Incident Response After Action Report

Prepared For:

ACME Corp.

Document Profile:

|  |  |
| --- | --- |
| Mission Id: | IR-YYYYMMDD-1 |
| Revision Id: | 1.1 |
| Date: | 2019-00-00 |
| Rating: | SEVERE ([NCCIC CISS](https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System)) |
| COA Completion: | 0/0 - n% |
| Condition: | GUARDED ([HSAS](https://en.wikipedia.org/wiki/Homeland_Security_Advisory_System)) |
| Authorized Distribution: | [alice@acmecorp.com](mailto:alice@acmecorp.com), [bob@acmecorp.com](mailto:bob@acmecorp.com) |
| CONFIDENTIAL//ATTORNEY-CLIENT PRIVILEGE//TLP:AMBER | |

This document is an after-action report that provides the details of an Information Security Incident signifying a violation of computer security policies, acceptable use policies, or standard security practices resulting in a compromise of this organization's assets.

This document is designated as Traffic Light Protocol (TLP): AMBER. Recipients may share TLP: AMBER information with members of their organization who need to know, and only widely as necessary to act on that information.

This document contains confidential and privileged material. Any interception, review, retransmission, dissemination or other use of or taking any action upon this information by persons or entities other than the intended recipient(s) is prohibited by law and may subject them to criminal or civil liability. This document contains material that may have been commissioned by counsel in anticipation of litigation. It should be treated as confidential to avoid waiver of the attorney/client privilege, the work-product privilege, or another applicable privilege. It was prepared for the sole use of the named recipient, and must not be relied upon by any third party.

This document is a deliverable that meets or exceeds a standard of reasonable cybersecurity practices.

GuardSight® is a registered trademark of GuardSight, Inc. All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners. © GuardSight, Inc.

Table Of Contents

[**Summary**](#_lacxyus2qu7e) **4**

[**Risk Of Compromise**](#_poryza8z56ev) **5**

[**Timelines**](#_9gik9t860wl1) **5**

[**Impacted Resources & Assets**](#_o73d3n3wp6hc) **5**

[**Indicators Of Compromise**](#_hoqygq9fg1j) **6**

[**Atomic**](#_1hekxjxjmhtv) **6**

[**Computed**](#_u4qhniy9tz3t) **6**

[**Behavioral**](#_e2y8s2twfh9d) **6**

[**Cyber Kill Chain**](#_5qbshjfj9nvr) **7**

[**Reconnaissance**](#_9w2e8ssbytvj) **7**

[**Weaponization**](#_7rvwc950uohh) **7**

[**Delivery**](#_26d3uk2wyzxg) **7**

[**Exploitation**](#_aq3lrs8ey5rq) **7**

[**Installation**](#_vq2l5x6d9ihk) **7**

[**Command and Control**](#_258btkm34pve) **7**

[**Actions on Objectives**](#_k1p0w51r7re8) **7**

[**Courses Of Action**](#_lnwc24io83rt) **8**

[**Inventory**](#_azkghl1eutuc) **8**

[**Containment & Eradication**](#_3ydxckagnpo3) **8**

[Detect](#_56gabpkg48ri) 8

[Deny](#_z7ft2kh3ltmf) 8

[Disrupt](#_k89h3f48a92k) 8

[Degrade](#_zgqhzwxavtip) 8

[Deceive](#_yonc41ii5lw) 8

[Destroy](#_5is8iczbo5ns) 8

[**Recovery**](#_xs9kods72qq0) **9**

[**Opportunities For Improvement**](#_fp4khbwwvm6p) **9**

[**Preparation**](#_uke8ovlqdsz9) **9**

[**Identification**](#_vijykhybx895) **9**

[**Containment**](#_4iz301abtux6) **9**

[**Eradication**](#_4zoiwnna7wfm) **9**

[**Recovery**](#_uo79eo87dnvw) **9**

[**Notes**](#_cfqebkugf0j5) **9**

[**Correspondence**](#_klcbuy331xm8) **10**

[**References**](#_ew2uqmbp0lu1) **10**

[**Contributors**](#_tyu8ubz8xxom) **10**

[**License**](#_fsy2b8toz7cb) **10**

# Summary

|  |  |
| --- | --- |
| Total Impacted Assets: | 0 |
| Time To Respond: | 0 Minutes |
| Total Dwell Time: | 0 Days |
| Response Duration: | 0 Hours |
| Weaponization: | Unknown |
| Exploitation: | Unknown |
| Data Compromise: | Negative |
| Date Legal Notified: | Not Required |
| Evidence Locker: | SEE NOTES |

Executive summary explanation…

1. Statement 1
2. Statement 2
3. Statement 3

# Risk Of Compromise

The Risk Of Compromise to the organization’s resources and assets is CONFIRMED due to the following factors:

1. X
2. Y
3. Z

# Timelines

The following provides the high level timeline summary of the activities conducted by both the adversaries and the response team members. All times are represented in Mountain Time unless otherwise annotated.

