EDITH COWEN UNIVERSITY

Assignment 1: Workshop Exercise

Cyber Security Incident Detection and Response

CSI3351.1

Name: Tanushka ELVITIGALA

SID: 10663914

lecturer: Dr. Jude Kiruparetnam

Name: Tanushka Elvitigala
ECU ID:10663914

Table of Contents

Name: Tanushka Elvitigala
ECU ID:10663914

Table Content

Figures Content

EXECUTIVE SUMMARY

In this report, we outline a comprehensive account of a sophisticated cyber attack on Frothly. The attack was executed with a high level of precision and involved multiple stages of malicious activity. Here's a detailed summary of what occurred:

I. **Initial Breach and Access**: The attackers initially compromised a cloud account associated with Frothly, using it to access and manipulate various cloud resources. They attempted to perform administrative tasks, including creating new resources and launching instances. This initial access set the stage for more severe actions.

II. **Malware Deployment**: The attackers uploaded a malicious Excel file named Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm. This file contained a hidden executable (HxTsr.exe), which was detected by security systems but only after significant damage had been done. This file was part of a broader strategy to implant malware on the compromised systems.

III. **Malicious Tool Usage**: Following the deployment of the malware, the attackers used it to execute further attacks. They ran scripts and tools that allowed them to scan the network, deploy additional malicious files, and gain higher levels of access to the system. They also utilized iexplorer.exe and other executables to execute remote code, escalate privileges, and manipulate system settings.

IV. **Unauthorized Activities and Data Theft**: The attackers performed a series of unauthorized actions, including cryptocurrency mining using the compromised systems. They also made significant changes to user accounts, such as disabling a key account and exfiltrating sensitive data. This included uploading and manipulating files in cloud storage and making a cloud bucket public, exposing potentially valuable information.

V. **Detection and Response**: The attack involved multiple interactions with Command and Control (C2) servers and involved extensive communication with external servers. Security systems detected various stages of the attack, including the creation of new user accounts and the start of brute force attacks. The final stages included efforts to clean up traces of the attack, such as making the cloud bucket private again and ending unauthorized mining activities.

VI. **Ongoing Concerns**: Even after initial response actions, the attack underscored vulnerabilities in the system and highlighted the need for more robust security measures. The recovery efforts focused on securing the systems, restoring normal operations, and preventing similar incidents in the future.

In summary, this report details a complex and multi-faceted attack on Frothly, illustrating the advanced tactics used by the attackers and the ongoing efforts required to address and mitigate such threats. The incident emphasizes the importance of maintaining vigilant security practices and being prepared to respond effectively to cyber threats.

1.0 INTRODUCTION

This report provides a detailed examination of a sophisticated cyber-attack on Frothly, outlining the sequence of events, investigative methods, and actions taken to address and mitigate the incident. The purpose of this report is to offer a comprehensive overview of the attack's impact, the steps followed during the investigation, and the measures implemented to secure the environment and prevent future breaches.

1.1 Overview of the Report

The report is structured to provide a clear understanding of the attack's progression, from the initial breach to the final recovery actions. It begins with an executive summary that outlines the key findings and overall impact of the attack. The main body of the report delves into the specifics of the incident, detailing the timeline of events, the nature of the malicious activities conducted, and the detection and response efforts. The report concludes with recommendations for enhancing security measures based on the lessons learned from the attack.

1.2 Investigation Approach

The investigation into the cyber-attack was approached methodically, focusing on several key aspects:

- **Initial Detection**: The investigation began with identifying the initial signs of the attack, which included unusual activities and potential security breaches (Van & Forno, 2001). This phase involved analyzing logs and alerts from various security systems to pinpoint the start of the attack.
- **Data Collection and Analysis**: Detailed examination of logs, system alerts, and network traffic was conducted to understand the scope and nature of the attack. This included reviewing event logs, file uploads, and interactions with external servers (Van & Forno, 2001). Special attention was given to identifying malicious files and tracking their deployment across the compromised systems.
- **Recovery and Recommendations**: The final phase involved recovering from the attack and strengthening security measures to prevent future incidents. This included restoring data, updating security protocols, and conducting a thorough review of the organization's cybersecurity posture.

1.3 Actions Undertaken

- **Post-Incident Review**: A comprehensive review was conducted to assess the effectiveness of the response and identify areas for improvement (O365 Advanced Threat Protection, n.d.). This included analyzing the attack's impact, evaluating the response actions, and developing recommendations for enhancing security measures.
- **Reporting**: Detailed documentation of the attack and response efforts was prepared, including this report, to provide insights into the incident and support ongoing security improvements.

2.0 Technical Details

In this section, we delve into the technical aspects of the cyberattacks identified during the investigation. By mapping each attack against the Lockheed Martin Cyber Kill Chain and the MITRE ATT&CK Framework, we can better understand the attacker's tactics, techniques, and procedures (TTPs). This approach provides a structured way to categorize the various phases of the attacks and assess their impact (*CyberDefenders: Blue Team CTF Challenges | Boss of the SOC V3*, 2023). We'll examine each identified attack, detailing its characteristics, the corresponding phases of the Kill Chain it affects, and the relevant techniques from the MITRE ATT&CK Framework. This analysis not only highlights the progression of the attacks but also aids in identifying defensive measures and response strategies.

