Mural by Edoardo Kobra in Minneapolis, Minnesota

Threat Hunting in the Microsoft Cloud

John Stoner

@stonerpsu

May 2020

whoami > John Stoner

GCIA, GCIH, GCTI

Principal Security Strategist

@stonerpsu

20+ years of cyber security experience

Blogger on Hunting and SecOps

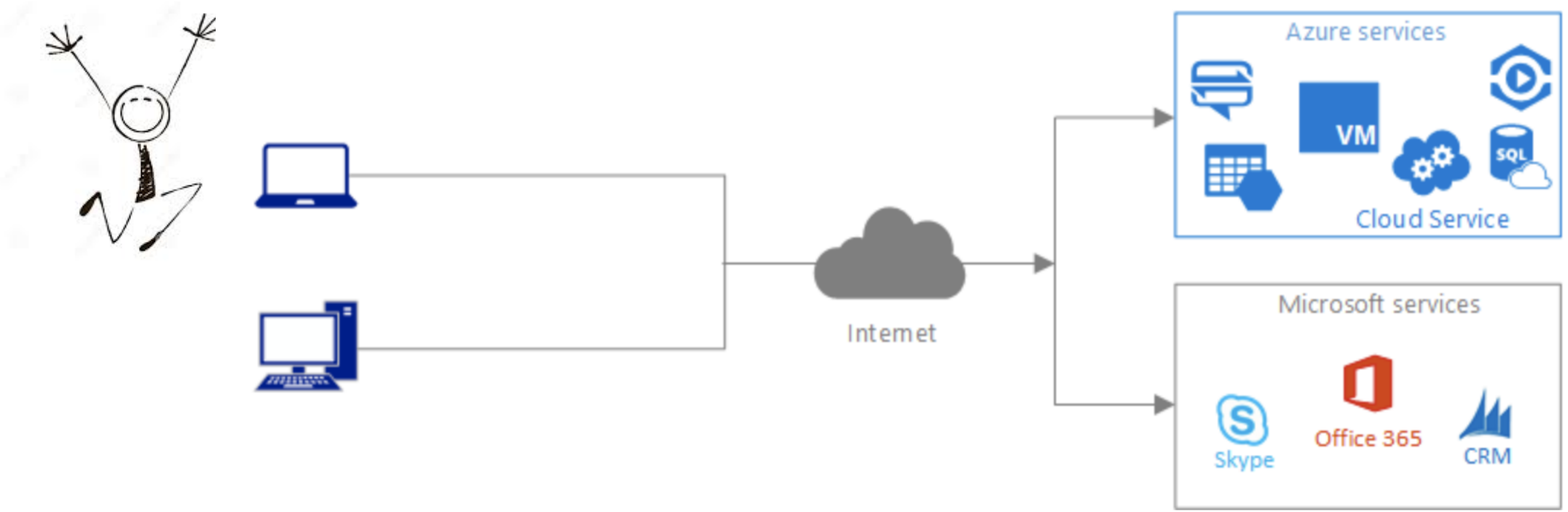
Built a fun little investigator/hunting app

Loves The Smiths and all 80’s sadtimey music

In the next 30 minutes…

- Implications of moving to the cloud using Microsoft's cloud services, Azure Active Directory and Office 365 and the Attack surface
- Compare was is available in the cloud compared to on-premise and how the logging changes
- Perform an abbreviated hunt in Azure AD and Office 365 to observe the fidelity of the events that a hunter would have access to
- Illustrate why cloud logging needs to be supplemented with on-premise logs
- Map to MITRE ATT&CK's cloud matrix

A **Very** High-Level View of Microsoft Cloud Services



Microsoft Cloud is a high value target

Phishing

"attackers have started to spoof the new Azure AD sign-in page in multiple phishing campaigns. We have so far seen several dozens of phishing sites used in these campaigns"
- Microsoft Security Intelligence ***2020***

Password Spray

"80% of those compromised enterprise accounts,… almost 1 million hacked accounts in January alone, were hit by either "password spray" or "replay" attacks."
- *Forbes,* ***March 2020***

Malware

"As Office 365 OAuth apps can give attackers complete access to an Office 365 account, they can be used for a variety of attacks."
- *bleepingcomputer.com,* ***Dec 2019***

Once in, they are in

Office 365 and Azure security is great unless adversary gets legitimate credentials

Logging can be challenging

Microsoft's cloud logging can be difficult to configure and it has some interesting event time to index time issues

Adversaries are targeting it, but we aren't looking

It's another place to hunt, with new detections to build

Password Spraying

Alert (TA18-086A)

Brute Force Attacks Conducted by Cyber Actors

Original release date: March 27, 2018 | Last revised: May 06, 2020

ACSC Releases Advisory on Password Spraying Attacks

Original release date: August 08, 2019

Print Tweet Send Share

The Australian Cyber Security Centre (ACSC) has released an advisory on password spraying attacks. Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

The ACSC provides recommendations for organizations to detect and mitigate these types of attacks against their external services, such as webmail, remote desktop access, or cloud-based services.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the ACSC advisory on password spraying attacks and the following CISA tips:

