Incident Report

Contents

[INCIDENT SUMMARY 2](#_Toc109542691)

[TIMELINE 2](#_Toc109542692)

[ADVERSARY ACTIONS 2](#_Toc109542693)

[RECOMMENDATIONS 2](#_Toc109542694)

[TECHNICAL ANALYSIS 4](#_Toc109542695)

[Console/Log Analysis 4](#_Toc109542696)

[EDR 4](#_Toc109542697)

[SIEM 4](#_Toc109542698)

[Firewall 4](#_Toc109542699)

[[Console] 4](#_Toc109542700)

[Hosts 4](#_Toc109542701)

[HOST1 4](#_Toc109542702)

[HOST2 4](#_Toc109542703)

[Indicators 4](#_Toc109542704)

# INCIDENT SUMMARY

On 2022-02-12, an alert triggered on the company jumphost. Security investigating was delayed as other security alerts were processed. The system was found compromised, attacker active and already gained privileged access (20:00) and was able to exfiltrate data (20:45). Around 20:50, the threat actor created backdoor accounts on domain controllers with privileges on all computers and after, they wiped event logs on domain controllers (X systems total). Network access was blocked to prevent further access and attacker actions, but attack is believed to be completed. Initial access is identified as password spray attack on Internet exposed system that were not protected by Multi-factor Authentication (MFA).

The Windows Active Directory environment is compromised and cannot be trusted forcing a shutdown of our operations until rebuilt. Estimate effort to rebuild is 14 days. Office email will be unavailable during that time. The Company website was unaffected as it is hosted on a non-Windows system and is not connected to the Active Directory. Outside of operational impacts, this could result in a loss of trust of our customers, a loss of reputation and legal actions from customers.

# TIMELINE

[Refer to IncidentTracking.xlsx and the “TIMELINE” here when completed]

# ADVERSARY ACTIONS

[Include which MITRE TTPs were observed and details of how it matches]

#### [Tactic]:

**[Technique]:** [Correlating Incident details]

#### [Tactic]:

**[Technique]:** [Correlating Incident details]

# RECOMMENDATIONS

|  |  |  |
| --- | --- | --- |
| Priority | Title | Description |
| High | Implement MFA | The initial access was a low effort password spray. Implementing MFA on accounts to protect VPN and email access could have prevented this from being an effective attack vector. |
| Medium |  |  |
| Low |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# TECHNICAL ANALYSIS

# Console/Log Analysis

## EDR

## SIEM

## Firewall

## [Console]

# Hosts

## HOST1

### Artifact

[Analysis Notes regarding the artifact]

#### Artifact2

[Analysis Notes regarding the artifact]

## HOST2

### Artifact

[Analysis Notes regarding the artifact]

### Artifact2

[Analysis Notes regarding the artifact]

# Indicators

### Network

[IP Address/DNS]

### File

[File Name/Hash]

### Users

[Domain and Username]