# **FileTour 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. Possible incident types for a FileTour-related infection 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 | Privilege escalation | Any cases of users being moved to a group with more privileges or gaining excessive privileges through exploits or account switching. |
| 7 | 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). |
| 8 | Inappropriate use of devices | Any cases of illegal activity of staff members through company assets. This includes browsing inappropriate websites, threatening/obscene/harassing communications, access/storage of illegal data and any other actions breaching the law and **<Organisation Name>**‘s policies. |
| 9 | Performance decline | Installing a lot of freeware and constantly showing ads may reduce the performance as the system’s resources will be used by malicious processes. The network’s bandwidth may be used to attack other victims as FileTour is known to be used for massive botnets. Some samples also contain crypto mining capabilities, using the infected system’s resources to obtain cryptocurrencies for the adversary. |

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

Depending on the affected organisation and possible capabilities of some FileTour strains, the malware could affect all three types of data classifications – **Official**, **Secret** and **Top** **Secret**. The infected organisation must carefully classify the data they hold, as well as how and what parts of the data are affected by the attack. Based on the data they must then identify the possible aftereffects for both civilians and diplomats, as well as the safety of the country.

Additionally, knowing that some strains can impersonate the infected users, organisations must be properly trained to recognise phishing attempts as this is the main way of propagation for the known samples found in the wild. Organisation members must be trained to recognise phishing attempts if the malware is not caught by the organisation’s IDS/Anti-Virus.

## **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**

In an event of an infection with FileTour, the Core IT CIRT must research the incident and perform an extensive analysis of the situation. Those actions must aim to obtain more intel about which machines were infected, how was the infection delivered, as well as the severity based on the types of the number and types of compromised systems and data. The first entity to receive the alert (the first Incident Responder) should conduct this investigation and then forwards the information to the incident manager. If the responder considers it appropriate, they can request help from other members of the team. It is crucial to identify whether the infection is real or a false positive as soon as possible, as the known strains could not only show interruptive ads but also steal valuable data and/or encrypt the user‘s files. Any false cases must be properly documented based on the incident-tracking procedures of the organisation. Due to the known capabilities of the infection, the severity score for FileTour is **High** and the incident must be escalated to the extended CIRT. Based on the affected information it must also be escalated to the government/law enforcement.

## **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.*

FileTour is a malicious bundleware used to deliver multiple files to the infected system. Some files may even be authentic freeware, while others may be exploited vulnerable freeware (altered to execute malicious code on start-up). The malware is severely obfuscated and contains multiple techniques for evasion detection and persistence. Some also have multi-stage payload drops, with some payloads being downloaded from external servers. FileTour is mainly known as Adware, but there are known cases of sophisticated spyware, botnets, and a combination of multiple or all three types with privilege escalation and backdoor capabilities. This places the incident as a High Severity Level threat as it may cause catastrophic damage to the reputation of 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**

With the following guideline, **<Organisation Name>** can categorise the severity of an incident based on the obtained intelligence and potential implications to the organisation. It will help with a critical decision point in the process of countering the attack – prioritisation of the response and its appropriate resources. The CIRT must tackle incidents based on multiple factors – the risk they pose to the organisation and its assets (both digital and physical. This section will give further information regarding the severity scores (Critical, High, Medium, and Low) from the Risk Matrix in section [**4.4.1 Severity Assessment**](#_Severity_Assessment)as well as the structure of how to determine the risk levels in **Table 4.4.4**.

Based on the capabilities of the malware and the fashion it operates in, it could potentially affect the entire corporate network of an organisation. Based on the scale of the damage, some samples contain cryptographic capabilities which may be used to encrypt files in the affected system. As some samples were used as botnets with backdoor capabilities, the organisation could have legal issues if their machines were used in the attack of another corporation. This may also severely affect the system’s resources and bandwidth, slowing down both the machines and the network. Due to the High Severity Level of the incident, the organisation should assign the entire CIRT and, if required, external entities such as Cyber Defence Departments and/or law enforcement.

|  |  |  |  |
| --- | --- | --- | --- |
| 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. |

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

Due to cases of FileTour botnets, the following authorities should be contacted: (**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.*

## **Severity Guidance**

It is important to conduct an initial triage to obtain more information about the malware and its artefacts. This includes a few subcategories – delivery, execution, and symptoms.

