called **NotPetya.dat**, the malware will look for a file called **NotPetya** in the beforementioned directory.

* + 1. **Documentation and Preservation**

It is advised to thoroughly document all steps of the analysis of the malware and if the previously mentioned capabilities are still present in the strain. Doing so will provide external entities (such as law enforcement) and the organisation’s executives with intel regarding the development of the situation, how many hosts/servers were infected, what assets/data was lost, and how it spread across the network. All intel must be presented in chronological order from the first received report for the incident to the containment, eradication, and recovery of the incident.

* 1. **Incident Containment**

The responsibility for the containment of NotPetya is given to the entire CIRT due to the severity of the infection. This can be achieved in a multitude of ways. It is highly recommended to contact law enforcement and third-party cybersecurity providers due to the severity of the attack. The following examples (but are not limited to) will show an example of how the incident should be contained (RedGoat, 2022):

* Quick actions – NotPetya is a type of malware which can cause severe destruction to a company’s data. Speed is a key requirement for damage minimisation.
* Identify systems, services, and timeframes (IP/MAC addresses, hostnames, protocols, active services, locations, user accounts and timestamps) and take appropriate actions against them:
  + Remove users from critical infrastructures;
  + Remove elevated privileges of users;
  + Stop any affected services;
  + Isolate any of the identified systems if needed;
  + Blacklist email/domain used by an attacker if the sample was delivered through social engineering.
* Isolate connections with external networks to prevent further spread. Infecting external partners/organisations will cause further issues and more work for the CIRT, making them less efficient.
* If required, contact specialists for help with the containment and documentation.
* Do not power off affected systems as this could alter valuable evidence and will encrypt the drive’s Master Boot Record.
* Identify, acquire, and preserve any possible sources of evidence:
  + Live and volatile data (encrypted files, network communications);
  + Application data (temporary files, system logs, hidden files);
  + Other logs (event, network traffic, Anti-virus/Yara detection);
  + Storage media (HDD/SSD, USB, MicroSD cards, etc.);
  + Metadata (dates, file access/creation/alteration times).
* Documenting all actions in chronological order (i.e., Chain of Custody System):
  + Personal information of the entity collecting and analysing the data as it must be done only by trained personnel;
  + Information regarding how the actions were undertaken (acquisition, preservation, analysis, and storage);
  + Backups for forensic copies and write blockers/permissions to ensure that all data will remain untouched and safe (i.e., ACPO Guidelines);
  + Any changes to forensic evidence (system shut down or any system changes to restore operations)
  + All evidence of a cyber incident must be secured within 24 hours.

If in doubt, further advice should be obtained from appropriate specialists such as Digital Forensic Analysts in third-party partner companies or the local police department.

* 1. **Incident Eradication**

After containing the incident and successfully analysing the cause and its effects on **<Organisation Name>**‘s assets and workflow, the extended CIRT must eradicate the incident. The following examples (but are not limited to) can be used to eliminate the cyberattack:

* Address the incident symptoms and correct them:
  + Malware infection:
    - Counter NotPetya’s capabilities (encryption, credential theft, network interrogation)
    - Attempt to halt any propagation mechanisms – disconnected all infected machines from the network
    - Discuss possible MBR decryption and recovery with external companies (though successful methods are improbable)
    - Do not pay the ransom – data will not be restored.
  + If a manual attack by an adversary was present (using the Pyramid of Pain or the Diamond Model):
    - Try to identify the attacker and any leads towards them or other systems they may be using
    - Find network and host artefacts related to the attack (installed software, altered files, file transfer, scan logs, etc.)
    - Identify the TTPs (Tactics, Techniques and Procedures) used by the adversary (i.e., MITRE ATT&CK) to show all steps taken by the attacker to access the system before executing the malware.
    - Make appropriate corrections (vulnerability patches, closing any backdoors, cooperating with other companies which may be affected by the attack, i.e., the attacker uses their servers)
* Address the root cause of the issue to prevent immediate reoccurrence:
  + Change network rulesets;
  + Change the IP address/network segment of the infected machines to prevent further spread;
* Constrain access to valuable data to users who need it for the normal operation of the organisation.
* Ensure backup data remains unscathed - If possible, keep backup data in online storage or a completely disconnected cloud storage as the malware may spread to that external network and render the data useless.
  1. **Incident Recovery**

Once the extended CIRT confirms that the attack has been eradicated, **<Organisation Name>** can act for the recovery of its operations back to a pre-incident state. It is still recommended to carefully monitor the network and its hosts (and their appropriate behaviour or services) to ensure that all vulnerabilities have been patched and that no traces of the incident remain. The following recovery actions (but are not limited to) can be taken:

* Restart stopped services after applying the newest security patches;
* Confirm host and application behaviour is benign;
* Conduct further vulnerability scans if the CIRT considers such as appropriate;
* Provide appropriate access to all personnel/customers to the data they are expected to access;
* If traffic was switched to a backup network, revert it to the main network;
* Restore systems with backup data;
* Request legal support – legal action can be taken against discovered adversaries.

1. **References**

Pownall, C. (2017). *Maersk NotPetya cyberattack response timeline*. [online] CharliePownall. Available at: https://charliepownall.com/maersk-notpetya-cyberattack-timeline/ [Accessed 26 Nov. 2022].

RedGoat (2022). *Maersk incident response*. [online] RedGoat. Available at: https://red-goat.com/why-you-should-test-your-incident-response-a-review-of-the-maersk-incident/ [Accessed 28 Nov. 2022].

Georgiev, M. (2022). *Analysis and Comparison of WannaCry and NotPetya*. [online] Github. Available at: https://github.com/Kyd1ct/Analysis\_and\_Comparison\_of\_WannaCry\_and\_NotPetya/commit/8ff0172ef1877dc6035d554379cdae4d40e8dbf4 [Accessed 28 Nov. 2022].