Navigating the Road to Resilience:
LAS IPE Risk Management Symposium
October 4, 2023

AMO Association of Municipalities Ontario

LAS | AMO Business Services

Ransomware Scenario: Critical IT Infrastructure Targeted!

Presented by:
Andrew Anderson & Adam Wong
ISA Cybersecurity

ISA CYBERSECURITY

isacybersecurity.com

Nice to meet you!

Andrew Anderson

Service Lead, Response

Adam Wong

Digital Forensics and Incident Response Specialist

CYBERSECURITY

Introduction

In this “tabletop exercise”, we will discuss a ransomware attack targeting critical IT infrastructure within a fictional organization called "**GlobalTech Solutions**" (**GTS**).

Key Features of the Simulation

- High-level walkthrough of a ransomware attack
- Attempt to uncover the cause of the breach, identify the attack's initiation, and confirm the absence of lingering system impacts
- Watch for “injects”, questions to reflect on, surprises along the way
- Lots of audience participation!

You are part of the story!

- You will learn the roles and actions of:
  - Threat Actors
  - Blue Team Incident Response (IR) members
  - Stakeholders

} more about these roles shortly!

- **Cybersecurity is a team sport**! Work together and collaborate with each other!

Why do a ransomware simulation?

- Important to recognize and respond to key elements of ransomware attacks, because ransomware is a prevalent method of attack for hackers
- Why are municipalities targeted?
  - financial resources
  - opportunity to access extensive PII from citizens
  - disruption of critical services makes city more likely to pay ransom

Key Features of Ransomware Attacks

Phishing

Double extortion

Ransomware as a service

Supply chain attacks

Attacking unpatched systems

Major Ransomware Attacks in 2023

- **January**:
  - Royal Mail (LockBit)
    - Ransom was $80 Million+
- **February:**
  City of Oakland, California (Play)
    - declared a local state of emergency due to a ransomware attack
- **March**: Yellow Pages Group (Black Basta)
    - stole employee and customer data
- **May**:
  - City of Dallas (Royal)
    - 26,000 people had their PII stolen
    - Paid over $8.6M in recovery services
  - City of Augusta, GA (BlackByte)
    - data leaked to dark web
- **June:**
  - MOVEit Attack (Cl0p)
    - 1146 organizations affected to date
- **September**:
  - MGM resorts and casinos (Scattered Spider)
    - ATMs, payments processing down
    - data breach

Who's Next…?

Understanding the Roles and Action

- **Threat Actors:** Individuals, groups, or entities responsible for initiating and executing cyber attacks with malicious intent
    - Phishing
    - Black market / dark web listings
    - Search for company income
        - Typically done via Google and sites such as ZoomInfo, Dun & Bradstreet, RocketReach, etc.

Understanding the Roles and Action

- **Blue Team Incident Response (IR)** members: The defensive side responsible for safeguarding an organization's IT systems and responding to security incidents
  - Identify affected systems and critical infrastructure components
  - Develop an incident response plan
  - Identify preventive measures
  - Ways to detect/prevent:
    - security awareness training
    - dark web monitoring

Understanding the Roles and Action

- **Stakeholders:** Individuals, groups, or entities with an interest or involvement in the organization's security
  - Interest in the potential impact of a ransomware attack on critical IT infrastructure
  - Financial and operational implications
  - Explore strategies for minimizing disruption

Let’s get started!

Scenario

GlobalTech Solutions is a multinational company that provides IT solutions and services to various industries. It operates a highly interconnected IT infrastructure consisting of servers, workstations, databases, and critical applications that are essential for its operations. GTS has a reputation for robust cybersecurity practices.

