Table of Contents:

Abstract

The purpose of this report is to present the analysis of the Lazarus Group's Cyber Attacks using the Soltra Edge TAXII service. The Soltra Edge and STIX objects will be used in this report to model the aspects of this lazarus Groups cyber attacks.

Scenario Introduction

The lazarus group is a famous NorthKorean based cybercriminal organisation, and they have been know to target financial institutions worldwide. This report analysis their attack targetted towards the Central Bank of Bangladesh dated in February 2016

Threat Actor

The lazarus group was run by North Korean government, however they have masked themselves as Russian hackers which allowed them to get away from researchers. To proxy network traffic , hackers used strings and specific debugging tools containing russian words to Client_TrafficForwarder new version, along with using the Russian commercial product the Enigma Protector for their executables protection.

Target

The target was the central bank in bangladesh which does financial transactions and keeps customer data that are sensitive.

Campaign

The opportunity for the attackers to hack into the banking system of Bangladesh is through the swift system. SWIFT verifies and does financial transactions across an international broad and is one of the most authentic ways in doing so.

The exploit

The hackers would try to send emails to the employers that disguise themselves as potential employees and will persuade them to click on the emails where malicious code will be installed.

<u>Stages of the Attack</u>

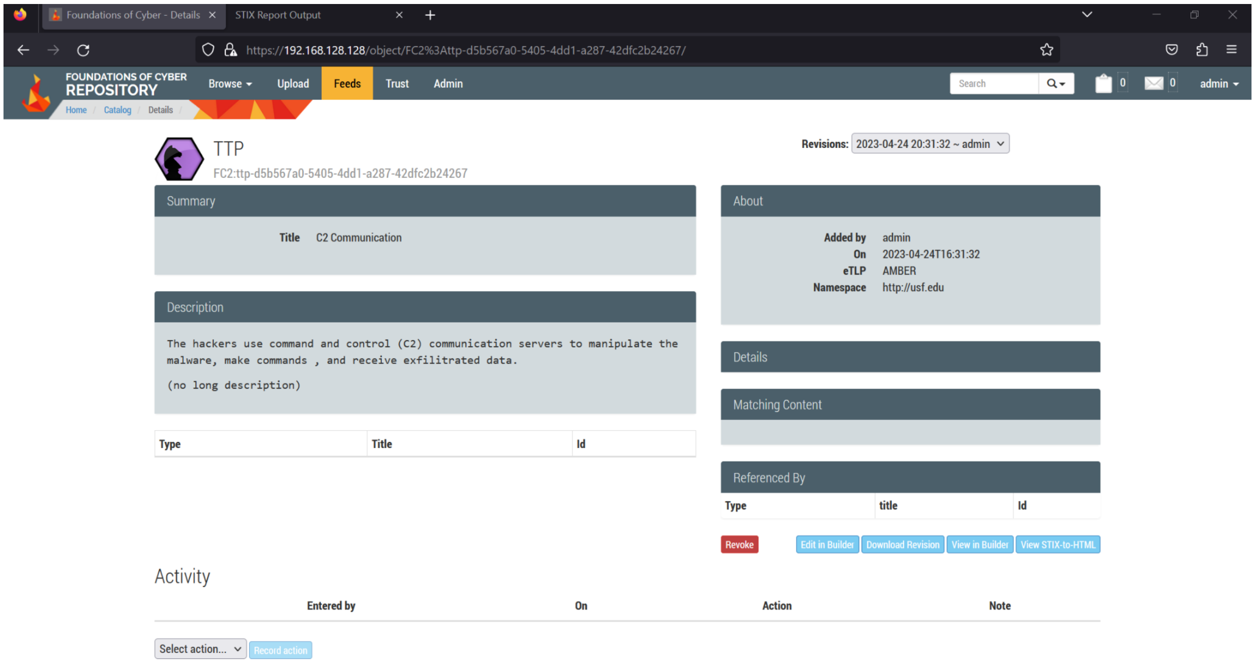
Reconnaissance: The Lazarus Group collected information on the financial institution, identifying key employees and systems to target

Weaponization: The malicious code was installed on the emails sent to employers in financial institutions. Client_TrafficForwarder was used alongside a dropper to download gpsvc.exe and MBLCTR.exe with byte size 75364

C & C: The Lazarus group used C2 methods to execute those malicious code

Actions on Objectives: The attackers initiated financial transactions that was unauthorized, by taking over the SWIFT system.