Name: Tanushka Elvitigala
ECU ID:10663914

Aligning Cases with the Lockheed Martin Cyber Kill Chain

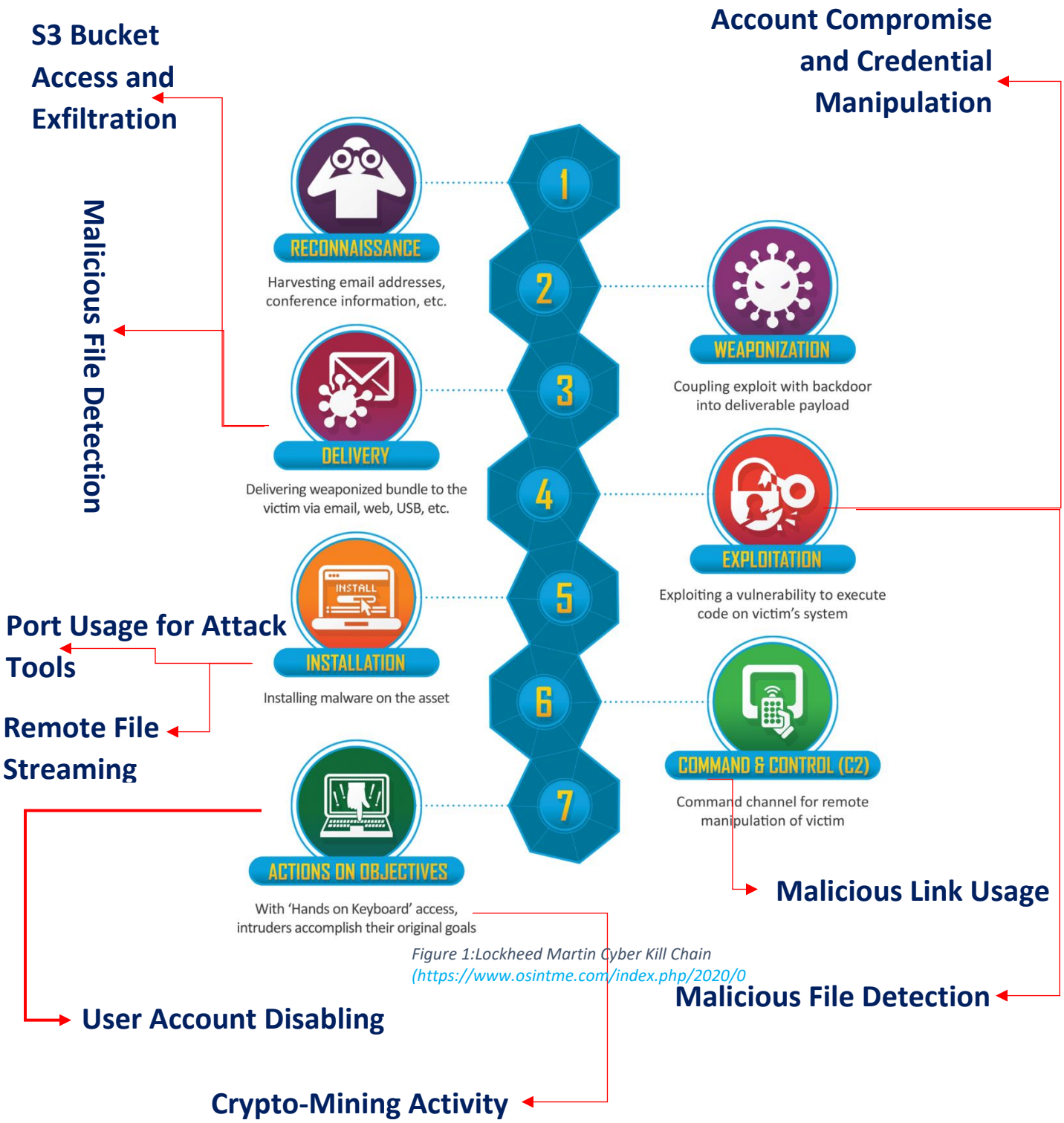


Figure 1:Lockheed Martin Cyber Kill Chain (https://www.osintme.com/index.php/2020/0

Name: Tanushka Elvitigala
ECU ID:10663914

Aligning Cases with the MITRE ATT&CK Framework

User Account Disabling

Remote File Streaming

Account Compromise and Credential Manipulation

Figure 2:MITRE ATT&CK Framework
(https://delinea.com/blog/what-is-the-

S3 Bucket Access and Exfiltration

Malicious File Detection

Crypto-Mining Activity

Port Usage for Attack

Malicious Link Usage

2.1 Case 1: User Account Disabling

Description of the Attack:

During the investigation, it was found that a user's domain account was disabled. The user whose account was disabled was bgist@froth.ly, and the account responsible for this action was fyodor@froth.ly.

Lockheed Martin Cyber Kill Chain:

- Actions on Objectives: The disabling of a user account falls under this phase as it affects the operational capabilities of the targeted user (Wang et al., 2021).

MITRE ATT&CK Framework:

- Account Manipulation (T1136): The action of disabling a user account is a form of manipulating accounts to disrupt or control access.
- Impair Defenses (T1562): By disabling accounts, attackers impair the defenses of the organization by removing critical users from the system.

2.2 Case 2: Malicious File Detection

Description of the Attack:

In this case, a series of phishing emails resulted in the detection of a malicious file named **Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm.** This file was designed to execute malicious payloads upon opening (Van & Forno, 2001). The embedded executable within the file, named **HxTsr.exe**, was detected by both Sysmon and Symantec security solutions. The HxTsr.exe file exhibited malicious behavior, but a deeper investigation also uncovered the presence of another suspicious executable**, hdoor.exe**, and **image files** that executed PowerShell commands.

Lockheed Martin Cyber Kill Chain:

- Delivery: The phishing emails served as the initial vector for delivering the malicious Excel file to the target system.
- Exploitation: The malicious Excel file was opened by the user, leading to the execution of the embedded HxTsr.exe payload (Wang et al., 2021). This execution further triggered the creation and execution of additional malicious files, including hdoor.exe and scripts embedded in image files.

MITRE ATT&CK Framework:

- Phishing (T1566): The phishing emails were used to deliver the initial malicious file (MITRE, 2024). This technique is commonly employed to trick users into downloading and opening files that contain malicious payloads.
- Execution (T1203): The opening of the malicious Excel file resulted in the execution of the embedded HxTsr.exe. This is a classic exploitation technique where malicious code is executed as a result of user interaction with a compromised file.
- Malware (T1071): HxTsr.exe is classified as malware, designed to perform unauthorized actions on the compromised system. Its detection by Sysmon and Symantec indicates its malicious nature.
- Command and Scripting Interpreter (T1059): The image files that executed PowerShell commands suggest that the attackers used PowerShell as a scripting language to perform further malicious activities on the system (Attack Signature Detail Page, n.d.). This technique is often used for tasks such as executing additional payloads or creating persistence mechanisms.
- Persistence (T1543): The additional executable hdoor.exe may have been used to establish persistence or maintain access on the compromised system. This executable, alongside the image files running PowerShell, indicates an effort to ensure continued control and access to the system.

2.3 Case 3: Malicious Link Usage

Description of the Attack: The link file **BRUCE BIRTHDAY HAPPY HOUR PICS.lnk** was used multiple times, with various IP addresses accessing it (Dr. Nadine Shillingford, 2023). This link facilitated the attacker's communication with their infrastructure.

Lockheed Martin Cyber Kill Chain:

- Command and Control: The use of the link indicates a method for the attacker to communicate with their command-and-control server.

MITRE ATT&CK Framework:

- Command and Control (T1071): The link facilitated communication with the attacker's server for command-and-control purposes (Wang et al., 2021).
- Network Reconnaissance (T1595): The usage of the link file involves gathering information about the network or systems for further exploitation.