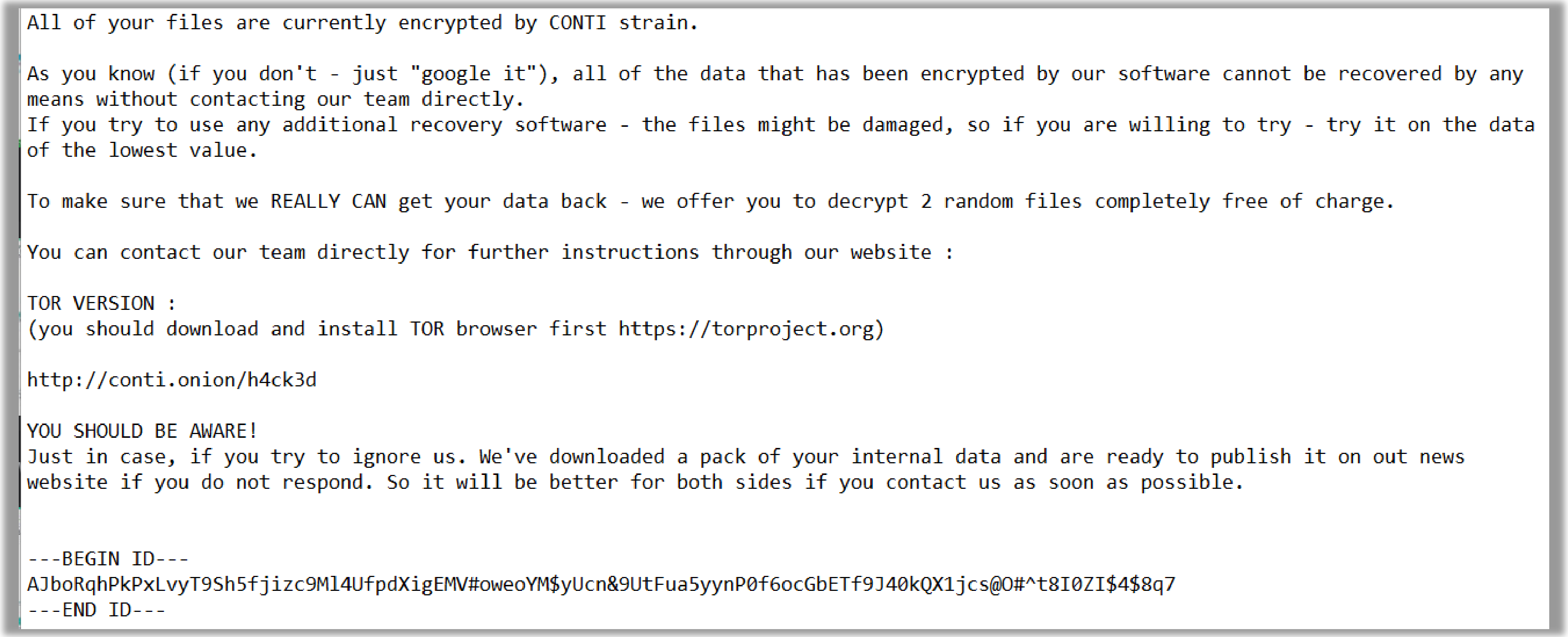
But no organization is completely immune to cyber threats…

Scenario

On **Monday, September 25, 2023**, at **9:00 a.m**. a staff member called in to report that they could not access their files.

Upon logging into the server, you find that everything now has the file extension **.xyz** and cannot be opened.