As previously mentioned, the malicious software’s main means of propagation are through social engineering and phishing techniques – email attachments, disguised as popular freeware or pirated software. If it is delivered after an adversary obtains access to a machine, they may upload it and execute it as administrator privileges are not required. Some strains have built-in capabilities to escalate their privileges and obtain full access to the machine’s resources – files, security logs, and tokens. It could also impersonate all users in the same session and any clients which connect to the machine. All evidence (IDS/IPS logs, emails, unexpected connections, memory forensics, files, and system changes) must be thoroughly documented as it can be used to identify the exact capabilities of the sample, how it ended on the system, as well as how it behaves (connections to any C&C servers, cryptographic functionalities, specific data theft, etc.)

As the FileTour samples and strains are broad, the team must look for the following (but not extensive) known **SHA256** hashes:

* ab5e597bf7316bd8fcaeca8cddeec38a9585704a7929d50ea92ba603b038d7f3
* ff2fba623a5fef5ad2ab852079c88fbe33d12e48cfb0a06c90390d4a19270d2c
* e6dff8475541ebddc1f0db47a311eb2c25581b7d5e62af8066d59c283114c2d3
* 8fe6c86b038ce91a991fe6eb8a9b323bb37b554ff6b4e5c18de3fe52d4aedf6d
* aa3c8a767a538de40293e531aba50c4cfa189510927a22d028f3e34f2997bf95
* da6332feebc2a530509de0c661231bbd427327c31d6607a6a9286db710b68795
* 9c9cdb438163a2e64adcb398a6f1f1abcdc81c1cf35ab5728441104a151240fd
* 4f4c2c9bdfef8a8cfbe2c8f84bf12cc86f26f59d54c277dab39f4c5e92948708
* 9453ddc4bebb87a937e3d53d38c56814907b2862496142ccdb568f48caf2d467
* 9c83561fb5253478d523e0ca20900b7e0ce87e60f686bfea25c9ca99716257c2
* 719838a1192ae6b53966159da56635e7a05754eb017f2538ca3f82c580543280
* d2d90f02ccd7c3fd1b46d667081529a1af8172e4a51feda461c8d250081c3548
* b3af0eb6e6ddce0f2e2993634d4b3edd86b3584c0c6f6000c5f94379f491698d

Other samples can be found in various forums such as Malware Bazaar. Regarding the execution, as previously said, some strains do not require administrator rights. Some symptoms may not be obvious as the samples try to remain hidden and evade any sort of detection by using self-modifying code and silent scripts to install the payloads.

## **Evidence Preservation**

It is advised to not stop the machines as this will alter the evidence. Stopping the machine’s internet connection can stop its communication with external servers/the botnet. If an image of the machine is taken, the process should be carried out with a write-blocker to ensure the data does not alter itself. Additionally, the permissions for the newly created image should be changed to read-only.

* + 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/Command & Control 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 the response process. 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, how it spread across the network and what measures were taken. 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:
  + Remove users from critical infrastructures;
  + Remove elevated privileges of users;
  + Stop any affected services;
  + Isolate any of the identified systems if needed.
* Isolate connections with external networks to prevent further spread or execution of multi-stage payloads. Network isolation will also ensure that the sample could not communicate with any C&C servers.
* 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 and volatile data (encrypted files, 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);
  + Mobile phones (call logs, contacts, emails, SMS, and appropriate application data);
  + Storage media (HDD/SSD, USB, MicroSD cards, etc.);
  + Metadata (dates, authors, access/creation/alteration times);
  + Navigation data (GPS data).
* Documenting all actions in chronological order (i.e., Chain of Custody System):
  + How was the sample delivered – social engineering, false freeware, or pirated software;
  + 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:
    - Identify the malware’s capabilities;
    - Counter the FileTour strain’s capabilities (encryption, data leakage, backdoor functionalities, bandwidth decline, command-and-control server control);
    - Attempt to find and eradicate any persistence mechanisms – altered services/hidden scripts;
    - In case of file encryption – consult third-party organisations regarding the risks of attempting decryption and possible data leakage/destruction;
    - If a backdoor is present, identify the backdoor it has created and stop it to prevent adversaries from accessing the network.
    - In case of a ransom – do not pay it.
  + 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;
  + 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;
* Ensure that no sensitive data was leaked.

In case of encryption or data leakage, law enforcement should be contacted immediately so they can respond to the crime. If any backdoor functionalities, bandwidth decline or C&C servers are present, the connections/processes should be identified and terminated. If possible, the internet connection to the infected machine should be stopped until a botnet is ruled out.

It is advised to contact law enforcement or a third-party incident response organisation if a manual attack was present. Identifying how the attack occurred and how it has affected the network may be harder unlike malware as an adversary can make changes to their strategy in real-time and does not follow specific commands.

## **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 if data was stolen/leaked.

# **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].