

OpTinselTrace24-3: Blizzard Breakdown

Sherlock Scenario

Furious after discovering he's been left off the Nice List this holiday season, one particular elf - heavily influenced by Krampus - goes rogue, determined to take revenge. Consumed by anger, he hatches a sinister plan to sabotage Christmas by targeting Santa Claus' most critical asset - its \$3 data archive! This repository holds sensitive information, including blueprints for new toys, holiday logistics, toy production schedules, and most importantly, the coveted gift list! With Christmas preparations in full swing, any disruption to this storage could cause chaos across the entire operation, threatening to derail everyone's holiday season. Will the holiday magic prevail, or will Christmas fall into dismay?

Task 1:

The Victim Elf shared credentials that allowed the Rogue Elf to access the workstation. What was the Client ID that was shared?

I investigated the user lannyl folders and found a folder called IceChat Networks.

I opened all the logs inside the directory C:\Users\lanny\AppData\Local\IceChat Networks\IceChat\Logs\irc.quakenet.org\Query with NotePad++ and found the client ID inside the W4yne-2024-11-13.log

```
[04:09.49] <W4yne> Great! Once it's running, send me your ID so I can connect and set things up for you.
[04:20.46] <Lanny> Sorry for the delay, I was just on a call.
[04:20.59] <Lanny> 95 192 516
```

Answer: 95192516

Task 2:

What is the IP address of the Rogue Elf used during the attack?

IP is in the same place like previous task:

```
Session Start: Wed Nov 13 03:37:28 2024
[03:37.28] <Wayne> Hey there, Lanny! Getting used to the workshop systems yet?
[03:37.29] ->> Wayne is ~IceChat95@146.70.202.35 (The Chat Cool People Use)
[03:37.29] ->> Wayne is on: #SnowHub
```

Answer: 146.70.202.35

Task 3:

What is the name of the executable the victim ran to enable remote access to their system?

I checked the Amcache and noticed some suspicious executable named aa_v3.exe.

The SHA1 was known as Ammy Admin

SHA1	Is Os Component	Full Path	Name
	<input checked="" type="checkbox"/>		
050b7eba825412b24e3f02d76d7da5ae97e10502	<input type="checkbox"/>	c:\users\lanny1\downloads\aa_v3.exe	AA_v3.exe

Answer: AA_V3.EXE

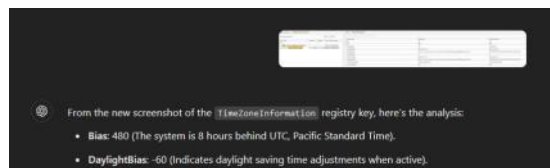
Task 4:

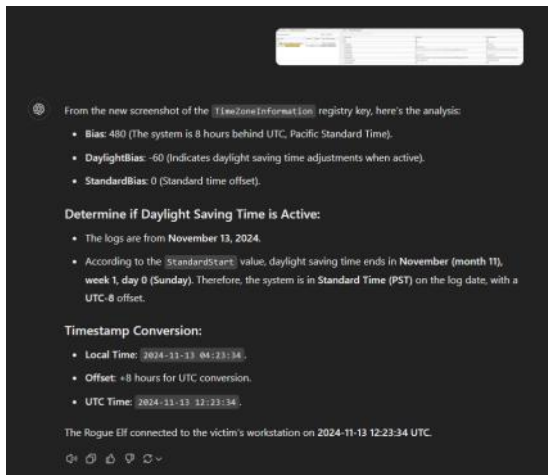
What time (UTC) did the Rogue Elf connect to the victim's workstation?

I checked the IceChat logs but the answer was not there.

Then I found in ProgramData the Ammyy folder but the timestamp was not there too.

I asked the ChatGPT and he told me to use check the System Hive TimeZoneInformation

[illegible]



Answer: 2024-11-13 12:23:34

Task 5:

The Rogue Elf compromised an AWS Access Key. What is the AWS Access Key ID obtained from the victim's workstation?

I searched for the Rogue Elf IP inside the AWS logs

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDA52GPOBQCHOIPNIEEH",
  "arn": "arn:aws:iam:949622803460:user/arctic-archive-user",
  "accountId": "949622803460",
  "accessKeyId": "AKIA52GPOBQCBFYGAYHI",
  "userName": "arctic-archive-user"
},
"eventTime": "2024-11-13T15:23:22Z",
"eventSource": "sts.amazonaws.com",
"eventName": "GetCallerIdentity",
"awsRegion": "us-east-1",
"sourceIPAddress": "146.70.202.35",
```

Answer: AKIA52GPOBQCBFYGAYHI

Task 6:

Which S3 bucket did the Rogue Elf target during the incident?

Found the S3 bucket at the bottom of the previous task log

```
"sourceIPAddress": "146.70.202.35",
"userAgent": "[aws-cli/2.20.0 md/awscrt#0.22.0]",
"requestParameters": {
  "list-type": "2",
  "bucketName": "arctic-archive-freezer",
```

Answer: arctic-archive-freezer

Task 7:

Within the targeted S3 bucket, what is the name of the main directory where the files were stored?

Same like previous task, the right log is at the bottom