<timeline sequence diagram>

1. 1970-01-01
   1. 00:00:00 [attacker] - <Event>
   2. 00:00:00 [response] - <Description>
2. 1970-01-02
   1. 00:00:00 [attacker] - <Event>
   2. 00:00:00 [response] - <Description>

# Impacted Resources & Assets

The following *GENERAL RESOURCES* **HAVE|HAVE NOT** been negatively impacted:

1. Customer Data
2. Employee Data
3. Financial Data
4. Legal Data
5. Intellectual Property

The following *SPECIFIC CRITICAL ASSETS* **HAVE** been negatively impacted:

1. X
2. Y
3. Z

# Indicators Of Compromise

Indicators Of Compromise (IOC) represent artifacts and attributes observed and collected by response team members and asset owners. IOC supply the evidence to support assertions of a high degree of confidence that adversary activity resulted in successful asset compromise.

## Atomic

1. Atomic artifacts are currently not known / do not exist.

## Computed

1. Computed attributes derived from data elements are currently not known / do not exist.

## Behavioral

1. Logical assertions based on atomic and computed indicators have not yet been developed.

# Cyber Kill Chain

Cyber Kill Chain (CKC) is a systematic analysis process used by response team members and asset owners to identify and communicate the stages of an attack. The patterns, behaviors, tactics, techniques, and procedures (TTP) used by adversaries are described using this analysis to subsequently develop Courses Of Action designed to target and engage adversaries.

## Reconnaissance

1. Reconnaissance TTP are not currently known / do not exist.

## Weaponization

1. Weaponization and payload TTP are not currently known / do not exist.

## Delivery

1. Delivery TTP are not currently known / do not exist.

## Exploitation

1. Exploitation TTP are not currently known / do not exist.

## Installation

1. Installation TTP for creating maintained persistensence are not currently known / do not exist.

## Command and Control

1. Command and Control TTP for maintaining persistence are not currently known / do not exist.

## Actions on Objectives

1. Actions on Objectives TTP for achieving goals are not currently known / do not exist.

# Courses Of Action

Courses Of Action (COA) derived from the Cyber Kill Chain represent the countermeasures, containment & eradication, and recovery actions that are being deployed by response team members and asset owners to target and engage adversaries.

## Inventory

1. There are no current COA to inventory assets associated with the vulnerability / exploit / compromise / adversaries.

## Containment & Eradication

### Detect

1. There are no current COA to detect the vulnerability / exploit / compromise / adversaries.

### Deny

1. There are no current COA to deny the vulnerability / exploit / compromise / adversaries.

### Disrupt

1. There are no current COA to disrupt the vulnerability / exploit / compromise / adversaries.

### Degrade

1. There are no current COA to degrade the vulnerability / exploit / compromise / adversaries.

### Deceive

1. There are no current COA to deceive the vulnerability / exploit / compromise / adversaries.

### Destroy

1. There are no current COA to destroy the vulnerability / exploit / compromise / adversaries.

## Recovery

1. There are no current COA to recover compromised assets.

# Opportunities For Improvement

Opportunities For Improvement (OFI) impart recommendations based on findings of response team members and asset owners during each phase of the response. These recommendations are provided to help reduce attack surfaces, enhance security posture, improve operational readiness, and boost the effectiveness of future response.

## Preparation

1. There are no current preparation OFI.

## Identification

1. There are no current identification OFI.

## Containment

1. There are no current containment OFI.

## Eradication

1. There are no current eradication OFI.

## Recovery

1. There are no current identification OFI.

# Notes

|  |  |
| --- | --- |
| Evidence Locker Location: |  |

# Correspondence

# References

# Contributors

# License

CONFIDENTIAL//ATTORNEY-CLIENT PRIVILEGE//TLP: AMBER

This document is an after-action report that provides the details of an Information Security Incident signifying a violation of computer security policies, acceptable use policies, or standard security practices resulting in a compromise of this organization's assets.

This document is designated as Traffic Light Protocol (TLP): AMBER. Recipients may share TLP: AMBER information with members of their organization who need to know, and only widely as necessary to act on that information.

This document contains confidential and privileged material. Any interception, review, retransmission, dissemination or other use of or taking any action upon this information by persons or entities other than the intended recipient(s) is prohibited by law and may subject them to criminal or civil liability. This document contains material that may have been commissioned by counsel in anticipation of litigation. It should be treated as confidential to avoid waiver of the attorney/client privilege, the work-product privilege, or another applicable privilege. It was prepared for the sole use of the named recipient, and must not be relied upon by any third party.

This document is a deliverable that meets or exceeds a standard of reasonable cybersecurity practices.

GuardSight® is a registered trademark of GuardSight, Inc. All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners. © GuardSight, Inc.