2.4 Case 4: Port Usage for Attack Tools

Description of the Attack:

The adversary used **port 3333** to download attack tools. This port was found to be rarely used and was associated with suspicious activities.

Lockheed Martin Cyber Kill Chain:

- Installation: The use of a specific port to download tools indicates the installation phase of the attack.

MITRE ATT&CK Framework:

- Data Staged (T1074): Using a port to stage the download of attack tools involves preparing data for exfiltration or further exploitation.

2.5 Case 5: Remote File Streaming

Description of the Attack:

Two files**, /tmp/definitelydontinvestigatethisfile.sh** and **/tmp/colonel**, were streamed to a Linux server's **/tmp directory.**

Lockheed Martin Cyber Kill Chain:

- Installation: Streaming files to the /tmp directory indicates the installation of additional tools or scripts (Wang et al., 2021).

MITRE ATT&CK Framework:

- File and Directory Discovery (T1083): Streaming files to a known directory involves discovering and using system directories for further activities.

2.6 Case 6: Crypto-Mining Activity

Description of the Attack:

A **Coinhive** DNS lookup was initiated, followed by the detection of **JSCoinMiner and Chrome Monero mining** on the compromised systems.

Lockheed Martin Cyber Kill Chain:

- Actions on Objectives: The use of crypto-mining malware is aimed at generating illicit revenue from compromised systems.

MITRE ATT&CK Framework:

- Cryptojacking (T1496): The attack involved unauthorized use of system resources for cryptocurrency mining.

2.7 Case 7: S3 Bucket Access and Exfiltration

Description of the Attack:

The attacker made the S3 bucket **frothlywebcode** public, uploaded files, and later made the bucket private again.

Lockheed Martin Cyber Kill Chain:

- Exfiltration: Making the bucket public and uploading files indicate data exfiltration activities.

MITRE ATT&CK Framework:

- Data Exfiltration (T1041): Accessing and modifying cloud storage settings for data exfiltration.

2.8 Case 8: Account Compromise and Credential Manipulation

Description of the Attack:

Multiple actions were taken on Azure AD accounts, including activation, password resets, and changes. Additionally, a domain admin account was compromised.

Lockheed Martin Cyber Kill Chain:

- Exploitation: The manipulation of Azure AD accounts and domain admin credentials indicates exploitation of administrative privileges (Wang et al., 2021).

MITRE ATT&CK Framework:

- Credential Dumping (T1003): The manipulation and resetting of credentials to gain further access (MITRE, 2024).
- Account Manipulation (T1136): Creating, modifying, and resetting accounts to maintain access

The cases reviewed demonstrate a sophisticated and multi-faceted approach to cyberattacks, beginning with phishing and culminating in advanced malware deployment and execution techniques (Dr. Nadine Shillingford, 2023). The incidents highlight the attackers' use of phishing to deliver malicious payloads, which, once executed, led to further compromise through additional malware and exploitation of system vulnerabilities. By leveraging various attack techniques from the Lockheed Martin Cyber Kill Chain and MITRE ATT&CK Framework, the attackers were able to establish persistence, execute unauthorized commands, and exfiltrate sensitive information. These cases underscore the importance of robust cybersecurity measures, including effective phishing defenses, vigilant monitoring of system activities, and prompt detection and response to malicious threats.

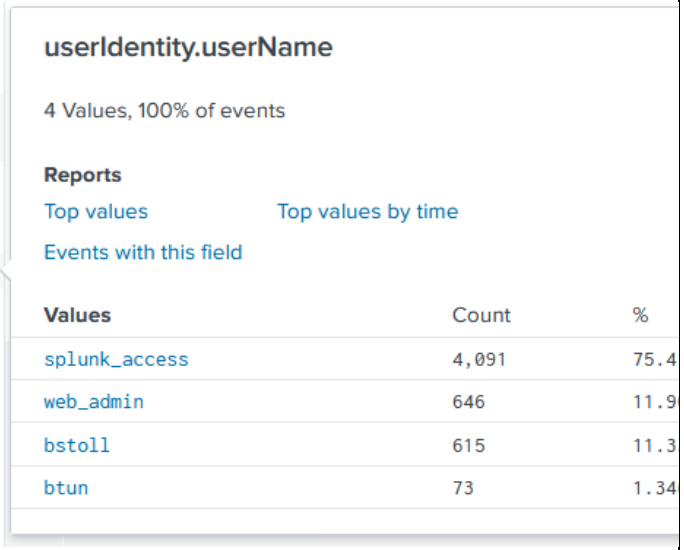
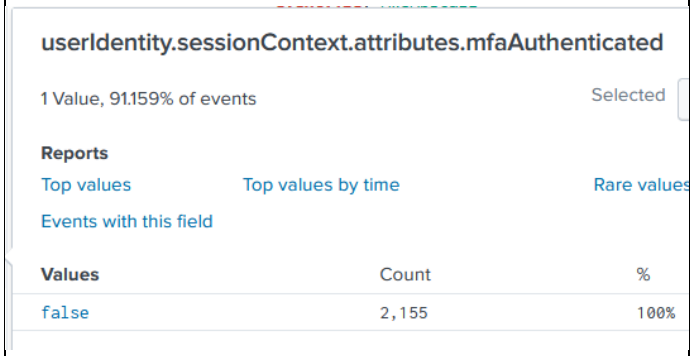
3.0 Recommendations

To enhance defenses against the types of attacks detailed in this report, organizations should implement the following measures:

- Strengthen Phishing Defenses: Employ advanced email filtering solutions to detect and block phishing attempts (Van & Forno, 2001). Regularly train employees on recognizing phishing emails and potential threats to minimize the risk of successful attacks.
- Enhance Endpoint Protection: Use comprehensive endpoint security solutions to detect and mitigate malicious files and executables. Implement real-time monitoring and automated threat detection to identify and respond to suspicious activities quickly.
- Regular Security Audits: Conduct frequent security audits and vulnerability assessments to identify and address potential weaknesses in the system. Regularly update and patch software to protect against known vulnerabilities.
- Improve Incident Response: Develop and maintain a robust incident response plan to ensure rapid and effective action in the event of a security breach (Van & Forno, 2001). This includes setting up monitoring tools to detect anomalies and having a clear process for containment and remediation.
- Access Controls and Monitoring: Implement strict access controls and regularly review user permissions. Utilize monitoring tools to track and log user activities, especially those involving sensitive data and critical systems.
- Data Protection and Encryption: Ensure that sensitive data is encrypted both in transit and at rest. Regularly back up important data and test backup restoration processes to mitigate the impact of data loss or corruption.

By adopting these recommendations, organizations can significantly improve their cybersecurity posture and reduce the likelihood of successful attacks, thereby protecting their assets and ensuring operational continuity.

