# **SnakeKeylogger Response Process**

## **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.

## **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.

## **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** (Grance; Nolan; Burke; Dudley; White; Good, 2006) 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).

## **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. Some of the most common incident types 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.) |

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

As this is a sophisticated keylogger, it is important to classify the data held on the infected machine/s. The malware attempts to steal various information from the victim’s machine including browser credentials, credentials of installed applications, clipboard contents, keystrokes and so on. Some samples can even take screenshots of the whole screen or specific windows without the user’s knowledge. Based on the stolen data, the consequences may be catastrophic for an organisation or even an entire country based on the class of the data. Since the samples lack any propagation mechanisms other than phishing emails and social engineering, infections may be unlikely if the staff are properly trained to recognise such attacks.

## **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.

## **Analysis and Assessment**

The Core IT CIRT is required to perform the initial triage in case of an infection with SnakeKeylogger. Those actions should aim to obtain more information about the infected systems, how it was delivered, and the severity based on the number of infected machines and the data they held. The first Incident Responder should conduct the investigation and provide the information to the incident manager. If they consider it to be appropriate, they can request additional help from the rest of the CIRT members. Due to the behaviour of the malware, it is unlikely to require more members unless multiple users have executed it on their machines. It is crucial to identify whether the infection is real or not and any false cases must be thoroughly documented based on the incident-tracking procedures of the organisation. If the incident is legitimate then the responder must identify the scale and the infected machines.

Due to the nature of the keylogger, the severity score of the malware can be either **High** or **Medium** based on the information held by the infected members of the organisation. If necessary, the organisation should contact law enforcement or the government to notify them about leaked data that may threaten the organisation, civilians and/or the country.

## **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.*

SnakeKeylogger is a type of malicious software that steals data from an infected user’s device. As the malware does not have any propagation mechanisms, does not attempt to elevate its privileges, and does not pose a risk to people’s health or the organisation’s physical assets, the incident can be placed as **Medium** or **High** depending on the affected data. This, of course, may vary based on the samples (newer samples may adopt more sophisticated techniques) and the affected organisation.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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.*

## **Severity Guidance**

As Snakekeylogger is a malware focusing on data theft, the severity could be either high or medium depending on the privileges of the infected user. The malware has no sophisticated means of propagation, making it a social engineering and phishing threat. Affected high-privileged users could provide the adversary with credentials to crucial web applications or even servers, allowing the threat actor to potentially cause significant damage.

|  |  |  |  |
| --- | --- | --- | --- |
| Severity Level | Impacts | | IR Characteristics |
| High | | Substantial impact affecting the proper operations of **<Organisation Name>**‘s business operations, public trust, and impacts on their personnel. The following impacts are indicators of this severity level:   * Large loss of confidential data, restricted information, and public confidence. * Destruction of corporate assets and capabilities with a large impact. * Substantial disruption of the normal operation process. * Large damages to the reputation. * Risk of large financial loss. | Albeit milder than the previous severity level, this one also requires the immediate attention of both the Core and extended CIRT. It may require extended work hours or even around-the-clock response activities. Such incidents have substantial negative impacts on operations and involve persistent and sophisticated attacks. Such attacks require large amounts of resources to contain, control and counter them. This level will also trigger policies from the local Cyber Defence Department. Possible indicators of this incident are:   * **<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). * Potentially involve law enforcement, engagement by some media outlets and support from multiple organisations. |
| Medium | | Moderate impacts on the proper functionality of **<Organisation Name>**‘s business operations and personnel. The following implications indicate this severity level:   * Some disruptions in the operations over a sustained period. * Limited loss of public trust and reputation damage. * Moderate loss/manipulation of restricted data. * Risk of moderate financial loss. * Multiple business departments and sites may be affected. | This severity level requires the notification of the extended CIRT and may involve several or most of its members. Selected members from both Core and extended CIRT may be selected to engage with the incident response. Initially may require extended work hours until the situation is contained. Such incidents have some impact on the organisation and involve attacks which require an organised effort to counteract. This severity level also triggers the policies of the local Cyber Defence Department. Possible indicators are:   * May require external support. * May involve law enforcement and a limited level of reporting. * Not likely to involve media outlets |

***Table 4.4.4*** *– Severity Levels Example Table (*UK Cabinet Office, 2018)*.*

The following entities must be contacted in cases of severity levels above **<Severity Level>** (**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 is delivered through social engineering attempts. With this, suspicious emails containing urgent/fearmongering messages will be the most common means of infection. 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’s network. As there are numerous samples of the Keylogger showing each day, it is hard to provide a complete list of hashes. Examples of hashes from February 2023 are:

* e8e100895fa60d667eb81cc2fb660ac12dd998f8f20aa6d7e0ea942854dc831f
* 7e1d956fe3ab418c915d24faecac0798be86b86a4244580ebf8af91bc01f752f
* ae1c76298164414736639b05b24e5c12078d7cffb85163b92cde019d943a62d5
* 2cc5b915835368d59f7a46adb02593d468bfa0cd63eea856e9e4cd55b29f8afb
* dfe752002f955e1facba9518dc6ac3854b9aa6ec196fcc22068f41e4f5c87cf3
* bde58e12d41cd833eb907de3955528c3ba4ea45f7e825b6ca038f74eaf594d26

In terms of execution, the file does not need to be run with administrator privileges. Execute itself and steal data even when it is run by a low-privilege account. The detonation symptoms will not be obvious, as its functions are done in the background, without displaying any windows or messages.