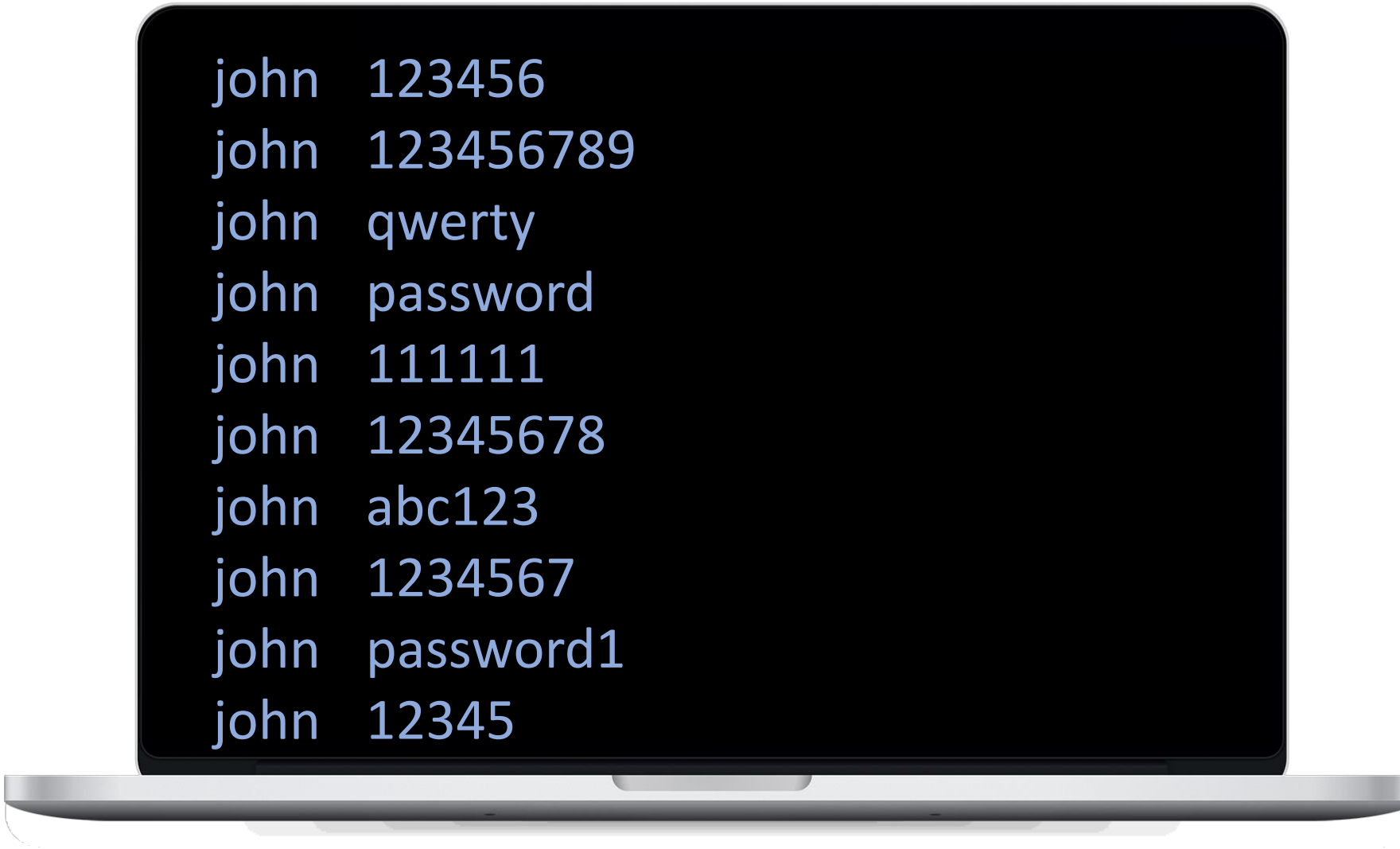
- Choosing and Protecting Passwords
- Supplementing Passwords

Brute Force Password Attack

Keep hitting the same user account with a dictionary of passwords and permutations until you get a hit

Thresholds in the authentication system trigger lock outs

SIEMs have rules to detect this



Password Spray Attack

Roll across users with the same password

Avoids the authentication lock out issue

SIEMs don't have a great way to monitor for this out of the box

Good password policies are key to foiling this

Also MFA

ON-PREMISES INFRASTRUCTURE MAPPED TO MS Cloud

TECHNOLOGY	ON-PREMISES SOLUTION	MS Cloud
Archiving	Tape library, off site tape storage	Azure Backup, Azure Storage archive access tier
Caching	Memcached, Redis	Azure Redis Cache
Computer	Hardware, virtualization	Azure Virtual Machines
Containers	Docker, Kubernetes	Azure Container Instances, Azure Container Registry, Azure Kubernetes Service (AKS), Service Fabric Mesh
Content delivery	CDN solutions	Azure Content Delivery Network
Data centers	Data centers	Availability Zones
Data warehousing	Specialized hardware and software solutions	SQL Data Warehouse
Databases	MS SQL, MySQL, Oracle, PostgreSQL	SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Cosmos DB
Deployment	Ansible, Chef, Fabric, Puppet, SaltStack	Azure Resource Manager, VM extensions, Azure Automation, App Service, Azure Automation
Disaster recovery	Multi-site data centers	Azure Regions
Domain name services	DNS providers	Azure DNS, Traffic Manager
Email	Email software	Office365
Identity management	LDAP	Azure Active Directory Domain Services, Azure Active Directory
Load balancing	Hardware and software load balancers, HA Proxy	Load Balancer, Application Gateway
Management and monitoring	Performance and user monitoring solutions	Azure Monitor, Azure Event Hubs, Azure Stream Analytics
Messaging and workflow	Messaging and workflow software	Azure Notification Hubs, Azure Queue Storage, Service Bus, Logic Apps
Network	MPLS, VPN	ExpressRoute, Virtual Network, Azure VPN Gateway
Scaling	Hardware and software clustering, Apache ZooKeeper	Virtual Machine Scale Sets
Security	Firewalls, NACLs, routing tables, disk encryption, SSL, IDS, IPS	Key Vault, Azure Storage Service Encryption, Application Gateway - Web Application Firewall, Azure Firewall, Security Center
Storage	DAS, NAS, SAN, SSD	Azure managed disks, Azure Blob storage, Azure Storage cool tier

Papa Murphy's
TAKE 'N' BAKE PIZZA

Words of Caution

Over time, clouds change shape

- The exact fields or detail may change over time at the discretion of the cloud provider
- When you set this up, you may find more data or less available to you
- Important to understand the differences compared to on-premise Windows logging

