INCIDENT RESPONSE SCOPING

# INITIAL QUESTIONS

#### Organization and key members?

* Magnum Tempus Financial

#### When was the incident reported?

* 2022-02-12T23:30:00Z

#### Who is assigned to the engagement?

* Team Obsidian

#### Who reported the incident? (Contact details)

* IT Department

#### Who is aware of the incident?

* IT Department

#### Is the incident ongoing?

* Yes

#### Are there “need-to-know” requirements needed for the incident? (Legal privilege, limit public knowledge)

* Not at this moment

#### What are the objectives?

* Determine the source of the email and what it

# DETECTION

*Try to convert all times into UTC or at the very least state specific time zones*

#### When was the incident detected

* 2022-02-12T21:10:06Z

#### Who detected the incident? (Contact details)

* IT Department

#### How would you categorize the detection? (mass malware, phishing, failed login, etc.)

* Phishing

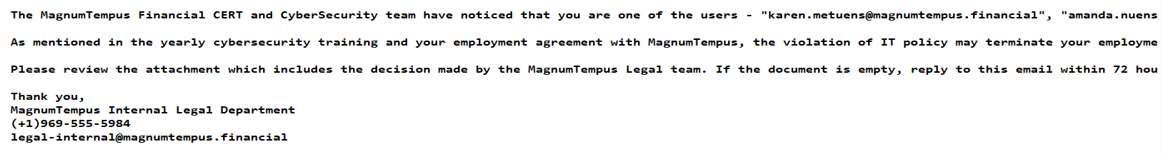
#### What tool, process or scan identified the incident?

#### Was the detection through a manual or automated process?

* Manual

#### What information was part of the initial detection?

* An email message detailing a “violation” of an IT policy and requiring additional



# IMPACT

#### What was the type and number of resources affected?

* Currently, one known email recipient
  + TBD

#### Is there a unique identifier for the affected resources? (Host naming, asset tag, static IP or range)

* Specific email phishing from magnumtempus.financial

## System Details

| **Hostname/Domain** | **Location** | **OS** | **Function** | **IP address** | **User/Admin** | **Backups?** | **Isolated?** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# ACTIONS

#### Who has accessed the systems since detection? What was done?

* IT gathered the email

#### Any remediation already done? (Block listing, firewall changes)

* None

# ENVIRONMENT

#### How many endpoints in the organization? (Servers, Workstations)

#### How many users?

#### Capabilities of the security/response team?

#### Toolset

* Network/Firewall
* EDR/AV
* DNS
* SIEM/Central Logging
* Asset Management
* DLP
* Mail Protection

# NETWORK

#### Suspicious IP’s or domains identified?

#### Availability of network monitoring?

#### Remediation steps already taken?

#### Network logs being preserved? (SIEM, Console retention)

#### Network diagrams or documented configurations?

# MALWARE

#### Date/Time of detection

#### How malware was detected

#### List of systems where it was found

#### Name of the file and file path

#### Is the malware currently active or showing active connections?

#### Has malware been quarantined or separately preserved?

#### Status of analysis at this time?

# NEXT STEPS

* Understand the potential actions taken from the email attachment
* Understand the scope of similar phishing emails