## Incident Investigation Report

### Incident ID: INC-123456

### Investigator: Example Name

### Restrictions: CONFIDENTIAL / TLP:AMBER

# 1 Table Of Contents

Insert Table Of Contents manually here. In Word choose “References” on the ribbon menu, click the first option “Table Of Contents”, click “Built in” -> “Automatic Table 1” or whichever style you prefer.

Unfortunately there doesn’t seem to be a reliable way to insert the TOC anywhere except the first page using Pandoc, so a manual workaround is required.

Table Of Contents goes here.

# 1.1 Report revisions

Use versioning for the reports. The first delivered version should be 1.0, and the revised version that takes into account customer feedback should increment minor versions.

This table shows the version of this report file. Previous versions are listed in a chronological order. Major changes are noted in the Comments column.

| Version | Published date | Author | Comments |
| --- | --- | --- | --- |
| 0.1 |  |  | First draft |
| 0.5 |  |  | Quality assurance |
| 1.0 |  |  | Release version |
| 1.1 |  |  | Final version |

# 1.2 Distribution list

The final report will be delivered to the following people:

| Name | Role | Method |
| --- | --- | --- |
| Ellie B. Example | Chief Information Security Officer | email |
| Aaron A. Aaronson | Security Specialist | email |
|  |  |  |
|  |  |  |

# 1.3 Disclaimer and reading guide

This part can be left as-is and included in the report. It provides guidance to the reader on how to interpret the report contents.

This report has been written based on the facts found during an investigation into a cyber security incident. The investigation conclusions and findings are based on the materials delivered for inspection and discovered during the investigation. All findings in this report are subject to change if new evidence is discovered or presented to the investigation team.

## Timestamps

Unless otherwise stated, all timestamps are presented in [Coordinated Universal Time](https://en.wikipedia.org/wiki/Coordinated_Universal_Time) (UTC) following the [ISO 8601](https://en.wikipedia.org/wiki/ISO_8601) format. The timestamps follow the following general format: YYYY-MM-DDTHH:MM:SSZ. The trailing Z signifies that the timestamp is presented in UTC. Standardizing on UTC allows the timestamps from globally dispersed systems to follow a common timeline. Some timestamps might be presented as a deviation from UTC when necessary (For example EET time stamps will be presented as UTC+2).

Example: 2024-10-04T11:15:12Z, 2024-10-04 11:15:12 (UTC+2)

## Statements of probability

All statements of fact are presented within a range of probability. The probability of all conclusions is based on the expertise of the investigation team and the quality of the evidence presented. Nothing in this report is presented with absolute certainty, especially conclusions that are reached due to the absence of evidence to the contrary. The following normalized statements will be used to convey the degree of certainty in any finding or conclusion:

| Chance percentage | Statement or wording |
| --- | --- |
| 1-10% | Very Unlikely, Almost certainly not, Very Improbable |
| 11-40% | Not Likely, Unlikely, Improbable |
| 41-60% | Even Chance |
| 61-90% | Probably or Likely, Strongly Suggested |
| 90-99% | Very Likely, Almost Certainly or Very Probably, Very Strongly Suggested |

## Statements of confidence

In addition to a statement of likelihood, a statement of confidence can be written. The statement of confidence is based on the subjective judgment of the investigation team on how the quality and amount of evidence affects the statement of likelihood. A confidence clause can be expressed using a three steps:

| Asserted with… | Description |
| --- | --- |
| High Confidence | The evidence strongly supports the statement, there is a large amount of evidence to point towards the conclusion and there is no evidence that would disprove the conclusion. |
| Medium Confidence | Asserted with Medium Confidence: The evidence supports the statement. The amount of evidence is sufficient, but other evidence could possibly surface that would question the conclusion. There might be evidence that would disprove the conclusion, but such evidence has not been presented. |
| Low Confidence | Asserted with Low Confidence: There is missing evidence and major questions are left unanswered. A single piece of contrary evidence could disprove the claim, but it has not been found. The statement seems logical and can not be immediately disproven. |

Example:

On October 3rd, 2024, at approximately 14:32 UTC, XDR logs recorded suspicious activity originating from a laptop (LAPTOP-E5SFX3) assigned to a user in the marketing department. The logs showed an executable file update.exe being run from an uncommon directory (C:\Users[username]\AppData\Roaming\Temp). The sequence of events, combined with the file’s unusual behaviour, **strongly suggests** malicious activity.