4.0 RUNNING SHEET

N0.	Query	Query Description	Output	Output Description
01	index=botsv3 sourcetype="*aws*" *IAM*	To list IAM users accessing AWS services, this query searches AWS logs for any reference to IAM users. By filtering for IAM in the logs and focusing on userIdentity.userName, it identifies which IAM users interacted with the AWS environment.		Lists the IAM users who accessed AWS services. The identified users are bstoll, btun, splunk_access, and web_admin, indicating who was involved in service access and potential misuse.
02	index=botsv3 sourcetype="*aws*" *MFA*	Identifies the field used to alert AWS API activity without MFA by searching for logs related to MFA authentication. The field userIdentity.sessionContext.attributes.mfaAuthenticated indicates whether MFA was used during the API request.	 userIdentity.sessionContext.attributes.mfaAuthenticated	The field indicates whether MFA was used (true or false). This is important for identifying API calls that lack MFA protection, potentially highlighting security gaps.

03	index=botsv3 sourcetype="hardware"	Searches for hardware-related logs to determine the processor model used in web servers. By focusing on fields related to hardware specifications, it identifies the processor model, which can be useful for understanding hardware capabilities and performance issues.	KEY VALUE CPU_TYPE Intel(R) Xeon(R) CPU E5-2676 v3 @ CPU_CACHE 30720 KB CPU_COUNT 2 HARD_DRIVES xvda 8 GB; NIC_TYPE <notAvailable> NIC_COUNT 1 MEMORY_REAL 4041808 kB MEMORY_SWAP 0 kB Collapse host = gacrux.i-09cbc261e84259b54 source = hardware	The processor model identified is E5-2676. Knowing the processor model helps in assessing the server's performance and identifying any anomalies or issues related to hardware.
04	index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" requestParameters.bucketName="*"	This query retrieves the event ID associated with making an S3 bucket publicly accessible. The PutBucketAcl event modifies the access control list (ACL) of the bucket. The event ID helps trace the exact API call responsible for the change in bucket permissions.	awsRegion: us-west-1 eventID: ab45689d-69cd-41e7-8705-5350402cf7ac eventName: PutBucketAcl eventSource: s3.amazonaws.com eventTime: 2018-08-20T13:01:46Z	The event ID ab45689d-69cd-41e7-8705-5350402cf7ac corresponds to the API call that altered the bucket's access settings, potentially making it publicly accessible.
05	index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" requestParameters.bucketName="*"	Identifies the name of the S3 bucket that was made publicly accessible by querying the `requestParameters.bucketName` field from the `PutBucketAcl` event. This helps in identifying the specific bucket affected by the configuration change.	requestParameters.bucketName 1 Value, 100% of events Reports Top values Top values by time Events with this field Values Cc frothlywebcode 1	The name of the bucket exposed is `frothlywebcode`. Knowing the bucket name helps in assessing what data might be at risk due to the exposure.

06	index=botsv3 sourcetype="aws:s3:accesslogs" "frothlywebcode" "*.txt"	Searches for text files uploaded to the publicly accessible S3 bucket by querying the access logs for `.txt` files. This query helps identify specific files that were uploaded and accessed while the bucket was exposed.	**prefix** 1 Value, 33.333% of events **Reports** Top values Top values by time Events with this field **Values** OPEN_BUCKET_PLEASE_FIX.txt	The file `OPEN_BUCKET_PLEASE_FIX.txt` was uploaded to the `frothlywebcode` bucket. This indicates that a specific text file was part of the public access issue.
07	index=botsv3 sourcetype="aws:s3:accesslogs" "frothlywebcode" "*.tar.gz" "REST.PUT.OBJECT"	Determines the size of `.tar.gz` files uploaded to the `frothlywebcode` bucket. This query examines the access logs for `.tar.gz` file uploads to measure their size, indicating the volume of data that was exposed.	`REST.PUT.OBJECT frothly_html_memcache Botocore/1.8.12" -` 2.93 MB	The size of the `.tar.gz` file is 2.93 MB. This helps in understanding the amount of data that might have been compromised during the public exposure of the bucket.

08	index=botsv3 sourcetype="cloud-init-output" packages	Retrieves the number of packages and dependent packages installed by analyzing `cloud-init-output` logs. This query helps verify the software installed during the cloud instance initialization, which is important for identifying any unauthorized changes.	`Install 7 Packages (+13 Dependent packages)`
			`Total download size: 18 M`
			`Installed size: 55 M`
			`Downloading packages:`
			`warning: /var/cache/yum/x86_64/latest/osquery-s`
			`Public key for osquery-3.2.6-1.linux.x86_64.rpm`
				The installation included 7 packages and 13 dependent packages. This information is used to ensure that only authorized software is installed on the system.

09	`index="botsv3" Coinhive`	Searches for the presence of Coinhive, a known cryptocurrency miner, to identify endpoints involved in mining Monero. This helps in pinpointing endpoints suspected of cryptojacking activities.	**host** 3 Values, 100% of events **Reports** Top values Top values by time Events with this field **Values** Count BSTOLL-L 21	The hostname `BSTOLL-L` is identified as the endpoint involved in cryptocurrency mining. This indicates which specific endpoint was compromised for mining activities.
10	index="botsv3" Coinhive sourcetype="stream:dns"	Counts the number of distinct cryptocurrency mining destinations visited by querying DNS logs for Coinhive-related queries. This provides insights into how many different mining servers were contacted by the endpoints.	**query{}** 6 Values, 50% of events **Reports** Top values Top values by time Events with this field **Values** Count coinhive.com 2 ws001.coinhive.com 1 ws005.coinhive.com 1 ws011.coinhive.com 1 ws014.coinhive.com 1 ws019.coinhive.com 1	Six unique mining destinations were visited. This helps quantify the extent of the mining activity across different servers.