8/23/17
5:06:56.000 PM

```
08/23/2017 05:06:56 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4624
EventType=0
Type=Information
ComputerName=wrk-ghoppy.frothly.local
TaskCategory=Logon
OpCode=Info
RecordNumber=110202
Keywords=Audit Success
Message=An account was successfully logged on.

Subject:
        Security ID:            NT AUTHORITY\SYSTEM
        Account Name:           WRK-GHOPPY$
        Account Domain:         FROTHLY
        Logon ID:               0x3e7

Logon Type:                     2

New Logon:
        Security ID:            FROTHLY\grace.hoppy
        Account Name:           grace.hoppy
        Account Domain:         FROTHLY
        Logon ID:               0xe3fd33d
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x1424
        Process Name:           C:\Windows\System32\winlogon.exe

Network Information:
        Workstation Name:       WRK-GHOPPY
        Source Network Address: 127.0.0.1
        Source Port:            0
```

Windows Event Log

4624 Login Event

8/20/18
2:04:56.808 PM


```
{ [-]
  appDisplayName: Office 365 Exchange Online
  appId: 00000002-0000-0ff1-ce00-000000000000
  correlationId: 9274aa2e-8c47-482a-b05e-14a1c6b76fe1
  dataSource: 1
  deviceInformation: ;MacOs;Chrome 68.0.3440;
  failureReason: null
  geoCoordinates: { [-]
    latitude: 40.72092056274414
    longitude: -74.00888061523438
  }
  id: a769b749-dcda-4783-b677-b85870bf0600
  ipAddress: 45.62.48.155
  location: { [-]
    city: Brooklyn Heights
    country: US
    state: New York
  }
  loginStatus: Success
  mfaAuthDetail: null
  mfaAuthMethod: null
  mfaRequired: false
  mfaResult: null
  signinDateTime: 2018-08-20T14:04:56.8086391Z
  signinDateTimeInMillis: 1534773896808
  signinErrorCode: 0
  userDisplayName: Grace Hoppy
  userId: 7b04c898-c35b-4c54-af11-5605b3572ea9
  userPrincipalName: ghoppy@froth.ly
}
```


Azure AD Sign-In Event

Accessing O365 Exchange in MS Cloud

OneDrive - File Modification Event

Key Fields of Note

ClientIP: 40.80.216.53

Workload: OneDrive

CreationTime: 2018-08-20T11:00:59

ObjectId: https://frothly-my.sharepoint.com/personal/ghoppy_froth_ly/Documents/Frothly-Shared/Supplies/Yeast-Pitching-Calculator.xlsx

SourceFileName: Yeast-Pitching-Calculator.xlsx

Operation: FileModified

UserId: ghoppy@froth.ly

CreationTime: 2018-08-20T11:00:59
EventSource: SharePoint
ObjectId: https://frothly-my.sharepoint.com/personal/ghoppy_froth_ly/Documents/Frothly-Shared/Supplies/Yeast-Pitching-Calculator.xlsx
Operation: FileModified
RecordType: 6
Site: 83382237-dd56-471d-a1cd-7997dddb1242
SourceFileExtension: xl
SourceFileName: Yeast-P
SourceRelativeUrl: Documents/Frothly-Shared/Supplies
UserAgent: MSWAC
UserId: ghoppy@froth.ly
UserKey: i:0h.f|membership|10030000a3250230@live.com
UserType: 0
Version: 1
WebId: 46ca8820-8a7b-46eb-b077-7d9024e32b39

Message Trace in MS Cloud

8/20/18
2:56:48.000 PM

{ [-]
DateReceived: 2018-08-20T14:56:48Z
FromIP: 107.77.211.7
Index: 1
MessageId: <CY4PR17MB139862746258E05465DA027AAF2B0@CY4PR17MB1398.namprd17.prod.outlook.com>
MessageTraceId: 0c550647-5dc0-44d6-59a2-08d5f2c56584
Organization: frothly.onmicrosoft.com
Received: /Date(153
RecipientAddress: bs
SenderAddress: fyod
Size: 18202
Status: Delivered
Subject: RE: BG
ToIP: null
}

Show as raw text

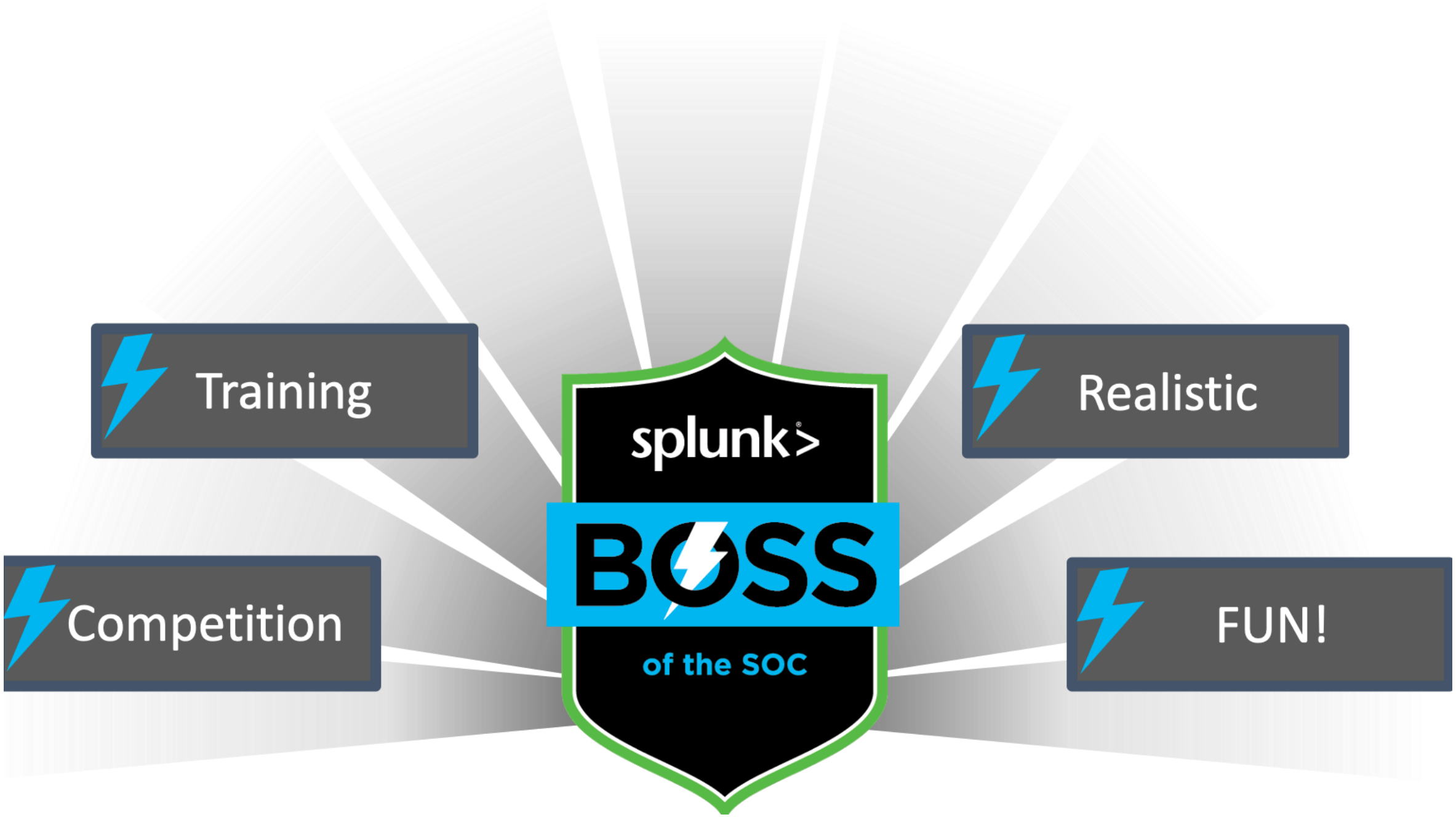
host = splunk.froth.ly | source = ms_o365_message_trace | sourcetype = ms:o365:reporting:messagetrace