The file executed from a temporary directory and attempted to connect to an external IP address known to host malicious content. Given these factors, it is **very likely** that update.exe is a malware executable attempting to establish communication with a command-and-control (C2) server. **This is stated with high confidence.**

## Investigators interpretation

The report text describes material findings that are based on the evidence presented. All conclusions, derivative theories or interpretations of facts are presented separately as a discrete quote. This quote will have the heading “Investigators interpretation”, and it contains the subjective interpretation of the presented facts guided by the expertise, experience and skill of the investigation team or investigator. The interpretation is not presented as a material fact, but as an educated opinion.

Example:

**Investigators Interpretation**

\*It is likely that the malware originated from a malicious email received by the recipient on the Outlook desktop application. However, no email logs were present and the users inbox was deleted before the investigation, so it is not possible to verify this interpretation. However, the location where the malware was found is typically the location where Outlook stores downloaded attachments, and there are several forum posts on the internet describing similar attacks with email being the initial attack vector.

# 1.4 Intended audience

Describe who the report is written for. If the report is highly technical, define which technical experts would most benefit from reading it. Remember, that the intended audience is not necessarily the final audience - a report might be read in court, it might be circulated among top leadership in a company, or handed out to external experts for scrutiny.

Defining the intended audience will help readers understand the level of technical sophistication required to read the full report. Some parts, like the conclusions and the executive summary, should be understandable by all stakeholders, including non-technical people and experts in other lines of business than IT or security.

This report is written for a technical audience like system administrators, security personnel or other people who work in roles related to the technical environment. The executive summary, conclusions and recommendations are written for all stakeholders.

# 2 Executive Summary

A clear and concise summary of the event, excluding technical details unless absolutely necessary. The executive summary should be written for a business audience with no assumed technical expertise. The summary should be written last, after all other reporting is done and the investigation is concluded. The target length of the executive summary is less than one printed page. It should encapsulate the report’s purpose, key findings, and actionable recommendations without delving into technical jargon.

Start by clearly stating the most critical information, such as the nature of the cybersecurity incident, its impact on the organization, and the steps taken to mitigate it. For example, instead of detailing every technical aspect, you might say, “Our investigation revealed a data breach that compromised sensitive information of 500 users, prompting immediate remediation actions and enhanced security protocols.”

This approach ensures that decision-makers can quickly grasp the essence of the report and understand the implications for the organization. Additionally, structure the executive summary to include essential sections such as key findings, incident summaries, and remediation recommendations. It is also beneficial to include metrics like time from detection to resolution and possible economic impacts where they are clearly measurable.

# 2.1 Business Impact Analysis

For writing a BIA chapter, it is essential to follow a structured approach to assess the potential implications of the incident on the organization’s operations. First, identify and outline the critical assets and processes that may be affected by the current incident. This includes evaluating key IT systems, communication channels, and any interdependencies that exist between various departments. Understanding which components are vital for business continuity will provide a foundation for assessing the overall impact.

Next, conduct a preliminary risk assessment to evaluate the likelihood and potential severity of the ongoing cyber threat. This involves analyzing how the current incident could disrupt essential business functions and estimating the financial and operational repercussions. For example, consider factors such as potential downtime, loss of revenue, regulatory fines, or damage to brand reputation.

Once these impacts are quantified, prioritize them based on their significance to the organization’s objectives. This prioritization will inform decision-makers about where to allocate resources effectively for mitigation and recovery efforts.

Lastly, ensure that this BIA chapter includes recommendations for immediate actions and long-term strategies to enhance resilience against similar incidents in the future, emphasizing the need for continuous updates as new information about the incident emerges.

## 1. Immediate Impact:

* **Unauthorized Access:** The malware exploited the open RDP session, gaining access to the domain controller and compromising the entire domain.
* **Service Disruption:** Critical services such as email, shared drives, authentication, and internal applications were disrupted, halting business operations.
* **Malware Propagation:** The malware rapidly spread across the network, infecting multiple systems and increasing the scope of the incident.

## 2. Short-Term Consequences:

* **Financial Losses:** Operational downtime resulted in lost productivity and potential ransom demands.
* **Data Breach Risk:** Sensitive company and client data were potentially accessed or exfiltrated.
* **Loss of Trust:** Clients, partners, and employees expressed concerns about data security and operational reliability.