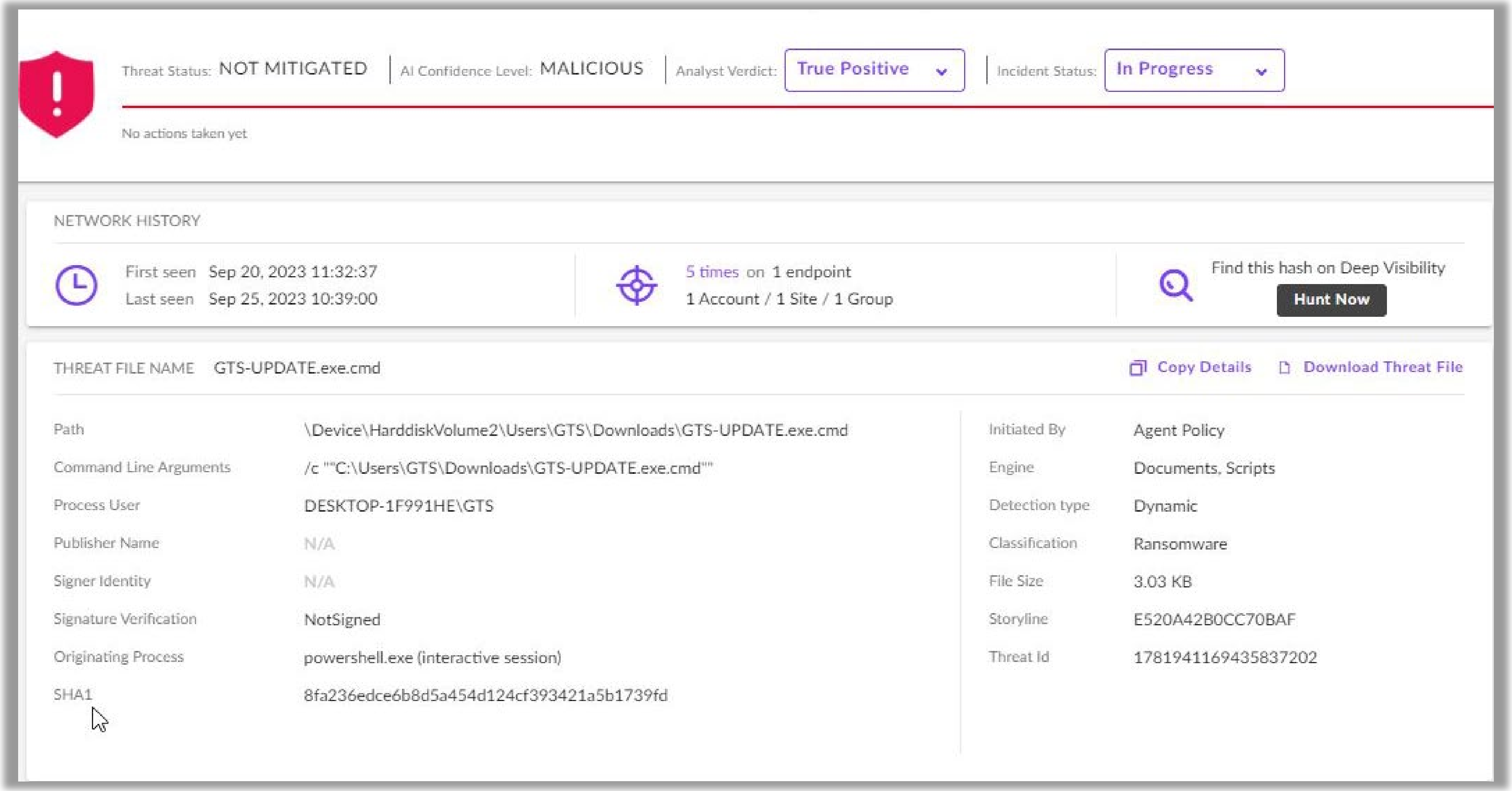
Scenario (continued)



```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any
means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data
of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti.onion/h4ck3d

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news
website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
AJboRqhPkPxLvyT9Sh5fjizc9Ml4UfpdXigEMV#oweoYM$yUcn&9UtFua5yynP0f6ocGbETf9J40kQX1jcs@O#^t8I0ZI$4$8q7
---END ID---
```

CYBERSECURITY

Blue Team Incident Response (IR) members



Threat Status: NOT MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: True Positive | Incident Status: In Progress