Soltra edge representation



Foundations of Cyber - Details
STIX Report Output
https://192.168.128.128/object/FC2%3Attp-d5b567a0-5405-4dd1-a287-42dfc2b24267/
FOUNDATIONS OF CYBER REPOSITORY
Browse
Upload
Feeds
Trust
Admin
Search
0
0
admin
Home / Catalog / Details /
Revisions: 2023-04-24 20:31:32 ~ admin
Revoke
Edit in Builder
Download Revision
View in Builder
View STIX-to-HTML
Select action...
Record action

TTP

FC2:ttp-d5b567a0-5405-4dd1-a287-42dfc2b24267

Summary

Title C2 Communication

About

Added by admin
On 2023-04-24T16:31:32
eTLP AMBER
Namespace http://usf.edu

Description

```
The hackers use command and control (C2) communication servers to manipulate the
malware, make commands , and receive exfiltrated data.
(no long description)
```

Type	Title	Id

Details

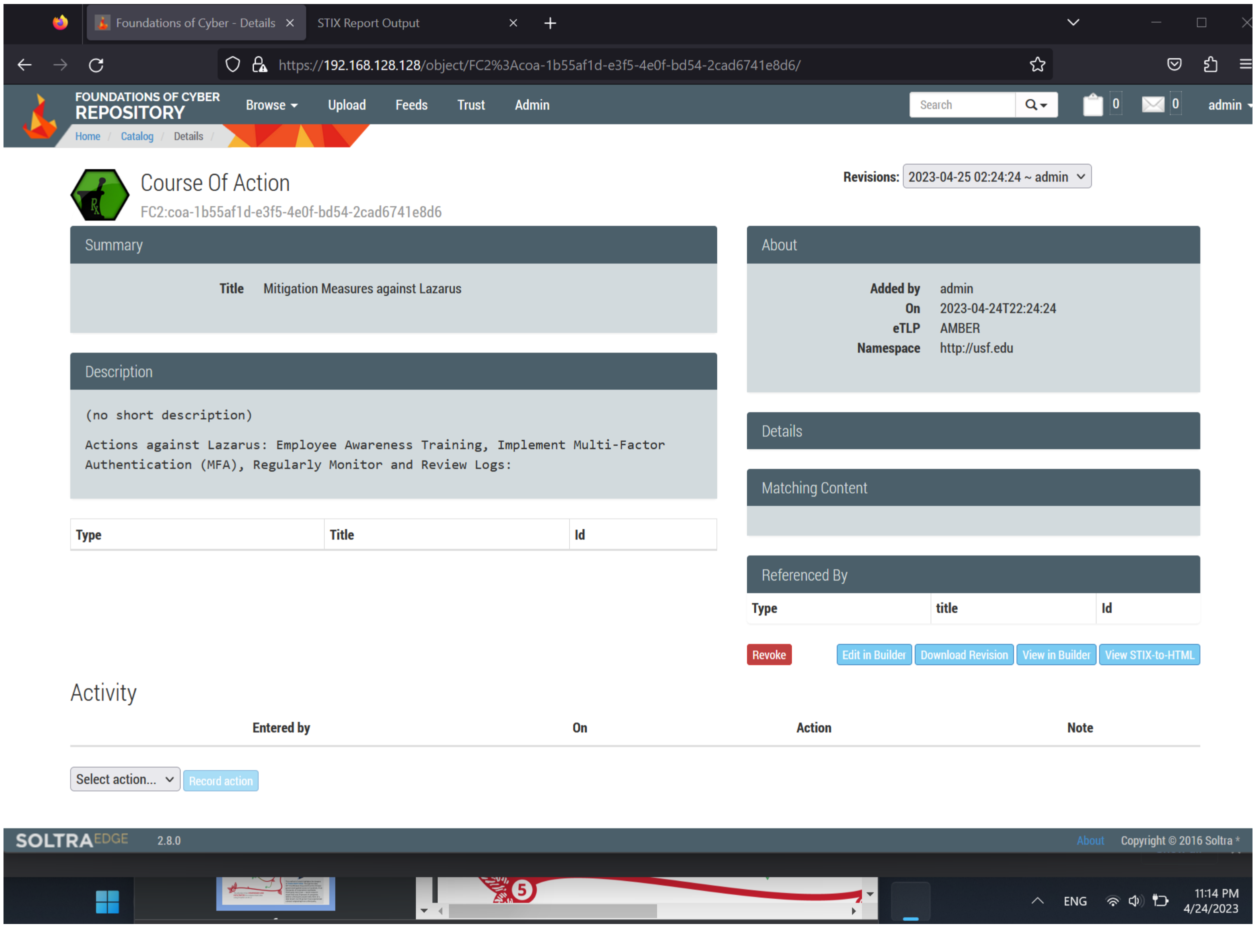
Matching Content

Referenced By

Type	title	Id

Activity

Entered by	On	Action	Note



Course Of Action

FC2:coa-1b55af1d-e3f5-4e0f-bd54-2cad6741e8d6

Revisions: 2023-04-25 02:24:24 ~ admin

Summary

Title	Mitigation Measures against Lazarus

About

Added by	admin
On	2023-04-24T22:24:24
eTLP	AMBER
Namespace	http://usf.edu

Description

```
(no short description)

Actions against Lazarus: Employee Awareness Training, Implement Multi-Factor
Authentication (MFA), Regularly Monitor and Review Logs:
```

Type	Title	Id

Details

Matching Content

Referenced By

Type	title	Id

Activity

Entered by	On	Action	Note

References

Lazarus Arisen: Architecture, Tools and Attribution - Group-IB.

https://www.group-ib.com/resources/research-hub/lazarus/.