Investigation Notes

Contents

[**Console/Log Analysis**](#_heading=h.80hre4nnqsg) **1**

[EDR](#_heading=h.30j0zll) 1

[SIEM](#_heading=h.1fob9te) 1

[Firewall](#_heading=h.3znysh7) 1

[Email](#_heading=h.6jm6uut5y0sv) 2

[[Console]](#_heading=h.2et92p0) 2

[**Hosts**](#_heading=h.tyjcwt) **2**

[HOST1](#_heading=h.3dy6vkm) 2

[Artifact1](#_heading=h.n36foi7h3crp) 2

[Artifact2](#_heading=h.e05ypg1k0dg) 2

[HOST2](#_heading=h.1t3h5sf) 2

[Artifact](#_heading=h.9tzxggk2xs4p) 2

[Artifact2](#_heading=h.7fidw2x37y3) 3

[**Indicators**](#_heading=h.4d34og8) **3**

[Network](#_heading=h.yjmn72s823iw) 3

[File](#_heading=h.6xwao3lfxwpv) 3

[Users](#_heading=h.g2hazc9lk758) 3

# Console/Log Analysis

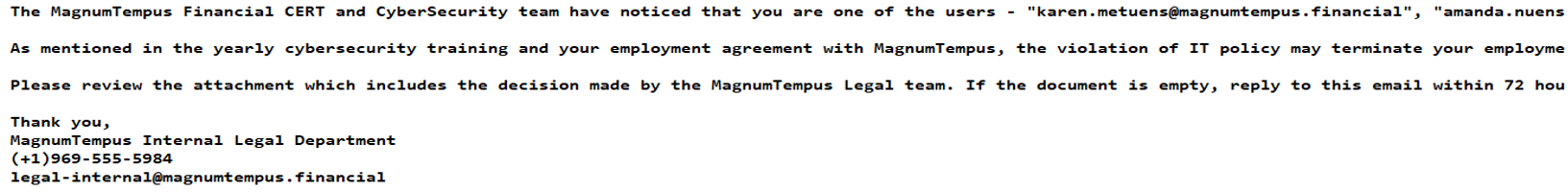
## EDR

## SIEM

## Firewall

## Email

At 2022-02-12T21:10:06Z, the team identified a suspicious email with the subject line “[ACTION REQUIRED] ORGANIZATION IT POLICY VIOLATION”. The email originated from “legal-internal@magnumtempus[.]financial” which the team validated was not a legitimate organization domain. The email received by “amanda.neunsis@magnumtempusfinancial[.]com” and the team is validating whether any similar emails were sent to other users. The contents of the email are noted below.



The contents of the email appear to attempt to coerce the employee into reviewing a fake IT policy violation by reviewing an attachment to the email.

## [Console]

# **Hosts**

## HOST1

| OS: | IP: |
| --- | --- |
| Function: | Primary User: |
| Evidence Type: | Additional Notes |

### Artifact1

### Artifact2

[Analysis Notes regarding the artifact]

## HOST2

| OS: | IP: |
| --- | --- |
| Function: | Primary User: |
| Evidence Type: | Additional Notes |

### Artifact

[Analysis Notes regarding the artifact]

### Artifact2

[Analysis Notes regarding the artifact]

# **Indicators**

### Network

[IP Address/DNS]

| Network Indicator | Description |
| --- | --- |
| magnumtempus[.]financial | Domain name associated with the sender of the fake IT policy violation phishing email |
|  |  |
|  |  |

### File

[File Name/Hash]

| File Indicator | Description |
| --- | --- |
|  |  |
|  |  |
|  |  |

### Users

[Domain and Username]

| User | Description |
| --- | --- |
| legal-internal@magnumtempus[.]financial | Sender of the fake IT policy violation phishing email |
| amanda.neunsis@magnumtempusfinancial[.]com | Recipient of fake IT policy violation phishing email |
|  |  |