No actions taken yet

NETWORK HISTORY

First seen Sep 20, 2023 11:32:37
Last seen Sep 25, 2023 10:39:00

5 times on 1 endpoint
1 Account / 1 Site / 1 Group

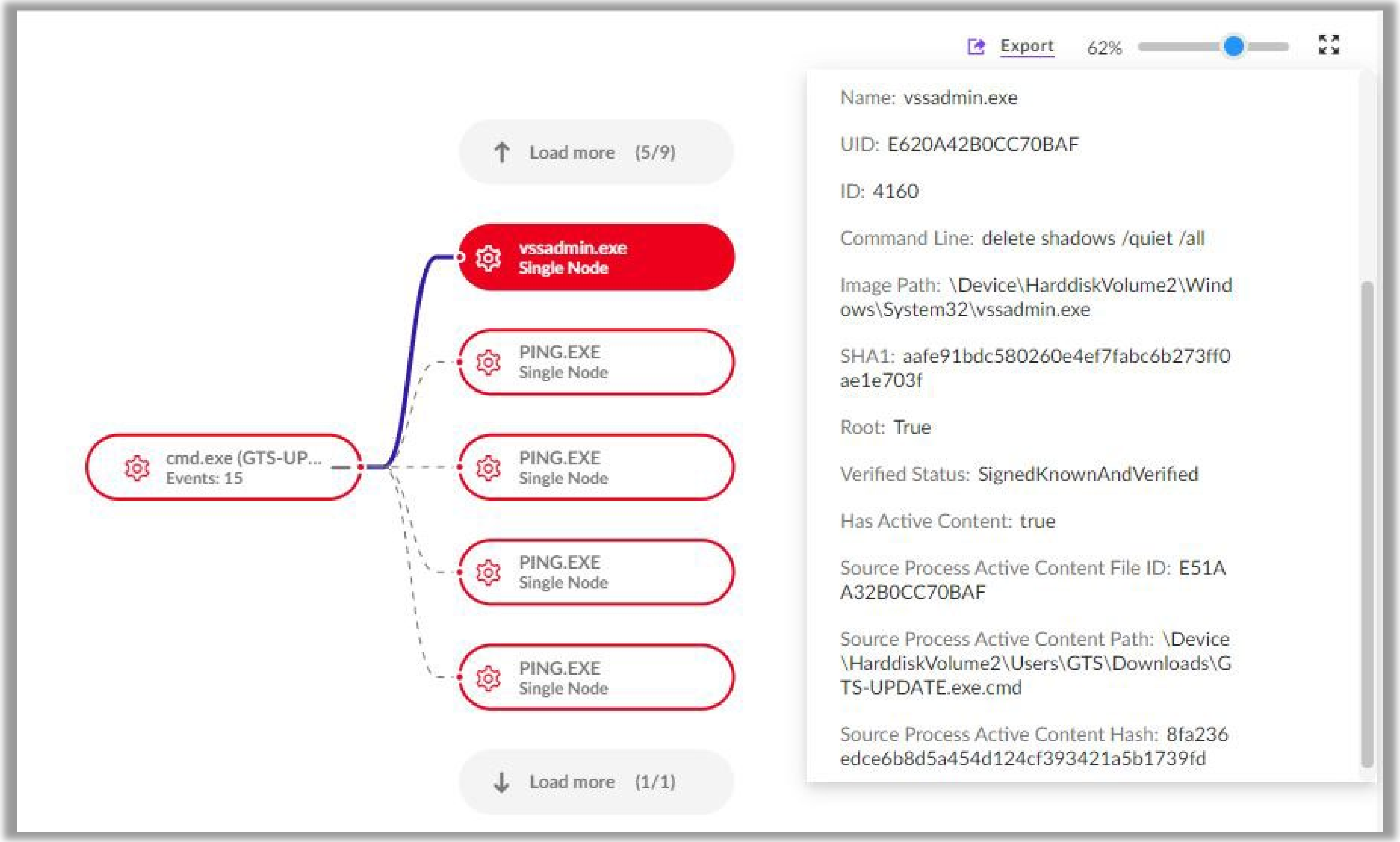
Find this hash on Deep Visibility

THREAT FILE NAME GTS-UPDATE.exe.cmd

Path	\Device\HarddiskVolume2\Users\GTS\Downloads\GTS-UPDATE.exe.cmd
Command Line Arguments	/c ""C:\Users\GTS\Downloads\GTS-UPDATE.exe.cmd""
Process User	DESKTOP-1F991HE\GTS
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	powershell.exe (interactive session)
SHA1	8fa236edce6b8d5a454d124cf393421a5b1739fd