* + 1. **Evidence Preservation**

It is advised to not stop the machines as this will alter the evidence. If images of the infected machines are taken, the process should be done with a write-blocker to ensure the data is not altered. It is only advised to stop the services related to the malware (name will differ based on the sample – i.e., **fzpceresn.exe**) as this will stop it from stealing more data.

* + 1. **Malware Analysis**

If more information about 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 based on the capabilities of the handling team. Each phase has two distinct categories – static and dynamic.

The basic static analysis shows the functionalities of the binaries carried by the bundleware without executing it. Hashes, human-readable strings, and blacklisted libraries/functions can show a lot of information about a malicious sample. The hashes can be used to identify common malware on databases like **VirusTotal**. The strings can show how it will possibly affect the system if it tries to contact any website/C&C server, 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), **Wireshark/Inetsim** (internet connection simulation and traffic monitoring), and **Volatility** (memory forensics) can be used to test the detonation conditions, as well as the behaviour of the sample (multiple stage payloads, encryption, data theft, etc.).

The advanced analysis takes a more in-depth look at the malware by analysing its code and exact functionalities, encryption algorithms, and embedded files. The dynamic side of it aims to alter or prevent the execution of samples. Advanced analysis can be extremely helpful and may even show well-hidden information that cannot be found with automated tools. It, however, requires in-depth technical knowledge to be effective.

* + 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.

## **Incident Containment**

The responsibility for the containment of the incident is given to the core or extended CIRT depending on the scale of the attack. This can be achieved in a multitude of ways depending on the type of infection and its capabilities. The following examples (but are not limited to) will show various ways of different cyber incidents:

* Identify systems, services, and timeframes (IP/MAC addresses, hostnames, protocols, active services, locations, user accounts and timestamps) and take appropriate actions against them:
  + Stop any services related to the spyware;
  + Identify any open connections;
  + Stop the internet connection of the machines as they would not be able to send the data to the adversaries;
  + Isolate the identified systems if needed.
* If required, contact specialists for help with the containment and documentation.
* Do not power off affected systems as this could alter valuable evidence
* Identify, acquire, and preserve any possible sources of evidence:
  + Live data (RAM, network connections);
  + Application data (temporary files, emails, images, swap, and hibernation files);
  + Logs (event, network traffic, Anti-virus);
  + Electronic documents (databases, PDF files, presentations, documentation);
  + Storage media (HDD/SSD, USB, MicroSD cards, etc.);
  + Metadata (dates, authors, 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) (ACPO, 2007);
  + Any changes to forensic evidence as sometimes they are required to access specific data (i.e., Phone rooting to bypass its password);
  + 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.

## **Incident Eradication**

After containing the incident and successfully analysing the cause and how it affects **<Organisation Name>**‘s assets and workflow, the core or extended CIRT (depending on the scale and severity) must eradicate the incident. It can be achieved in multiple ways depending on the type and cause of 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 SnakeKeylogger’s capabilities (data theft and communication with external servers);
    - Attempt to find and eradicate any persistence mechanisms;
    - Attempt to halt any propagation mechanisms – identify the malicious email addresses;
  + Manual attack by an adversary (using the Pyramid of Pain (Bianco, 2013) or the Diamond Model (Caltagirone; Pendergast; Betz, 2013)):
    - 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 their capability capacity and the adversary’s arsenal – what tools were used and what vulnerabilities/exposures allowed the exploitation of the network;
    - Identify the TTPs (Tactics, Techniques and Procedures) used by the adversary (i.e., MITRE ATT&CK) (MITRE, 2018) to show all steps taken by the attacker to compromise the system.
    - 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;
  + Constrain access to valuable data to users who need it for the normal operation of the organisation.
* Identify the stolen data and discuss potential consequences for the affected organisations and/or people.

## **Incident Recovery**

Once the core or 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;
* Ensure performance (separate host performance and network bandwidth) remain unaffected as in the pre-incident state;
* 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;
* Request legal support – legal advice will be beneficial in case of data theft.

# **References**

CM Alliance (2015 – Present Day). Cyber Incident Response Plan Template. [online] Available at: https://www.cm-alliance.com/cyber-incident-response-plan-template [Accessed 29 Oct. 2022].

Scottish Government (2021). Cyber resilience: incident management. [online] Available at: https://www.gov.scot/publications/cyber-resilience-incident-management/ [Accessed 15 Nov. 2022].