## 3. Long-Term Ramifications:

* **Reputational Damage:** The incident harmed the company’s reputation, potentially leading to customer attrition and difficulty acquiring new clients.

# 2.2 Investigation limitations

All investigations have limitations - logs go back only so far, endpoints can not be acquired for forensic analysis, there is time pressure and sometimes the customer sets a time limit on how long an investigation can go on.

In this chapter, outline the main limitations of the investigation and explain their effect on the depth and detail of the report. Describe which logs were not available, or how an insufficient retention time limited looking back in time. If devices were not available due to lack of remote tools or physical access, describe that.

This chapter can also hold recommendations on ensuring that necessary digital evidence is available when it is needed. Log time retention is a common problem in DFIR investigations, so describe which logs are insufficiently retained.

Suggestions for log time retention can and should be derived from common standards. One easy to remember option is PCI DSS, which requires that logs are available 90 days indexed and searchable, and retained 365 days in cold storage. This can provide a good guideline for making recommendations to your customer going forward.

Lack of internal resources is also a limitation, but be careful not to disclose too much when describing lack of personnel on the service provider’s side.

* Logs were available only for the last two weeks on endpoints XXX and YYY
* AV was installed but was not updated since 2021
* Firewall logs were not collected
* Workstation XYZ was wiped before a forensic image was collected

# 2.3 Investigation goals and targets

The goals of the investigation are the outcomes that the investigation aimed to reach. These are best formulated in the form of research questions that can then be answered in the final conclusions. Forming the investigation goals into research questions helps to guide the investigation and keep the goal clear - this limits the risk that an investigation will dive into rabbit holes and lose focus of what the main goal is.

Research questions can be augmented with subquestions, and these should be reiterated in investigation sync meetings.

Example investigation questions:

## Investigation research questions

* What was the initial point of entry to the network?
  + Subquestion: What method was used to gain initial access?
* Which credentials are suspected of being compromised?
* Are there any signs of data exfiltration?
* Was personal data compromised?
  + Subquestion: How many records were suspected or confirmed compromised?
  + Subquestion: Which regulatory environment did the data breach happen in?

# 2.4 Glossary of terms

When proofreading the report, make sure to expand all less-known acronyms inline and gather them on this page for a more detailed explanation. Terms of the trade, tools and software should be described when first referenced. Even though terms like IDS, IPS, Snort, Firewall and Port scanning are regular occurences in the DFIR expert’s daily life, they might require explanation to lay audiences.

Terms used in this report are gathered here with their brief explanations.

| Term | Explanation |
| --- | --- |
| IDS | Intrusion Detection System, a system (software or hardware) that detects and alerts on network intrusions |
| IPS | Intrusion Prevention System, a system (software or hardware) that detects and blocks traffic considered malicious |
| Port Scanning | The process of enumerating open services and communication ports on an endpoint |
|  |  |

# 3 Timeline of events

Write a sub-chapter explaining the two following timelines, or choose one to structure your report around. There are two distinct timelines that can be used to describe the chronological order of events. The timelines run parallel, but describe different things. In cases, where it is reasonable to combine these timelines, that should be done but beware of complexity. Any sufficiently complicated attack chain intermixed with the investigative actions will quickly render the timeline unreadable.

Consider adding a graphical overview timeline that shows the main events on a visual line. This will serve as a timeline summary and make it easy to understand the order of the unfolding events. The detailed timeline can be presented as a table that contains columns for a timestamp, event, the affected resource and who was either responsible or acting on the issue. The investigation timeline should describe the steps taken by investigators and other personnel who were working on identifying, containing, eradicating and recovering from this incident. This timeline typically contains things like shutting down machines, resetting credentials, removing malware and restoring backups.

Additionally, you can add a graphical high-level timeline showing the most significant events of the investigation to summarize the table.

The next main chapter, Investigation description, is where the investigation story is told. Timeline entries should be short, concise and clear.