Initiated By	Agent Policy
Engine	Documents, Scripts
Detection type	Dynamic
Classification	Ransomware
File Size	3.03 KB
Storyline	E520A42B0CC70BAF
Threat Id	1781941169435837202

Blue Team Incident Response (IR) members



Name: vssadmin.exe

UID: E620A42B0CC70BAF

ID: 4160

Command Line: delete shadows /quiet /all

Image Path: \Device\HarddiskVolume2\Windows\System32\vssadmin.exe

SHA1: aafe91bdc580260e4ef7fabc6b273ff0ae1e703f

Root: True

Verified Status: SignedKnownAndVerified

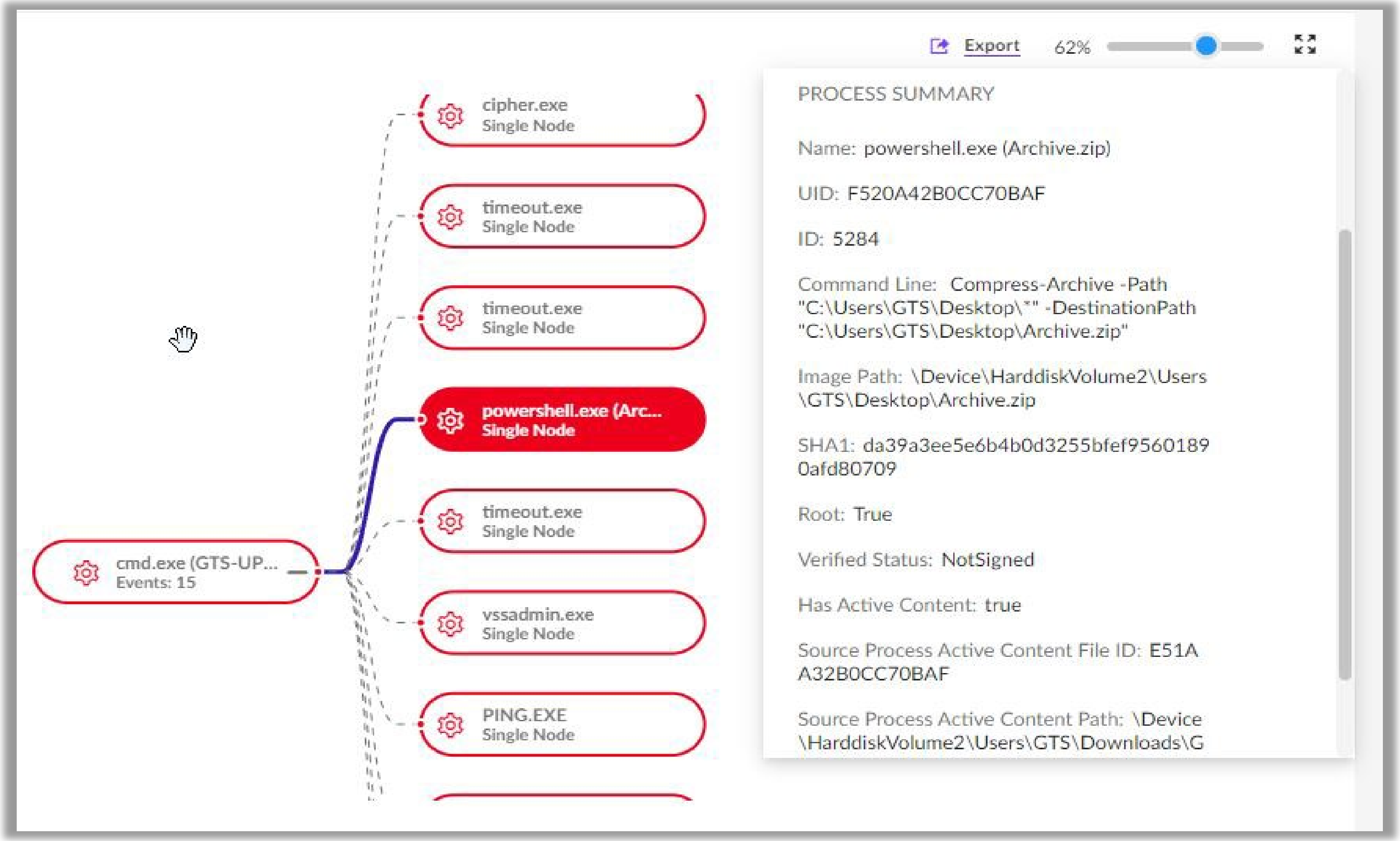
Has Active Content: true

Source Process Active Content File ID: E51AA32B0CC70BAF

Source Process Active Content Path: \Device\HarddiskVolume2\Users\GTS\Downloads\GTS-UPDATE.exe.cmd

Source Process Active Content Hash: 8fa236edce6b8d5a454d124cf393421a5b1739fd

S1 Threat Explore - Data Exfil



PROCESS SUMMARY

Name: powershell.exe (Archive.zip)

UID: F520A42B0CC70BAF

ID: 5284

