Incident Investigation Report

Incident ID: INC-123456
Investigator: Example Name

Restrictions: CONFIDENTIAL / TLP:AMBER

1 Table Of Contents

1.1 Report revisions

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 after customer comments

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 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 (UTC) following the 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.**

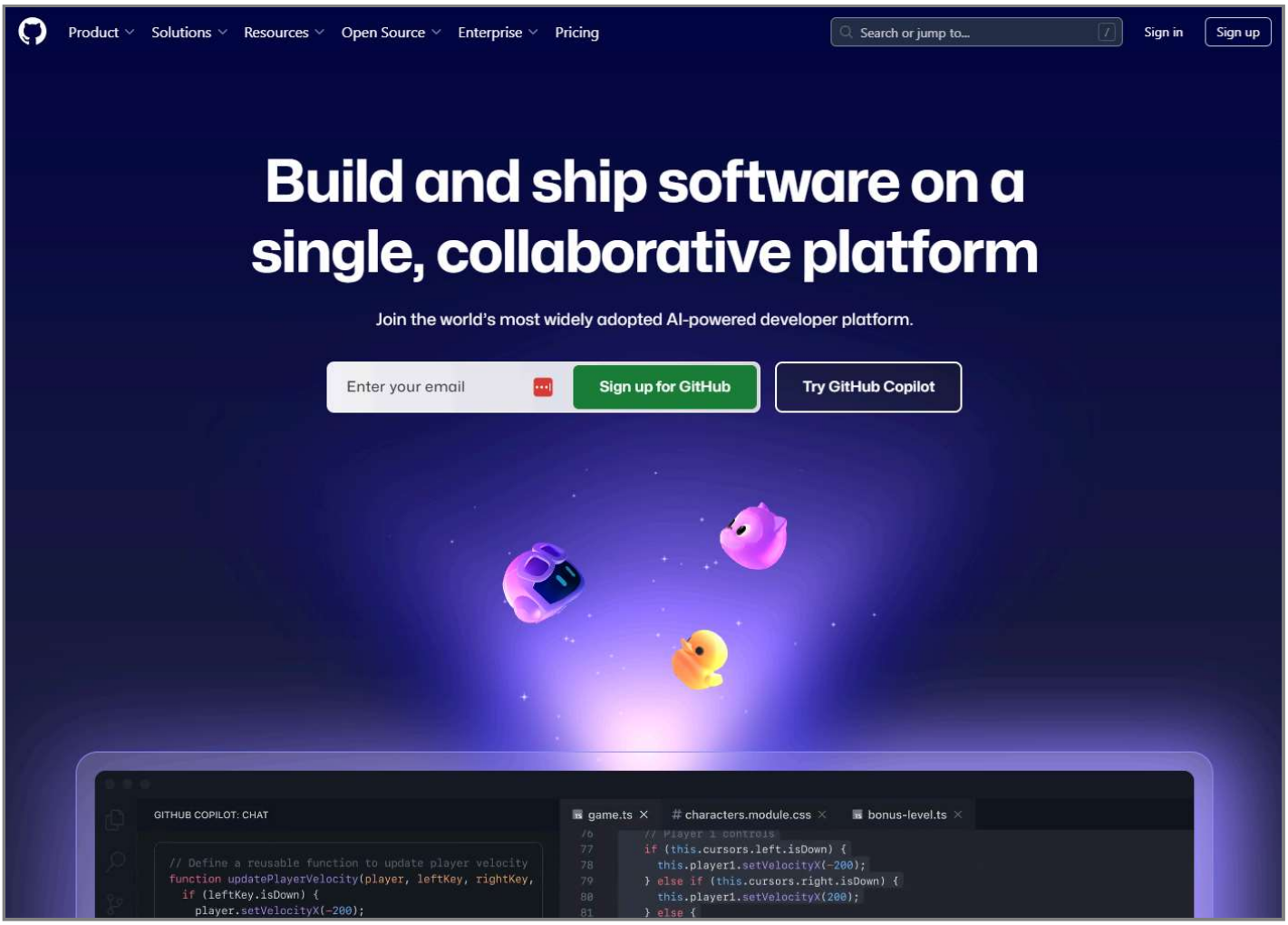
Investigators interpretation

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.

This is a defanged url with a distinct style: hxxps://this-would-be-clickable.com. This text is highlighted. Use the `span` tag for inline text and `div` tag for block-level text.



An example screenshot of the GitHub front page

1.4 Intended audience

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

2.1 Business Impact Analysis

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

- 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

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

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

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

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

Investigation conclusions go here.

Recommendations

Recommendation
Ensure all endpoints have endpoint detection and response tooling installed
Ensure servers XX and YY are assigned an end-of-life date and removed
Deploy passkeys to domain administrators as the only way to authenticate
Triple your cyber security budget