11	index="botsv3" host="SEPM" *signature*	Retrieves the first signature ID related to the coin miner threat from Symantec Endpoint Protection (SEP) logs. This signature ID helps identify the specific coin miner threat detected by SEP.	34116F08B2C090E34C2D506183F9BCA,MD-5: ,[SID: 30358] Web Atta ROME\APPLICATION\CHROME.EXE,Local: 192.168.3.130,Local: 0000 18-08-18 21:00:27,Occurrences: 1,Application: C:/PROGRAM FIL t 80,CIDS Signature ID: 30358,CIDS Signature string: Web Att Payload URL: tion Manager\data\d... sourcetype = symantec:ep:security:file	Signature ID `30358` is associated with the coin miner threat. This ID is used to understand which threat signature was first detected.
12	Google search	Looks up the severity of the coin miner threat with signature ID `30358` on Symantec's website. This provides information about the threat's impact level.	C:/PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATION/CHROME. tring: Web Attack: JSCoinminer Download 8,CIDS Signature medium	The severity of the threat is classified as `Medium`. This indicates the potential risk level of the coin miner threat according to Symantec.
13	index="botsv3" host="SEPM" *signature*	The goal of this query was to find the short hostname of the Frothly endpoint that successfully mitigated a cryptocurrency mining threat. The search used the index "botsv3" and host "SEPM," focusing on signature logs related to the mitigation. This query aims to identify which system played a key role in stopping the threat.	20 13:46:47,Major,BTUN-L,SHA-256: 268A0463D7CB907D45E1C been blocked for this application: C:\PROGRAM FILES (X8 0000,Inbound,TCP,Intrusion ID: 0,Begin: 2018-08-18 21:0 Default,User: BillyTun,Domain: AzureAD,Local Port 6349 Intrusion URL: www.brewertalk.com/ Intrusion Payload U	The short hostname "BTUN-L" was identified as the endpoint that successfully stopped the cryptocurrency mining activity. The output indicates that this system was involved in mitigating the threat based on the logs.
14	index="botsv3" source="cisconvm sysdata" "windows 10"	Queries Cisco NVM flow data to find the FQDN of an endpoint running Windows 10. This helps identify systems running a different OS version from the others in the environment.	/="nvzFlow_v3" ysn="BGIST-L.froth.ly" udid="1DD75F nvmsysdata sourcetype = syslog	The FQDN `BSTOLL-L.froth.ly` is the endpoint running Windows 10. This information is used to identify discrepancies in OS versions across endpoints.

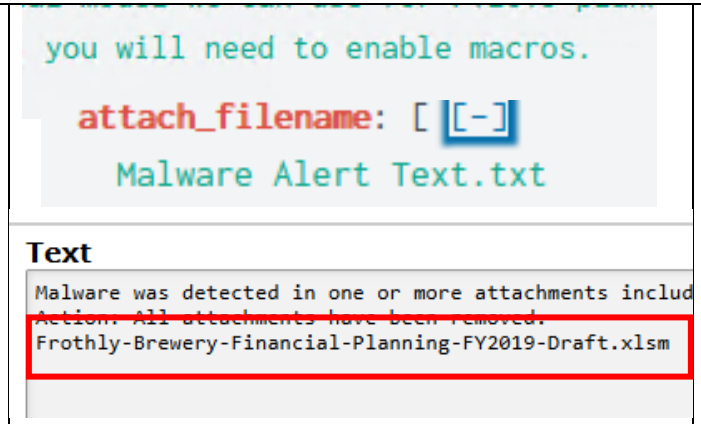
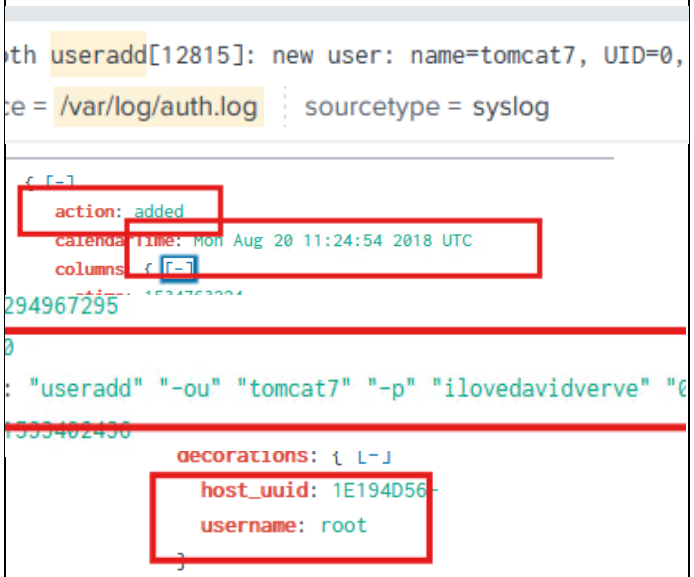
15	`index="botsv3" source="cisconvm flowdata" coinhive	stats min(fss) as starttime, max(fes) as endtime	timetaken 1667	Calculates the duration of cryptocurrency mining activity by analyzing flow data for Coinhive. This helps measure how long the mining activity persisted.
16	index="botsv3" sourcetype="stream:smtp" bud	Searches for emails sent by Bud that include file attachments with Splunk visualizations related to the coin miner issue. The visualizations help illustrate the problem to recipients.	sender: Bud Stoll <bstoll@froth.ly> sender_alias: Bud Stoll sender_email: bstoll@froth.ly server_response: 250 2.0.0 Ok: queued illy. I did find the issue! Look at the Splunk chart below - s spin up which was strange. Then I looked at the CPU of my I owser and noticed it spiked to 100%! I will work on recoverir ks like some malicious code got into our forums. 002.jpg@01D4247D.2394E720]	The output shows that the visualization attached in Bud's email was a column chart. This chart was used to illustrate the cryptocurrency mining threat, providing visual evidence to Frothly employees.
17	index="botsv3" sourcetype="aws""userIdentity.type"=IAMUser errorcode eventSource="iam.amazonaws.com"	stats dc(errorMessage) as errors by userIdentity.accessKeyId	userIdentity.accessKeyId AKIAJOGCDXJ5NW5PXUPA AKIAIGKL572SFDPOKLHA ASIAZB6TMXZ7MJUJJK6X	The query focused on identifying which IAM user's access key generated the most distinct errors when accessing IAM resources. It searched AWS CloudTrail logs for IAM user types, filtering for error messages related to failed access attempts. The goal was to determine the most problematic access key.

18	index="botsv3" aws support case	This query aimed to find the support case ID created by Amazon after Bud Stoll accidentally leaked AWS access keys, leading to a security compromise. By searching through the AWS support case logs, the query looks for correspondence related to the compromised AWS account.	New Support case: 5244329601 src_mac: 06:E3:CC:18:AA:33 src_port: 46966 subject: Amazon Web Services: New Supp time_taken: 380680 timestamp: 2018-08-20T09:16:54.880499Z	The output reveals that AWS support opened case ID "5244329601" on Bud's behalf after detecting the security breach caused by the accidental key leak. This support case reflects Amazon's response to the reported incident.
19	index="botsv3" aws support case	Building on the previous investigation, this query was designed to find the actual secret access key that was leaked to an external code repository. Searching the same logs, the query aimed to uncover the specific key details.	https://github.com/FrothlyBeers/BrewingIOT/ = AKIAJOGCDXJ5NW5PXUPA key = Bx8/gTsYC98T0oWiFhpmdROqhELPtXJSR9vFPNGk	The output provided the secret access key that was compromised: "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." This key was exposed to an external repository, leading to unauthorized access.