Command Line: Compress-Archive -Path "C:\Users\GTS\Desktop\*" -DestinationPath "C:\Users\GTS\Desktop\Archive.zip"

Image Path: \Device\HarddiskVolume2\Users\GTS\Desktop\Archive.zip

SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709

Root: True

Verified Status: NotSigned

Has Active Content: true

Source Process Active Content File ID: E51AA32B0CC70BAF

Source Process Active Content Path: \Device\HarddiskVolume2\Users\GTS\Downloads\G

ISA CYBERSECURITY

Break time – 5 Minutes

Inject #1

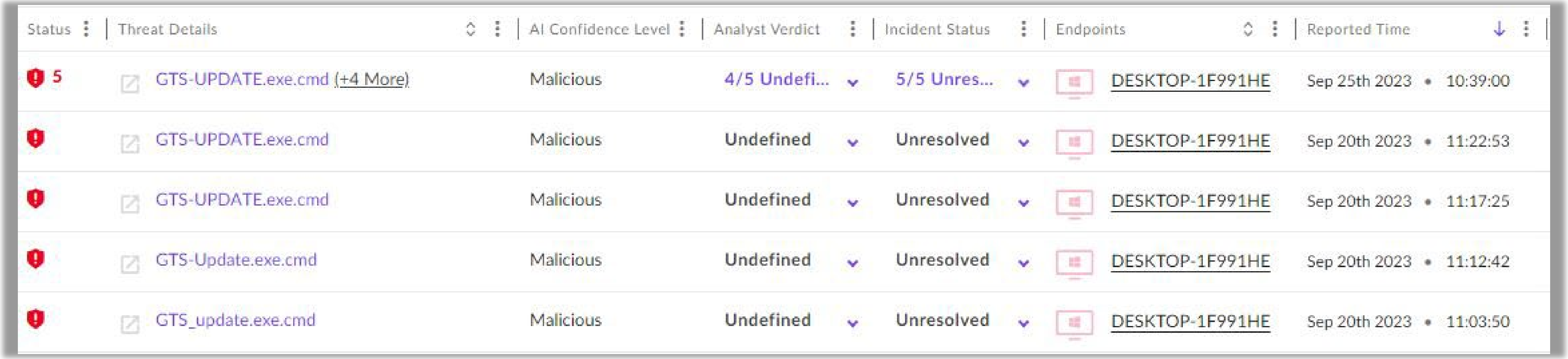
It was discovered that the employee who initially reported the issue was the one who had executed the malicious script.

Inject #1 - Discussion

It was discovered that the employee who initially reported the issue was the one who had executed the malicious script.

- How would you determine if it was an accidental or intentional execution?
- Who would you need to get involved in this investigation?