Subject: RE: BG

RecipientAddress: bstoll@froth.ly

SenderAddress: fyodor@froth.ly

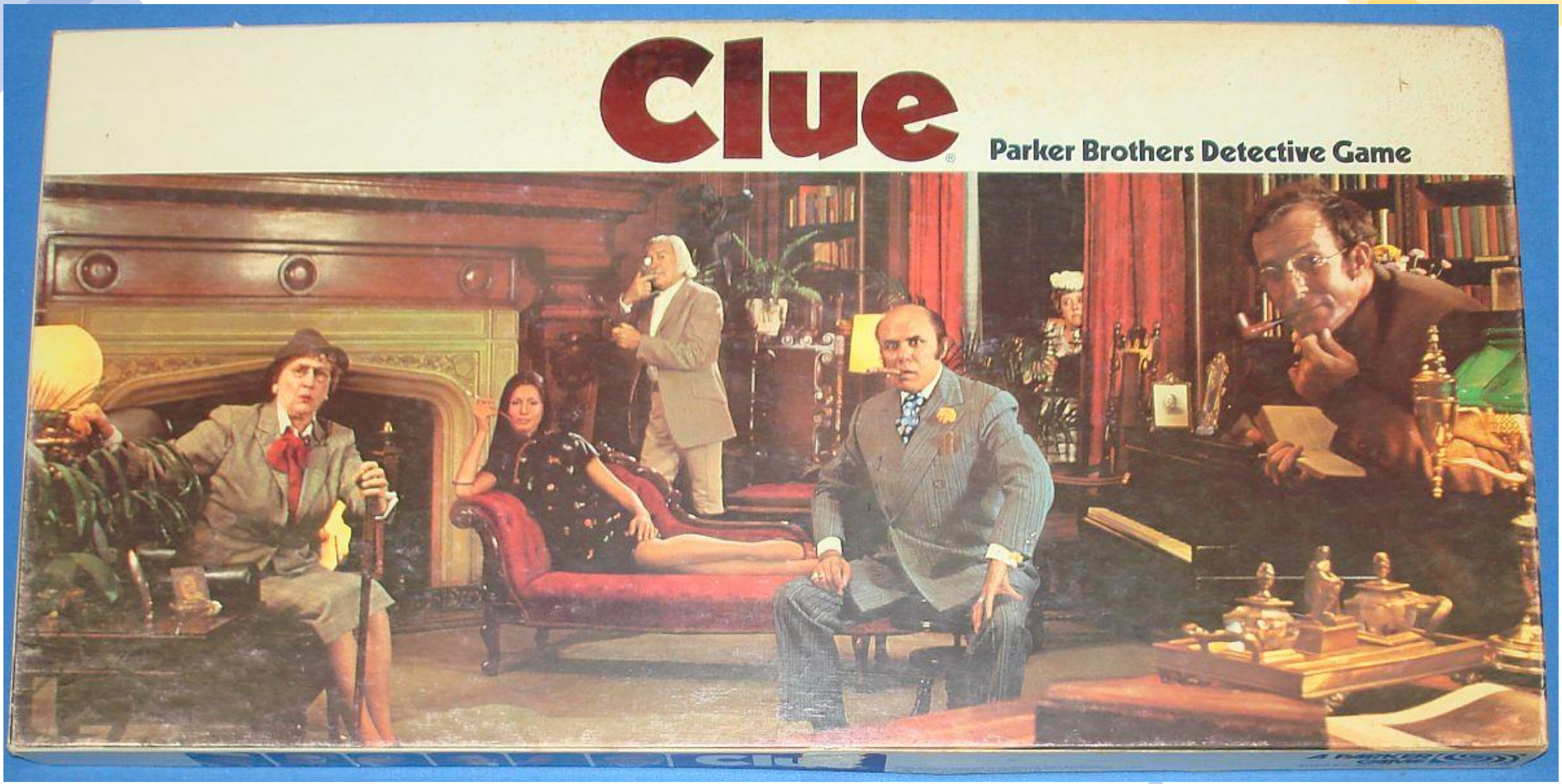
Size: 18202


Training
Realistic
splunk>
BOSS
of the SOC
Competition
FUN!