```
"eventName": "ListObjects",
"awsRegion": "us-east-1",
"sourceIPAddress": "146.70.202.35",
"userAgent": "[aws-cli/2.20.0 md/awscrt#0.22.0 ua/2.0 os/windows#10]",
"requestParameters": {
  "list-type": "2",
  "bucketName": "arctic-archive-freezer",
  "encoding-type": "url",
  "prefix": "Claus_Operation_Data/",
  "delimiter": "/",
  "Host": "arctic-archive-freezer.s3.us-east-1.amazonaws.com"
```

Answer: Claus_Operation_Data

Task 8:

What time (UTC) did the Rogue Elf disable versioning for the S3 bucket?

I searched for status - Suspended

```
"eventTime": "2024-11-13T15:31:15Z",
"eventSource": "s3.amazonaws.com",
"eventName": "PutBucketVersioning",
"awsRegion": "us-east-1",
"sourceIPAddress": "146.70.202.35",
"userAgent": "[aws-cli/2.20.0 md/awscrt#0.22.0 ua/2.0 os/windows#10
"requestParameters": {
  "bucketName": "arctic-archive-freezer",
  "Host": "arctic-archive-freezer.s3.us-east-1.amazonaws.com",
  "versioning": "",
  "VersioningConfiguration": {
    "Status": "Suspended",
    "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/"
  }
}
```

Answer: 2024-11-13 15:31:15

Task 9:

What is the MITRE ATT&CK Technique ID associated with the method used in Question 8?

I asked the ChatGPT

The action of disabling versioning for an S3 bucket aligns with the MITRE ATT&CK technique **T1490: Inhibit System Recovery**. This technique involves adversaries hindering or preventing recovery mechanisms, such as disabling or modifying backup and versioning features, to make it more difficult to restore systems or data after an attack. MITRE ATT&CK

In the context of AWS S3, suspending bucket versioning can prevent the recovery of previous versions of objects, thereby inhibiting system recovery efforts. This tactic is often employed in ransomware attacks to ensure that victims cannot easily restore their data without paying the ransom. SPLUNK RESEARCH

Therefore, the MITRE ATT&CK Technique ID associated with disabling versioning for the S3 bucket is **T1490**.

Answer: T1490

Task 10:

What time (UTC) was the first restore operation successfully initiated for the S3 objects?

I searched for the event name "RestoreObject"

```
},
"eventTime": "2024-11-13T15:43:49Z",
"eventSource": "s3.amazonaws.com",
"eventName": "RestoreObject",
"awsRegion": "us-east-1",
"sourceIPAddress": "146.70.202.35",
"userAgent": "[aws-cli/2.20.0 md/awscrt#0.22.0 ua/2.0 os/windows#10
"requestParameters": {
  "bucketName": "arctic-archive-freezer",
  "Host": "arctic-archive-freezer.s3.us-east-1.amazonaws.com",
  "RestoreRequest": {
    "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
    "Days": 1,
    "GlacierJobParameters": {
      "Tier": "Expedited"
    }
  }
},
"restore": "",
"key": "Claus_Operation_Data/AI_HoHoHoliday_Helper_Link.txt"
```

Answer: 2024-11-13 15:43:49

Task 11:

Which retrieval option did the Rogue Elf use to restore the S3 objects?

Same in previous task

Answer: Expedited

Task 12:

What is the filename of the S3 object that the Rogue Elf attempted to delete?

I analyzed several logs until a I found some csv file

```

"bucketName": "arctic-archive-freezer",
"Host": "arctic-archive-freezer.s3.us-east-1.amazonaws.com",
"RestoreRequest": {
  "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
  "Days": 1,
  "GlacierJobParameters": {
    "Tier": "Expedited"
  }
},
"restore": "",
"key": "Claus Operation Data/gift lists/GiftList Worldwide.csv"

```

Answer: GiftList_Worldwide.csv

Task 13:

What is the size (MB) of the S3 object that the Rogue Elf targeted in Question 12?

I found that the mentioned object was downloaded in parts, each part beign 8,388,608 bytes. There were a total of 19 parts, and the total size was 152 MB.

Answer: 152

Task 14:

The Rogue Elf uploaded corrupted files to the S3 bucket. What time (UTC) was the first object replaced during the attack?

I searched for event name PutObject and found the file

```

{
  "eventTime": "2024-11-13T16:10:03Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "146.70.202.35",
  "userAgent": "[aws-cli/2.20.0 md/awscrt#0.22.0 ua/2.0 os/windows#10",
  "requestParameters": {
    "bucketName": "arctic-archive-freezer",
    "Host": "arctic-archive-freezer.s3.us-east-1.amazonaws.com",
    "key": "Claus_Operation_Data/AI_HoHoHoliday_Helper_Link.txt",
    "x-amz-storage-class": "GLACIER"
  }
}

```

Answer: 2024-11-13 16:10:03

Task 15:

What storage class was used for the S3 objects to mimic the original settings and avoid suspicion?

Same in previous task

```

{
  "x-amz-storage-class": "GLACIER"
},
"responseElements": {
  "x-amz-server-side-encryption": "AES256",
  "x-amz-storage-class": "GLACIER"
}

```

Answer: glacier