20	index="botsv3" sourcetype=*aws* userIdentity.accessKeyId="AKIAJOGCDXJ5NW5PXUPA"	This query sought to identify what resource the adversary attempted to create an access key for using the compromised access key ID. By searching AWS CloudTrail logs for attempts to create access keys, it helps trace adversarial actions within the compromised account.	accessKeyId: AKIAJOGCDXJ5NW5PXUPA accountId: 622676721278 arn: arn:aws:iam::622676721278:user/web_a principalId: AIDAJNUCQVD57VVGYEFTQ type: IAMUser userName: web_admin	The output indicates that the adversary attempted to create a key for a resource called "web_admin." This suggests that the adversary sought access to manage or modify the web administrator account.
21	index="botsv3" sourcetype="aws:cloudtrail" userIdentity.accessKeyId="AKIAJOGCDXJ5NW5PXUPA"	The goal of this query was to track down the full user agent string associated with an unauthorized attempt to describe an AWS account. The query focused on filtering CloudTrail logs for the specific access key ID and relevant events.	responseElements: null sourceIPAddress: 82.102.18.111 userAgent: ElasticWolf/5.1.6 userIdentity: { [+]	The output revealed that the application used in this unauthorized attempt was "ElasticWolf/5.1.6," a popular AWS management tool. This information helps trace the adversary's activities back to the software used in their operations.
22	index=botsv3 (AKIAJOGCDXJ5NW5PXUPA OR web_admin) sourcetype="aws:cloudtrail" eventName="RunInstances"	This query was used to identify which operating system version (Ubuntu) the adversary attempted to launch in their first attempt. The query focused on AWS CloudTrail logs with the specific event name "RunInstances."	requestParameters.instancesSet.items{}.imageId 15 Values, 100% of events ami-5d055232 ami-1157157d ami-1ee65166 ami-2581aa40	The output identifies that the operating system launched by the adversary was "Ubuntu 16.04 Xenial Xerus." This is the codename for the first OS version used in the attacker's instance launch attempt.
23	index=botsv3 source="lambda" brewertalk.com	This query aimed to determine the average length of distinct third-level subdomains involved in DNS queries to "brewertalk.com." The query aggregated data from the "lambda	8.1	The output shows that the average length of distinct third-level subdomains in queries to "brewertalk.com" was 8.1 characters. This statistic provides insight into the complexity of the DNS queries involved.

		" source, focusing on subdomain length.		
24	index=botsv3 source="stream "	Using the payload data from the memcached attack, the objective is to identify the name of the .jpeg file used by the Taedonggang group to deface brewery websites. The query leverages UDP stream data and searches for specific patterns or strings in the payload, such as usernames or other indicative data. Through reverse investigation and web searches, the .jpeg file "/images/index1.jpeg" is identified as being used in the defacement.	"dest_content": "$VALUE injected 0 50000 6HOUL@G3RpwnzFrothyl4Life6HOUL@G3RpwnzFrothyl4L", "dest_ip": 1, "endtime": 2018-08-20T11:17:16.0, "site": "www.lilyandhops.com", "timestamp": 2018-08-20T11:17:16.043179, "uri_path": "/images/index1.jpeg" set injected 0 3600 105 CRYP70KOL5CH-OWNS-YOUCRYP70KOL setinjected03600105 CRYP70KOL5CH-OWNS-YOUCRYP70KOL getinjected	Identifies the `.jpeg` file name used by Taedonggang for defacing brewery websites by analyzing the content from memcached attack data. This information reveals how the attackers used a specific image file for their defacement campaign.
25	index=botsv3 sourcetype="ms:o365 " Operation=FileUploaded"	The goal is to discover the user-agent string responsible for uploading a malicious link file to OneDrive. Initially, the query filters events from OneDrive logs. Upon filtering out duplicates and focusing on specific OneDrive file upload operations, it is revealed that the upload was made by a user with a North Korean browser, NaenaraBrowser/3.5b4. This helps link the suspicious activity to a potential source.	"SourceFileExtension": lnk, "SourceFileName": BRUCE BIRTHDAY HAPPY HOUR PICS.lnk, "SourceRelativeUrl": Documents/Birthday Pictures, "UserAgent": Mozilla/5.0 (X11; U; Linux i686; ko-KP;, "UserId": bgist@froth.ly, "UserKey": i:0h.f|membership|10033fffa361a98c@live.c Wikipedia https://en.wikipedia.org/wiki/Naenara_(browser) Naenara (browser) - Wikipedia Naenara is **a North Korean intranet web browser software** develo **Computer Center** for use of the **national Kwangmyong intranet.** It version of Mozilla Firefox and is distributed with the Linux-based Red Star OS that North Korea developed due to licensing and ... Se	Provides the full user-agent string for the upload action of a malicious link file to OneDrive. This helps in identifying the software or browser used by the attacker for file uploads.

26	Index=botsv3 sourcetype="ms: aad " expired	to find the external client IP address that successfully logs into Frothly using an expired account. By filtering login attempts with the keyword "expired," and further narrowing the results based on specific user events,		Reveals the external client IP address that successfully logged into Frothly using an expired user account. This information highlights potential unauthorized access or misuse of expired credentials. the investigation uncovers that an IP address from Canada (199.66.91.253) successfully logged into the system under an expired account.

27	index=botsv3 macro*	the malware discovery date related to a macro-enabled file. It starts by finding macro-related events and then decodes the associated malware message.		The search eventually leads to the identification of the malware name as W97M.Empstage, and using external resources like Symantec's site, the malware's discovery date is found to be 2016/11/11.
28	index="botsv3" source="/var/log/auth.log" (adduser OR useradd)	This tracks the creation of a new user on a Linux system by the root account. By searching for user creation commands (`adduser` or `useradd`), the investigation leads to the discovery of the user account "tomcat" and eventually reveals the associated password after filtering through system logs.		Finds the password associated with the user account created by the "root" user on the on-premises Linux system. This helps in understanding if any credentials were exposed or misused during the account creation process. Reveals the external client IP address that successfully logged into Frothly using an expired user account. This information highlights potential unauthorized access or misuse of expired credentials.