Good morning. ghoppy@froth.ly we hacked you again. I hope your beer is better than your

'Meeting to discuss project plan and hash out the details of implementation',NULL,NULL,0),
('c11f78ae-
b124-931b-4cd7-5b44265760aa','lily@brokenhands.com','','rlait@converseloverscom','',''Lo
for new craft beers',NULL,NULL,0),('c68c9a00-a56e-1ba3-
a46e-5b44265bc081','JohnnyStoner@stoutlover.com','','DavidHerrald@basements.com','','',
yeast that has the taste of candycorn',NULL,NULL,0),('cc0b352b-4708-b54f-
a891-5b4426f12d47','tomsmit@mainecabanaboys.com','','mattyv@scootersafety.com,'','','Ca
about new brewery in St. Louis'',NULL,NULL,0),('d1d8ea88-90bd-
ede3-7400-5b4426a1ce21','davidveuve@bellyandshouldershimmies.co.uk','','jimmybrodsky@fi
mortuaries.it','','','Very intersted in discussing floral notes of peat and dirt in sco
ale',NULL,NULL,0),('d767c134-0327-6f28-5a14-5b4426f95e21','

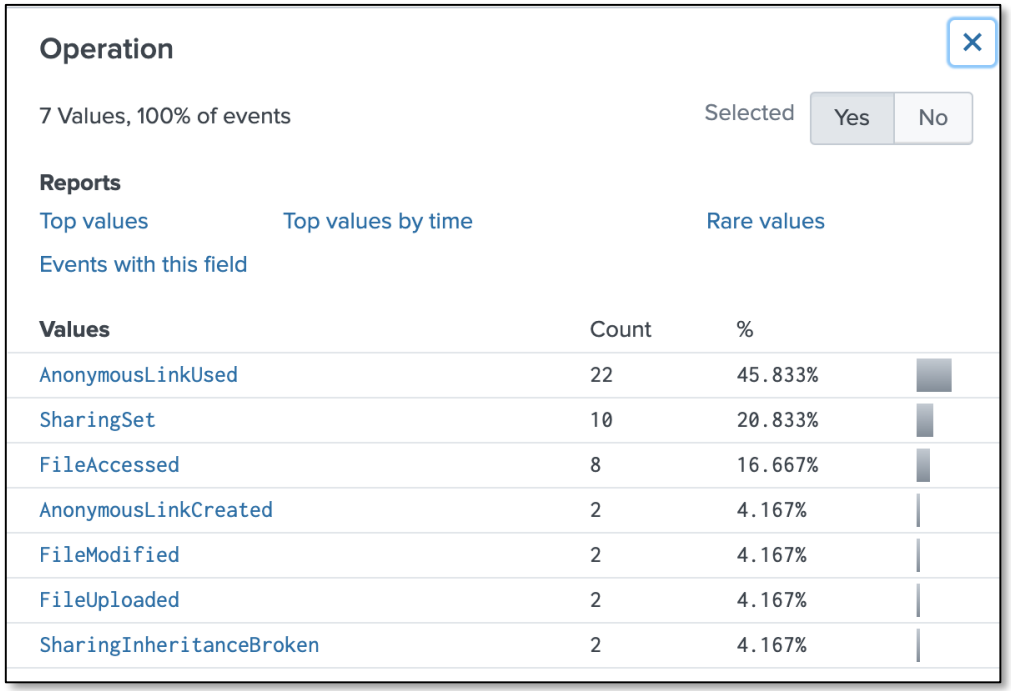
- Taedonggang


Clue®
Parker Brothers Detective Game

Initial intelligence around Taedonggang indicates that they may use link files to gain access to a targeted environment

.LNK Visibility?

- What is the name of the link file that was associated with anonymous clicks?
- Which users are associated with that link file?
- Who was the first named user to click the link?
- What workload is the anonymous file access associated with?



Values	Count	%
AnonymousLinkUsed	22	45.833%
SharingSet	10	20.833%
FileAccessed	8	16.667%
AnonymousLinkCreated	2	4.167%
FileModified	2	4.167%
FileUploaded	2	4.167%
SharingInheritanceBroken	2	4.167%