# 3.1 Incident timeline

The incident timeline records the events from first breach to end of attacker activities. This timeline starts from the earliest detected adverse event.

| Time and date (UTC or local time) | Event | Source | Destination |
| --- | --- | --- | --- |
| 2024-12-17 13:12 | RDP connection initiated with user admin01 credentials using password authentication. | 92.239.292.23 | XMPL-DC02 |
| 2024-12-17 15:16 | First detected Cobalt Strike beacon traffic | XMPL-DC02 | 102.394.22.123:53 |

# 3.2 Investigation timeline

The investigation timeline details the events that took place during the incident response process.

| Time and date (UTC or local time) | Event | Resource | Actor / responsible |
| --- | --- | --- | --- |
| 2024-12-17 15:18 | ThreatHunter EDR alert: Cobalt Strike beacon detected on server | XMPL-DC02 | SOC |
| 2024-12-17 18:21 | Tier 1 analysis concluded the alert to be a true positive, escalated to Tier 2 | - | SOC |
| 2024-12-17 18:45 | Requested permission to start DFIR investigation | - | SOC |
| 2024-12-18 09:11 | DFIR permission granted, investigation started. | - | Firstname Lastname @ Customer |
| 2024-12-18 09:18 | Requested server snapshot for forensic analysis from customer data center team (datacenter@customer.tld) | XMPLC-DC01, XMPLC-DC02 | SOC DFIR Team |

# 4 Investigation

This is the main chapter of the report. This is where you describe the investigation method, how the investigation started, what actions were taken, what outcomes came out of those actions and how the incident was resolved.

This chapter should be broken down into subchapters that describe the individual “subplots” of the investigation. This is guided by the investigation itself - typically compromised accounts, compromised endpoints, malware analysis and such can get their own chapters. If the description of an event runs several pages, it should be broken into constituent parts. Remember, that often different readers will have different emphasis on what chapters they focus on, so separating things like how accounts were compromised and abused from how the network segregation was not sufficient is a good idea.

For readability, use a monospace font to differentiate usernames, servernames, ip addresses and software used. This makes it easier to follow along the text when descriptive words are clearly separate from technical terms. Use code blocks for lists like IP addresses if such are presented. Remember, if a list is multiple pages long, it belongs in an attachment, not in the middle of the report.

For an example case, this chapter might look something like this: ## 4.1 Account compromise for admin01 #### 4.1.1 Initial access on admin endpoint #### 4.1.2 Privilege escalation attempts on endpoint #### 4.1.3 RDP password spraying attacks on domain controllers ## 4.2 Attacker activities on XMPL-DC02 #### 4.2.1 Lateral movement and abusing CVE-2021-12345 #### 4.2.2 Compromised credentials on server #### 4.2.3 File passwords.txt on server desktop ## 4.3 Indicators of compromise #### 4.3.1 Further activities from suspected IP addresses #### 4.3.2 YARA results on found malware hashes

# 5 Conclusions and recommendations

This chapter carries the conclusions of the investigator. A good way to approach the conclusions is to take the original research questions and attempt to answer them based on the facts uncovered by the investigation. Questions that no definitive answer was found for should also be addressed here, and the explanation for why the question could not be answered should be found in the investigation limitations chapter.

This is by it’s nature a subjective chapter, and care should be taken when considering cause and effect, certainty and especially culpability. Refer to the general style guide to ensure statements of certainty follow a defined pattern.

The conclusions should serve as a neutral, technical explanation of the incident. Pointing fingers or talking about individual people instead of user accounts is not good practice, and might lead to undesirable consequences. The job of the incident responder is not to figure out which admin made a mistake and where, but to document the technical facts in the environment where the incident happened. When describing someone doing something, describe what an *account* did instead of what a *user* did. This is technically factual and can be proven with forensic evidence. ## Recommendations

The recommendations chapter is based on your conclusions, expertise as a security professional, and should focus on how to prevent similar incidents in the future. This is the chapter where the failures of security that lead to the incident in the first place can be corrected. The recommendations should be grounded on concrete findings and be specific enough to be used as points of entry to further development. General recommendations like “do security better” are not useful, but actionable recommendations like “monitor and block open RDP ports on the network” are.

Remember, that these conclusions and recommendations will most likely be read very carefully and discussed in security steering groups and other leadership decision-making forums. If they are easy to understand and possible to implement without massive investment, they will most likely be executed on.

# 6 Attachments

**File name**: dummyfile 2.bin  
**File size**: 16384  
**File hash**: d2813820ecbacd8476cd4a961a8dd86300183008339e0add508cd219a1afac15

**File name**: dummyfile 3.bin  
**File size**: 15984  
**File hash**: 83c48c0b37029f76c07243a95d8e054a1b32722fd78e75b51810fb9a0ce7b98d

**File name**: dummyfile.bin  
**File size**: 16384  
**File hash**: 85b339ef3903c83d59deb070df1fd2245edc79b9fc4fc432996ddf2c6568e2f6