29	index="botsv3" EventCode=4720	The goal is to identify the name of the user created after an endpoint was compromised. By searching for event code 4720, which logs new user creation, the account "svcvnc" was found to have been created on the compromised endpoint.	New Account: Security ID: FYODOR-L\svcvnc Account Name: svcvnc Account Domain: FYODOR-L	Identifies the user account created after the endpoint was compromised. This shows which new user accounts were set up as part of the post-compromise activity.
30	index="botsv3" dest_port=1337	This query aims to find the process ID (PID) of a process listening on port 1337 (leet port). By filtering events based on this destination port, the query reveals the process ID (PID: 14356) associated with port 1337.	dest_port 1337 dvc_id 254926 fd 3u ip_version 4 pid 14356 transport TCP	Finds the process ID (PID) of the process that is listening on port 1337, commonly referred to as a "leet" port. This information can be used to investigate what process is running on this port and its potential role in the attack.
31	sourcetype="ms:o365 " Workload="Exchange" *query*	The query seeks to identify a suspicious search string originating from an external IP address linked to Frothly's mail server. By filtering Microsoft Office 365 Exchange logs and looking for search queries, the string "cromdale OR beer OR financial OR secret" was identified as being suspicious.	SearchQuery cromdale OR beer OR financial OR secret	Extracts the search strings used from an external IP address associated with Frothly's mail server. This provides insight into what terms or keywords were queried during the attack, potentially revealing the attacker's intent.

32	index="botsv3" host="FYODOR-L" source="WinEventLog /Operational" EventCode=1	The goal is to find the MD5 value of a file downloaded to Fyodor's endpoint system, which was used to scan Frothly's network. By searching the event logs and filtering for specific files in the temp directory, the query leads to the discovery of an executable file `hdoor.exe`, with the MD5 hash `586EF56F4D8963DD546163AC31C865D7`.	**Values** C:\Windows\Temp\unziped\lsof-master\iexeplorer.exe C:\Windows\Temp\hdoor.exe id'>{EBF7A186-8503-5B57-0000-0020981C >MD5=586EF56F4D8963DD546163AC31C865D7 1}</Data><Data Name='ParentProcessId'>	Retrieves the MD5 hash of the file downloaded to Fyodor's endpoint system, used to scan Frothly's network. This allows for identifying and tracking the specific file involved in the
33	index=botsv3 EventCode=4732	Based on prior findings, this query determines the groups assigned to the user "svcvnc" after the endpoint was compromised. By searching for event code 4732, which logs changes to group memberships, the user is found to have been added to the "Administrators" and "Users" groups.	Group: Security ID: BUILTIN\Administrators Group Name: Administrators Group Domain: Builtin Group: Security ID: BUILTIN\Users Group Name: Users Group Domain: Builtin	Lists the groups that the user `svcvnc` was added to after the endpoint compromise. This indicates the permissions and roles assigned to the compromised account, which can help in understanding the scope of the attacker's access.
34	index=botsv3 sourcetype="ms:aad:audit" Operation=AccountDisabled	At some point during the attack, a user's domain account is disabled. The goal is to determine the email addresses of both the user whose account was disabled and the one who disabled it.	actor: { [-] userPrincipalName: fyodor@froth.ly targets: [[-] targetResourceType: User userPrincipalName: bgist@froth.ly	Fyodor, using elevated privileges, disabled the account of bgist@froth.ly. The logs show multiple successful events tied to this action, suggesting that Fyodor's account was likely compromised or the attacker was using their credentials to perform malicious actions

35	index=botsv3 sourcetype="stream:smtp" attach_filename	Another phishing email was sent to Frothly employees after the adversary had gained access to the network. This query attempts to identify the malicious file left as an artifact by the phishing attempt.	From: Peat Cerf Sent: Wednesday, July 25, 2018 6:51 PM To: Billy Tun <btun@froth.ly> Subject: meeting with F **Base64*** /9j/4AAQSkZJRgABAgIATgBOAAD/4hxtSUNDX1BST0ZJTEUAAQEAABxdTGlubwIQAABtbnRyUkdC IFhZWiAHzgACAAkABgAxAABhY3NwTVNGVAAAAABJRUMgc1JHQgAAAAAAAAAAAAAAAAA9tYAAQAA AADTLUhQICAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABFj cHJ0AAABUAAAADNkZXNjAAABgwAAAGx3dHB0AAAB7wAAABRia3B0AAACAwAAABRyWFlaAAACFwAA ABRnWFlaAAACKwAAABRiWFlaAAACPwAAABRkbW5kAAACUwAAAHBkbWRkAAACwwAAAIh2dWVkAAAD SwAAAIZ2aWV3AAAD0QAAACRsdW1pAAAD9QAAABRtZWFzAAAECQAAACR0ZWNoAAAELQAAAAxyVFJD Decode Base64 to Image **Preview Image** | **Toggle Background Color**  Action: All attachments have been removed. Frothly-Brewery-Financial-Planning-FY2019-Draft.	A macro-enabled spreadsheet file `Brewery-Financial-Planning-FY2019-Draft.xlsm` was found as an attachment in a phishing email sent to multiple employees. The spreadsheet contains malicious macros designed to download further malware onto the victim's machine. This file was identified after a thorough search of all SMTP attachments.

36	index=botsv3 sourcetype="WinEventLog" SourceName="Symantec AntiVirus"	search "Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm"` Based on the XLSM file discovered , this query seeks to uncover the embedded executable within the malicious document.	Security Risk Found! W97M.Empstage in Fil l-Planning-FY2019-Draft[66].xlsm by: Auto 5B58 0000 0010CC95 42(3bbwe\HxTsr.exe</Data inancial-Planning-FY2	The executable `HxTsr.exe`, embedded within the malicious XLSM file, was detected by Symantec AntiVirus. This executable is associated with Windows Mail and Calendar, but in this case, it was likely used to gain a foothold within the system by exploiting vulnerabilities in the application.
37	index=botsv3 BRUCE BIRTHDAY HAPPY HOUR PICS.lnk Operation=AnonymousLinkUsed	The adversary used a link file to lure users into executing malicious code. This query attempts to count how many unique IP addresses clicked on the malicious link file.	ClientIP 7 Values, 100% of events Reports Top values Top values by time Events with this field Values Count 107.77.212.175 10 104.238.59.42 2 107.77.213.96 2 157.97.121.5 2 174.215.1.81 2 64.64.117.111 2 91.207.175.56 2	A total of seven unique IP addresses accessed the malicious `.lnk` file titled `BRUCE BIRTHDAY HAPPY HOUR PICS.lnk`. This indicates that multiple users or machines within the Frothly network interacted with the file, potentially leading to further malware dissemination.