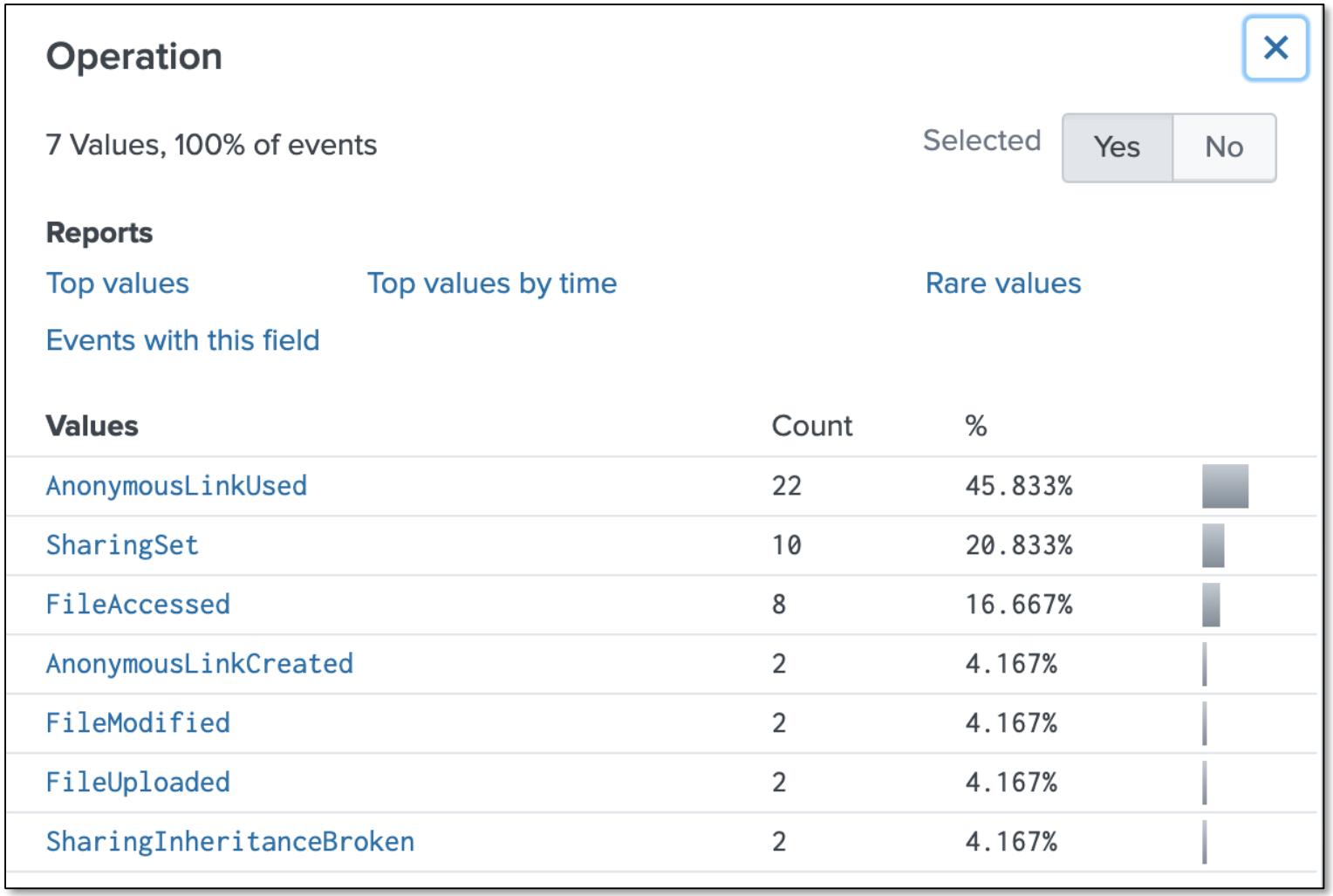
Suspicious Link File

- What was the first operation seen?

_time	SourceFileName	user	Workload
2018-08-20 11:28:30	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	bstoll@froth.ly	OneDrive
2018-08-20 10:01:13	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:28	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	bstoll@froth.ly	OneDrive
2018-08-20 10:01:07	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 10:00:39	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:04	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 10:00:35	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:10	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:18	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:05	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	anonymous	OneDrive
2018-08-20 09:59:41	BRUCE BIRTHDAY HAPPY HOUR PICS.lnk	bgist@froth.ly	OneDrive

firstTime	earliest(Operation)
Mon Aug 20 09:57:33 2018	FileUploaded

Anonymous Link Creation



Anonymous Link Creation

8/20/18
9:58:02.000 AM

{ [-]
  ClientIP: 104.207.83.63
  CorrelationId: 324e7e9e-20d5-6000-32f0-2f072f7259d4
  CreationTime: 2018-08-20T09:58:02
  EventData: <Type>Edit</Type>
  EventSource: SharePoint
  Id: 04651ac9-e87f-4f8e-9226-08d5f25cea7e
  ItemType: File
  ListId: 67091393-e290-421e-ac6a-2734e2b12a94
  ListItemUniqueId: 0aa10299-8655-4f7e-b293-965cc699f48a
  ObjectId: https://frothly-my.sharepoint.com/personal/bgist_froth_ly/Documents/Birthday Pictures/BRUCE BIRTHDAY HAPPY HOUR PICS.lnk
  Operation: AnonymousLinkCreated
  OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
  RecordType: 14
  Site: b6bb6c66-e23c-48a3-aca1-77763108cd9d
  SiteUrl: https://frothly-my.sharepoint.com/personal/bgist_froth_ly
  SourceFileExtension: lnk
  SourceFileName: BRUCE BIRTHDAY HAPPY HOUR PICS.lnk
  SourceRelativeUrl: Documents/Birthday Pictures/BRUCE BIRTHDAY HAPPY HOUR PICS.lnk
  UniqueSharingId: 95bee31f-0697-472f-8732-9a34d27f2932
  UserAgent: 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
  UserId: bgist@froth.ly
  UserKey: i:0h.f|membership|10033fffa361a98c@live.com
  UserType: 0
  Version: 1
  WebId: 7acb35b6-e1ec-44ed-9099-38580e330ed0
  Workload: OneDrive
}

Show as raw text

Tell Us More About Bruce…

8/20/18
9:51:09.676 AM


```
{ [-]
   appDisplayName: Microsoft Office 365 Portal
   appId: 00000006-0000-0ff1-ce00-000000000000
   correlationId: 72983ccf-4960-451e-962a-195b95b2a2b8
   dataSource: 1
   deviceInformation: ;;aBrowser 3.5;
   failureReason: null
   geoCoordinates: { [+]
   }
   id: 0cf13345-f991-473b-adc3-0ef107ca3800
   ipAddress: 104.207.83.63
   location: { [-]
     city: Hong Kong
     country: HK
     state: null
   }
   loginStatus: Success
   mfaAuthDetail: null
   mfaAuthMethod: null
   mfaRequired: false
   mfaResult: null
   signinDateTime: 2018-08-20T09:51:09.6763166Z
   signinDateTimeInMillis: 1534758669676
   signinErrorCode: 0
   userDisplayName: Bruce Gist
   userId: d85d399c-9cb6-480f-8789-88cbf56e3764
   userPrincipalName: bgist@froth.ly
}
```