S1 Threat Details – Malicious Actions



Status	Threat Details	AI Confidence Level	Analyst Verdict	Incident Status	Endpoints	Reported Time
5	GTS-UPDATE.exe.cmd (+4 More)	Malicious	4/5 Undefi...	5/5 Unres...	DESKTOP-1F991HE	Sep 25th 2023 • 10:39:00
	GTS-UPDATE.exe.cmd	Malicious	Undefined	Unresolved	DESKTOP-1F991HE	Sep 20th 2023 • 11:22:53
	GTS-UPDATE.exe.cmd	Malicious	Undefined	Unresolved	DESKTOP-1F991HE	Sep 20th 2023 • 11:17:25
	GTS-Update.exe.cmd	Malicious	Undefined	Unresolved	DESKTOP-1F991HE	Sep 20th 2023 • 11:12:42
	GTS_update.exe.cmd	Malicious	Undefined	Unresolved	DESKTOP-1F991HE	Sep 20th 2023 • 11:03:50

Inject #1 – Discussion (continued)

- Discuss what could have assisted GTS in preventing the encryption of their critical IT infrastructure.

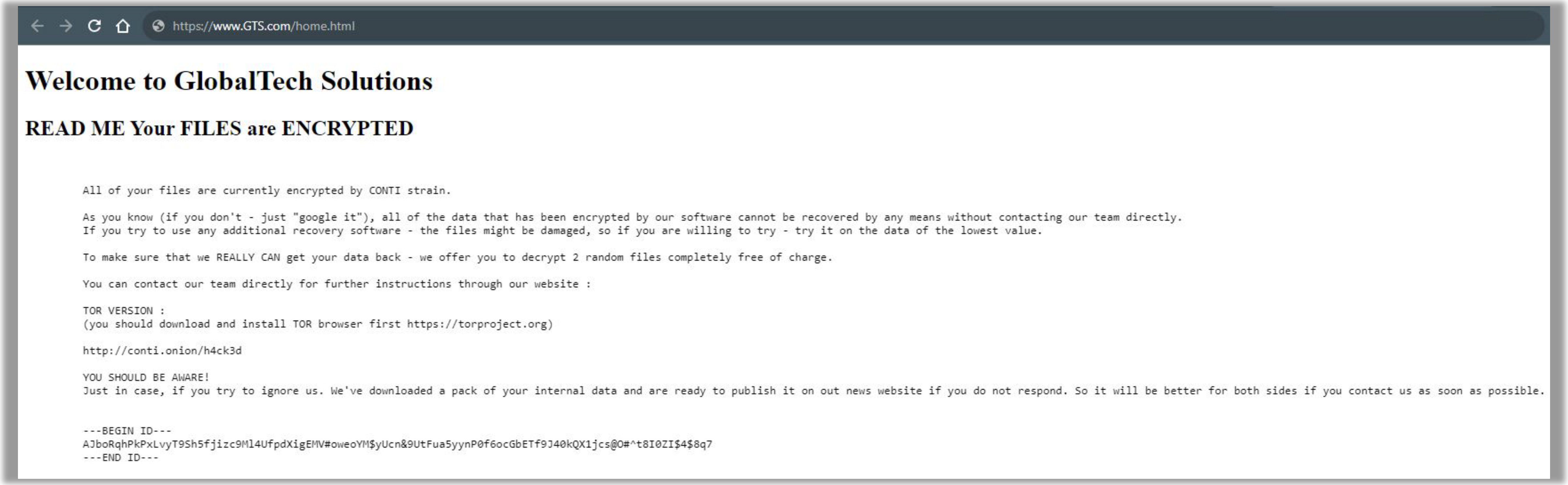
Inject #2

- In a startling turn of events, it has been discovered that the employee who executed the malicious script stemmed from resentment after being passed over for a promotion in favour of a junior colleague.
- During an interview with the employee, it was uncovered that the malicious script was purchased from the dark web, and the employee was unaware of its function/capabilities.

Inject #2 - Discussion

- What legal recourse is available to GTS?
- Discuss the potential implications of the Insider Threat incident.