38	index=botsv3 sourcetype="stream " rare dest_port	This query seeks to determine which port was used by the adversary to download attack tools onto the compromised system.	dest_port 3333 50504 22790 40552 me='Image'>C:\W n v1.0\powershell.exe</Data> Data Name='SourceIp'>192.168	After filtering through rare destination ports, it was identified that the adversary utilized port 3333 to transfer their attack tools. The use of this port, likely unmonitored or rarely used, helped the attacker avoid detection during the download process.
39	`index=botsv3 */tmp/* sourcetype="XmlWinEventLog /Operational" dedup ParentCommandLine	Two files were remotely streamed to the `/tmp` directory of an on-premises Linux server. The query attempts to identify the names of these files.	Values /images/logos.png tion "cat /tmp/colonel.c"	These two files, streamed remotely by the adversary, are highly suspicious. The `/tmp/definitelydontinvestigatethisfile.sh` script suggests an attempt to obfuscate the malicious activity. The `/tmp/colonel` file could potentially be a backdoor or a tool to escalate privileges. Both files pose a significant risk to the server's security.

40	sourcetype="stream" rare dest_port`	Based on information from Q40, this query infers the file that contains the attack tools used by the adversary.	**Values** /images/logos.png	The file `logos.png`, while appearing to be an image file, likely concealed the adversary's attack tools. Image files can be used as a form of steganography, where malicious code is embedded within seemingly harmless files to evade detection.
41	`index=botsv3 sourcetype="WinEventLog /Operational"  "hdoor.exe"`	This query seeks to find the first executable that was uploaded to the domain admin account's compromised endpoint system.	C:\Windows\Temp\hdoor.exe ll\v1.0\powershell.exe	The first executable uploaded was `hdoor.exe`, which is a known backdoor malware. After the file was uploaded, it was executed through PowerShell, allowing the adversary to maintain persistent access to the compromised system and enabling further exploitation of the network.

Table 1: Running Sheet

5.0 TIMELINE

Date	Time	Event
2018-08-20	09:16:12	AKIAJOGCDXJ5NW5PXUPA/web_admin initiates access to IAM resources.
2018-08-20	09:16:12	AKIAJOGCDXJ5NW5PXUPA/web_admin attempts to create nullweb_admin.
2018-08-20	09:16:22	AKIAJOGCDXJ5NW5PXUPA/web_admin launches a Xenial Xerus instance.
2018-08-20	09:27:07	AKIAJOGCDXJ5NW5PXUPA/web_admin finishes accessing IAM resources.
2018-08-20	09:55:14	Malicious attachment Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm is detected.
2018-08-20	09:55:52	HxTsr.exe from the malicious attachment is flagged by Sysmon.
2018-08-20	09:56:39	Symantec identifies HxTsr.exe from the same attachment.
2018-08-20	09:57:33	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk uploaded to OneDrive.
2018-08-20	09:59:04	First use of BRUCE BIRTHDAY HAPPY HOUR PICS.lnk.
2018-08-20	10:01:44	Initial contact with C2 server
2018-08-20	10:08:17	svcvnc Windows account created and added to Administrators and Users groups.
2018-08-20	10:11:02	Reconnection to C2 server
2018-08-20	10:43:10	hdoor.exe initiates a network scan
2018-08-20	11:05:40	First remote code execution using iexplore.exe (CVE-2017-9791)
2018-08-20	11:08:48	Streaming of definitelydontinvestigatethisfile.sh via iexplore.exe

2018-08-20	11:24:28	Kevin Lagerfield's Azure AD account activated.
2018-08-20	11:28:30	Last use of BRUCE BIRTHDAY HAPPY HOUR PICS.lnk.
2018-08-20	11:31:54	netcat starts listening on port 1337
2018-08-20	11:34:49	tomcat8 runs ./colonelnew for privilege escalation (CVE-2017-16995)
2018-08-20	11:41:36	Kevin Lagerfield's Azure AD account password reset
2018-08-20	11:48:38	root user clears history with rm /usr/share/tomcat8/.bash_history.
2018-08-20	13:01:46	frothlywebcode S3 bucket is made public
2018-08-20	13:02:44	OPEN_BUCKET_PLEASE_FIX.txt uploaded to frothlywebcode
2018-08-20	13:33:24	gacrux.i-0cc93bade2b3cba63 autoscaled.
2018-08-20	13:37:33	BSTOLL-L initiates a Coinhive DNS lookup**,** signaling the start of cryptocurrency mining**.**
2018-08-20	13:37:40	First detection of BTUN-L JSCoinMiner, used for unauthorized cryptocurrency mining on the compromised machines.
2018-08-20	13:37:50	BSTOLL-L **starts** Chrome Monero mining
2018-08-20	13:46:47	Last detection of BTUN-L JSCoinMiner.
2018-08-20	13:57:54	frothlywebcode S3 bucket is made private again
2018-08-20	14:47:12	bgist@froth.ly Azure AD account disabled by fyodor@froth.ly
2018-08-20	15:07:22	Brute-force attacks against web servers from 5.101.40.81 start.
2018-08-20	15:08:12	Brute-force attacks from 5.101.40.81 conclude.
2018-08-20	15:15:00	An email bragging about the exfiltration of customer data is sent.

Table 2:TimeLine

6.0 References

Amazon. (2024). *PutBucketAcl - Amazon Simple Storage Service*. Amazon.com. https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketAcl.html#:~:text=Sets%20the%20permissions%20on%20an%20existing%20bucket%20using

Attack Signature Detail Page. (n.d.). Www.broadcom.com. https://www.broadcom.com/support/security-center/attacksignatures/detail?asid=30358

AWS. (2024). *What Is AWS CloudTrail? - AWS CloudTrail*. Docs.aws.amazon.com. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

CyberDefenders: Blue team CTF Challenges | Boss Of The SOC v3. (2023, June 6). Web.archive.org. https://web.archive.org/web/20230606083826/https://cyberdefenders.org/blueteam-ctf-challenges/8#nav-questions

Dr. Nadine Shillingford. (2023). *Data Analytics Using Splunk 9.x*. Packt Publishing Ltd.

MITRE. (2024). *MITRE ATT&CK™*. Mitre.org. https://attack.mitre.org/

O365 Advanced Threat Protection. (n.d.). Www.law.upenn.edu. https://www.law.upenn.edu/its/docs/office/office-365-ATP.php

Safe Links & Safe Attachments Information. (2023, February 3). Information Technology Services. https://its.gmu.edu/knowledge-base/safe-links-safe-attachments-information/

Van, K. R., & Forno, R. (2001). *Incident response : [planning & management]*. O'reilly.

Wang, Y., Zhang, T., & Ye, Q. (2021). *Situation awareness framework for industrial control system based on cyber kill chain*. EDP Sciences.