Show as raw text

Different Users, Same IP

_time	appDisplayName	deviceInformation	ipAddress	location.city	location.country	loginStatus	userDisplayName
2018-08-20 09:51:09.676	Microsoft Office 365 Portal	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 09:51:15.371	O365 Suite UX	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 09:51:21.735	Office 365 Exchange Online	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 09:51:22.706	Office365 Shell WCSS-Client	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 09:51:50.004	Azure Portal	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 09:56:36.200	Office 365 SharePoint Online	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Bruce Gist
2018-08-20 10:40:46.934	Microsoft Office 365 Portal	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Fyodor Malteskesko
2018-08-20 10:40:52.330	O365 Suite UX	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Fyodor Malteskesko
2018-08-20 10:41:02.267	Office365 Shell WCSS-Client	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Fyodor Malteskesko
2018-08-20 10:41:05.048	Azure Portal	;;aBrowser 3.5;	104.207.83.63	Hong Kong	HK	Success	Fyodor Malteskesko

Azure Active Directory and Fyodor

_time	activity
2018-08-20 10:48:08.596	Set Company Information
2018-08-20 11:20:00.234	Set Company Information
2018-08-20 11:24:28.377	Update user
2018-08-20 11:24:28.486	Set user manager
2018-08-20 11:24:28.736	Update user
2018-08-20 11:25:15.525	Add member to role
2018-08-20 11:41:36.490	Reset user password
2018-08-20 11:42:51.051	Reset user password
2018-08-20 14:13:15.553	Set Company Information
2018-08-20 14:15:46.592	Update user
2018-08-20 14:15:46.592	Update StsRefreshTokenValidFrom Timestamp
2018-08-20 14:45:58.271	Set Company Information
2018-08-20 14:47:12.515	Update user
2018-08-20 14:47:12.515	Disable account
2018-08-20 14:47:12.632	Update StsRefreshTokenValidFrom Timestamp
2018-08-20 14:47:12.648	Update user
2018-08-20 14:55:35.381	Update StsRefreshTokenValidFrom Timestamp
2018-08-20 14:55:35.381	Update user

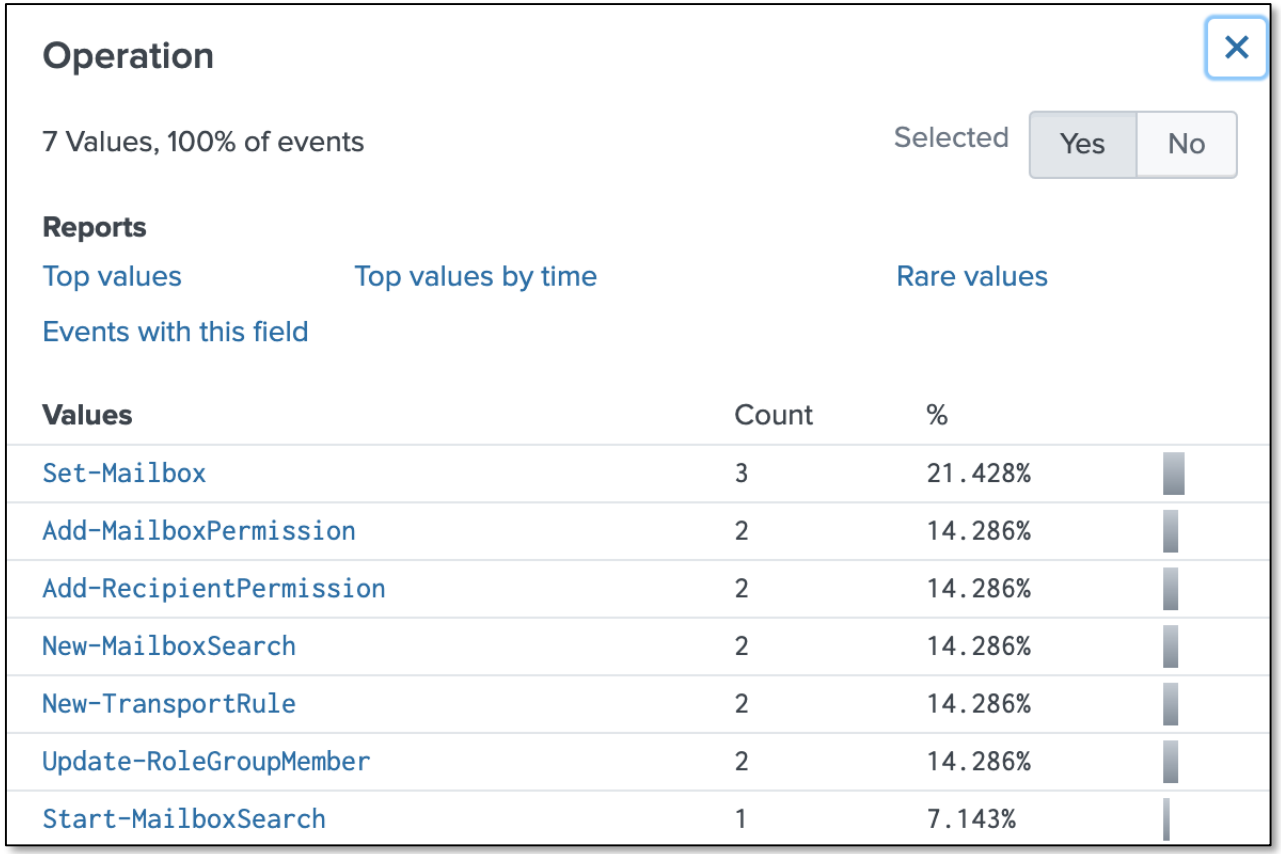
What Accounts Are Being Modified?

