Analysis 2/5

Attack Vectors

Tactical Phase

Productivity	Less than 1% of systems; less than 1% of workforce	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Widespread	Minimal	Moderate	High	None	N/A
Commonality	Commonly Seen	Occasionally happens	Rare	Never	N/A
Damage	Minimal	Moderate	High		N/A
Affected Parties	Less than 1% of systems; less than 1% of	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Business Impact	Minimal	Moderate	High		N/A

After you complete your selection of choices for this table, please click "continue" to advance to the next section. All decisions are final and you can Not go back to modify them, after advancing

Fill all options

Continue

Analysis 3/5

Motivation

Tactical Phase

Based on the Malware detection. Define the adversary's motivation(s).
You may select more than one motivation factor, if needed to complete your analysis.

Control Network/System	Fun	Cryptomining	Steal a company's intellectual property.
Hacktivists	Steal banking information	Espionage	Grudge

Continue

Decision-making

Communication

Tactical Phase

At this point, the Company is unable to determine the full extent of the damages in the system and/or users' workstations.

The company does not know if the traditional communication channels are still compromised. Therefore, you next task is to suggest:

Communication

An alternative communication channel for the IRT members - to continue their tasks.

An alternative communication channel to connect/inform/update with all users about new developments

Write your comments

short message service(SMS) to mobile devices and phone call

short message service(SMS) to mobile devices and phone call
Deploy a temporary wifi network using a new access point not compromised

Continue

Analysis 4/5

Risk Factors

Tactical Phase

Event	This event is being launched by know entities.	This event could be exploited for criminal activities.	This kind of event has been recorded before in the company
Productivity	Customers are affected by this incident.	Products/goods/services are affected by this attack.	Ability to control/record/measure/track any significant amounts of inventory/products/cash/revenue has been lost.

Based on the Malware detection. Select the risk factors.

You may select more than one risk factor, if needed to complete your analysis.

Continue

Analysis 5/5

Risk Factors

Tactical Phase

Based on the Malware detection. Select the risk factors.

You may select more than one risk factor, if needed to complete your analysis.

Information	Internal PII or other protected information at risk of being exposed.	External user PII or other protected information at risk of being exposed.	PII or other protected information has been compromised.
Stakeholders	There is internal knowledge of this incident.	There is external knowledge or this incident.	Reputation or company's credibility has been affected.
Social Responsibility	Personnel safety affected.	Partners have been affected and contacted regarding this event.	Public or state safety affected.

Continue

Decision-making

Tactical Phase

Analyze the SLA, and answer the questions below

SLA

Does the service level agreement was adequate to respond to a cyber event?

Write your comments

No

What aspects do you consider this document lacks to be more effective in the face of an attack?

Include the entity "cybersecurity event"
Reduce response time

Continue

Analysis 1/3

Strategic Phase

Set up notification systems to rapidly reach your stakeholders. Employing more than one type of communications platform

SYSTEMS NOTIFICATIONS

SYSTEM NAME	PROVIDER/ARCHITECTURE	Appropriate for	PRIORITY (1 to 5, being 1 the highest)
EJ. Social Media (one to many)	Owner (Company blog) Third party (Facebook)	Time sensitive information/ Updates	5
SMS (one to many)	Third-party(T-Mobile)	Time sensitive information//critical	1
Phone call(one to one)	Third-party(T-Mobile)	Time sensitive information//critical	2
Social Media (one to many)	Third-party(Twitter)	Update	5

Continue

Print/Save Analysis

Analysis 2/3

Strategic Phase

KEY MESSAGE PLANNER

AUDIENCE		TOP THREE KEY MESSAGES	DELIVERY CHANNELS & SPOKESPERSON
ALL STAKEHOLERS	1.	A cyber incident has been detected.	channel(s): SMS Barry Hector Olsson +49886475770
	2.	The main channel of communication regarding this event will be by SMS.	
	3.	The network will be down from 4:00 p.m. to 6:00 p.m.	
Law enforcement	1.	The malware has been identified as TrickBot	channel(s): email, phone call Joshua Jack Thomas +496335584757
	2.	The malware has been contained	
	3.	The process of recovery initiate within 24 hours	

Continue

Print/Save Analysis