Scenario (continued)



Welcome to GlobalTech Solutions

READ ME Your FILES are ENCRYPTED

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://conti.onion/h4ck3d

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
AJboRqhPkPxLvyT9Sh5fjizc9Ml4UfpdXigEMV#oweoYM$yUcn&9UtFua5yynP0f6ocGbETf9J40kQX1jcs@O#^t8I0ZI$4$8q7
---END ID---
```

Inject #3

The incident has gone public!

The threat actors have defaced GTS's website and have stated on the website that they have hacked and stolen data from you.

Inject #3 - Discussion

The incident has gone public!

The threat actors have defaced GTS’s website and have stated on the website that they have hacked and stolen data from you.

- What is your communication plan to reduce the impact of this disclosure?

Small Group Discussion (10 mins)

- Who is responsible for coordinating the public message? Is this process a part of any established plan?
- What information are you sharing with the public? Employees?
- Does your department have pre-drafted statements in place to respond to media outlets?
- Does your department have staff trained to manage your social media presence?

Break time – 5 Minutes

CYBERSECURITY

Group Discussion (10 mins)

- Who decides whether we pay the ransom?
- What is the process?
- What are the advantages/disadvantages of paying?
- What are the potential political ramifications?
- What outside partners/entities do you need to contact?

Law Enforcement Discussion (15 mins)

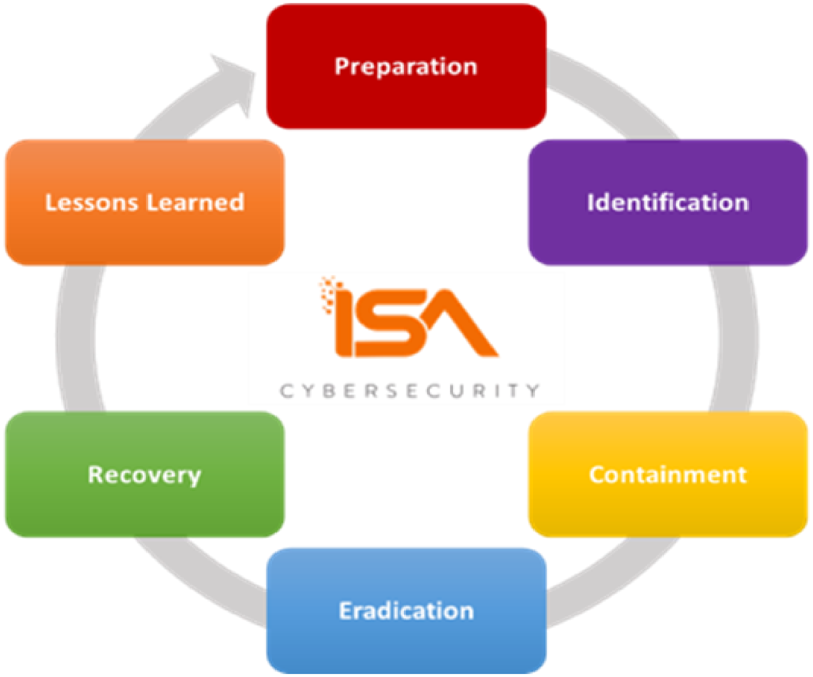
- Who oversees notifying law enforcement?
- Who oversees seeking internal legal counsel?
- Are systems in place to maintain business operations knowing that law enforcement may seize servers for their investigation?

Incident Response Framework

1. **Preparation** covers planning, training of staff, and communication plans.

2. **Identification** deals with the detection and determination of whether a deviation from normal operations an incident is.

3. **Containment** limits the damage and prevent any further damage from happening



4. **Eradication**, affected systems are evaluated to ensure that any remnants of the incident are cleaned up and removed.

5. **Recovery**, systems are evaluated to ensure that confidentiality, integrity, and availability are restored to normal.

6. **Lessons Learned**, processes are reviewed, and improvements are implemented.

Questions and Answers

ISA
CYBERSECURITY

THANK YOU !

We’re here to help!

info@isacybersecurity.com

ISA CYBERSECURITY

isacybersecurity.com