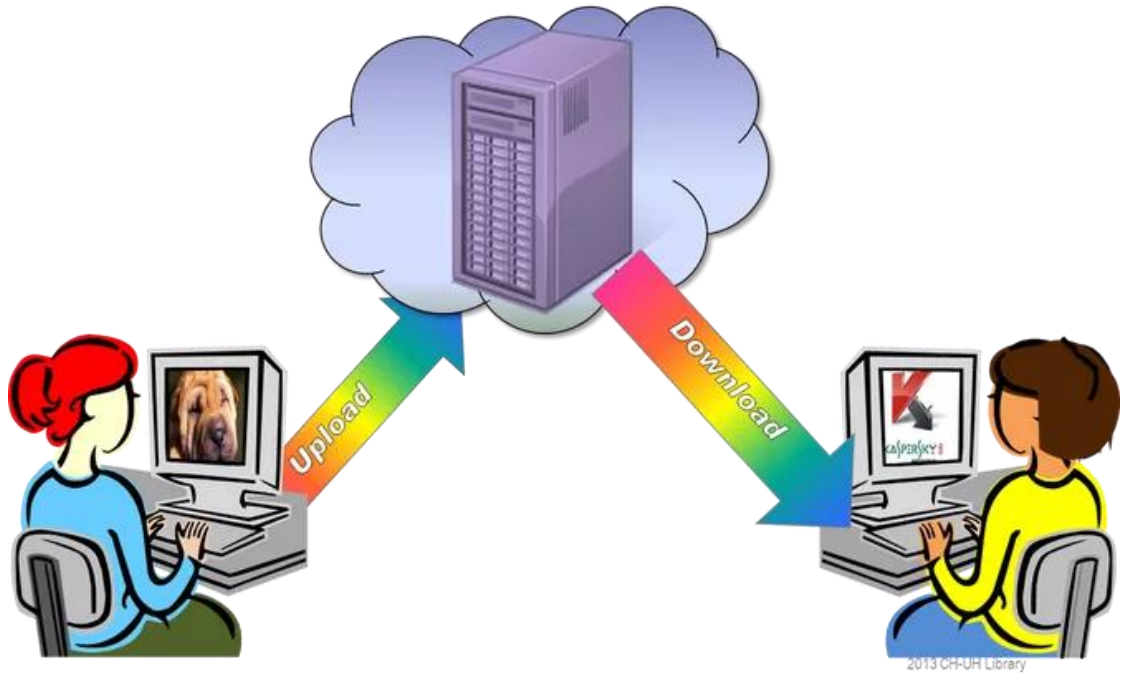
activity	targets{}.userPrincipalName
Update user	klagerfield@froth.ly
Set user manager	klagerfield@froth.ly
Update user	klagerfield@froth.ly
Add member to role	klagerfield@froth.ly
Reset user password	klagerfield@froth.ly
Reset user password	klagerfield@froth.ly
Update user	fyodor@froth.ly
Update StsRefreshTokenValidFrom Timestamp	fyodor@froth.ly
Update user	bgist@froth.ly
Disable account	bgist@froth.ly
Update StsRefreshTokenValidFrom Timestamp	bgist@froth.ly
Update user	bgist@froth.ly

activity	targets{}.modifiedProperties{}.name	targets{}.modifiedProperties{}.newValue
Update user	TargetId.UserType	"Member"
Set user manager	New Manager	"None"
Update user	AccountEnabled Included Updated Properties TargetId.UserType	[true] "AccountEnabled" "Member"
Add member to role	Role.ObjectID Role.DisplayName Role.TemplateId Role.WellKnownObjectName	"412cdb0f-49b2-4b49-82d3-3b35f37361a8" "Company Administrator" "62e90394-69f5-4237-9190-012177145e10" "TenantAdmins"

Properties Being Changed?

Exchange Visibility





_time	sourcetype	ClientIP	Operation	SourceFileName	ObjectId
2018-08-20 11:49:42	o365:management:activity	107.77.213.96	FileSyncUploadedFull	blargh.tgz	https://frothly-my.sharepoint.com/personal/fyodor_froth_ly/Documents/blargh.tgz
2018-08-20 11:55:22	o365:management:activity	199.66.91.253	FileDownloaded	archive.tar	https://frothly-my.sharepoint.com/personal/fyodor_froth_ly/Documents/archive.tar
2018-08-20 11:55:22	ms:o365:management	199.66.91.253	FileDownloaded	archive.tar	https://frothly-my.sharepoint.com/personal/fyodor_froth_ly/Documents/archive.tar

sourcetype

7 Values, 100% of events

Selected: Yes | No

Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
osquery:results	7	46.667%
o365:management:activity	2	13.333%
stream:http	2	13.333%
WinEventLog:Security	1	6.667%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	1	6.667%
access_combined	1	6.667%
ms:o365:management	1	6.667%

Things We Can't See

- Workstations Logs
- Servers not in Azure
- Network/Wire Data

What We Learned From Our Hunt

- Bruce Gist's account was compromised
  - Created an anonymous link that was used to gain additional access to Frothly
- Fyodor's account was compromised
  - Fyodor had elevated privileges
  - This account was used to enable a dormant user and assign elevated creds to maintain persistence
  - This account also modified Exchange permissions and rules to gain access to emails
- Files were moved around and out of Frothly

What Can We Operationalize?

Logins of different users from the same IP?

Tenant/Site Admin modifications?

Exchange Rule Creations?

File Upload/Download?

Tough by itself, perhaps with additional criteria based on behavior

ATT&CK for Microsoft Cloud Services

Azure, Azure Active Directory and Office365

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
4 items	6 items	1 items	6 items	6 items	9 items	3 items	5 items	1 items	1 items
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Spearphishing Link	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Trusted Relationship	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Valid Accounts	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

What Techniques Did We Observe the Adversary Using?

Azure, Azure Active Directory and Office365

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
4 items	6 items	1 items	6 items	6 items	9 items	3 items	5 items	1 items	1 items
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Spearphishing Link	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Trusted Relationship	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Valid Accounts	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

Summary

- Understand the difference between the logging MS Cloud provides compared to Microsoft logs on premise
- Much of it is easy to understand
  - BUT…it is cloaked in JSON
- Use who, what, where, when, why and how to form the basis of your hunt
- Schemas and fields may change over time

Data Set That Includes Cloud Data to Play With!!!

BOTS version 3

- https://www.splunk.com/en_us/blog/security/botsv3-dataset-released.html
- Dataset - https://github.com/splunk/security_datasets

Thank You

John Stoner | @stonerpsu