# It’s Just a Jump To The Left (of Boom)

## Prioritizing Detection Implementation With Intelligence and ATT&CK

# Introduction

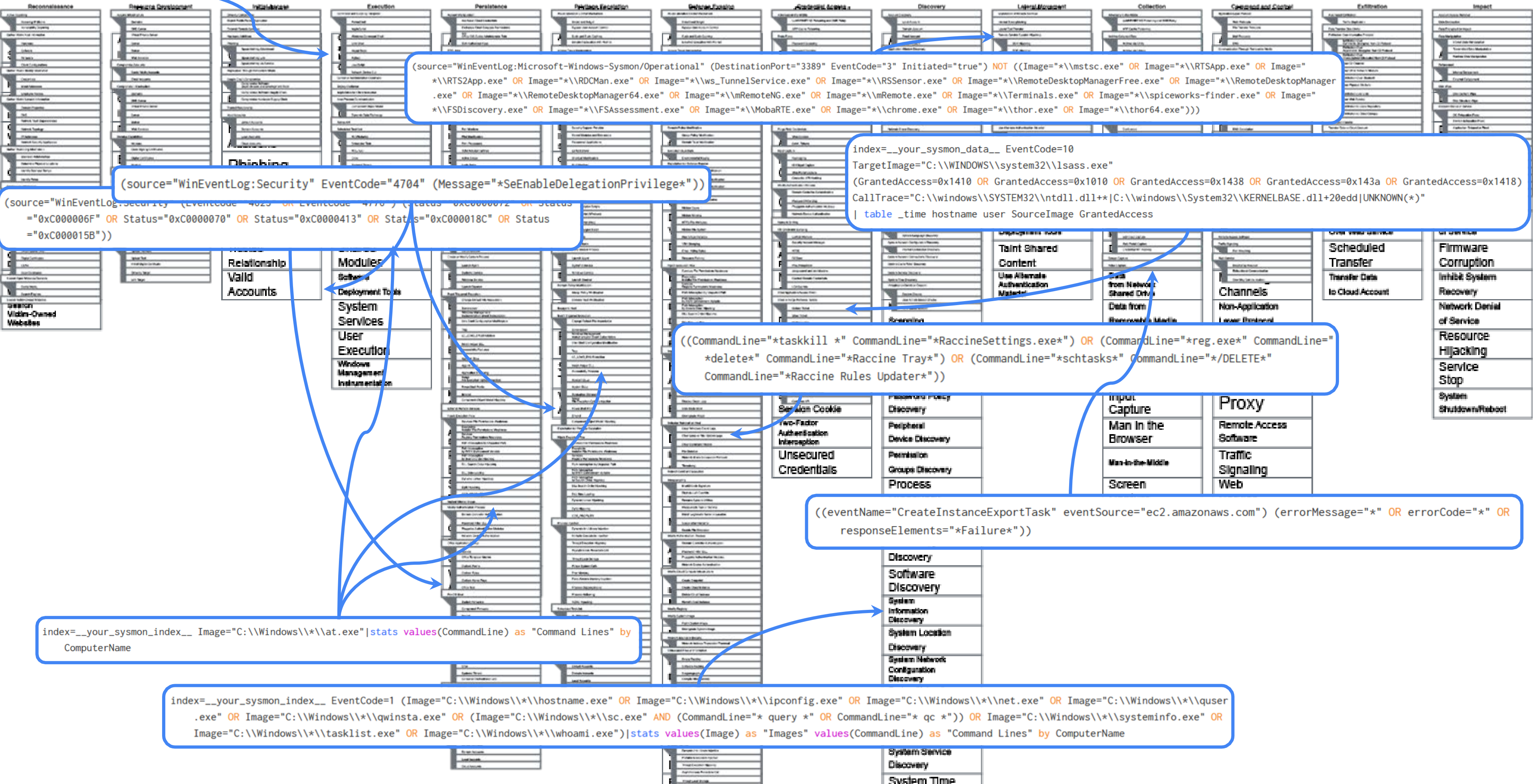
**Lindsay Kaye**
Senior Director, Operational Outcomes, Insikt Group
Recorded Future
@TheQueenofELF

**Scott Small**
Sr Analyst - Intelligence, Emulation, & Purple Team
Major U.S. retailer
@IntelScott

# Disclaimer

All content contained in this presentation is solely the view of the presenter, and does not represent the opinions, beliefs, experiences, policy, or operating agreements of any organizations the speaker currently works for or has worked for in the past.

untless implementations 9,000+ detection rules, 2,100+ tests



```
index=__your_sysmon_index__ EventCode=1 Image="C:\\Windows\\*\\powershell.exe" ParentImage!="C
   :\\Windows\\explorer.exe"|stats values(CommandLine) as "Command Lines" values(ParentImage) as "Parent
   Images" by ComputerName
```

```
(source="WinEventLog:Microsoft-Windows-Sysmon/Operational" (DestinationPort="3389" EventCode="3" Initiated="true") NOT ((Image="*\\mstsc.exe" OR Image="*\\RTSApp.exe" OR Image="
   *\\RTS2App.exe" OR Image="*\\RDCMan.exe" OR Image="*\\ws_TunnelService.exe" OR Image="*\\RSSensor.exe" OR Image="*\\RemoteDesktopManagerFree.exe" OR Image="*\\RemoteDesktopManager
   .exe" OR Image="*\\RemoteDesktopManager64.exe" OR Image="*\\mRemoteNG.exe" OR Image="*\\mRemote.exe" OR Image="*\\Terminals.exe" OR Image="*\\spiceworks-finder.exe" OR Image="
   *\\FSDiscovery.exe" OR Image="*\\FSAssessment.exe" OR Image="*\\MobaRTE.exe" OR Image="*\\chrome.exe" OR Image="*\\thor.exe" OR Image="*\\thor64.exe")))
```

```
index=__your_sysmon_data__ EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
| table _time hostname user SourceImage GrantedAccess
```

```
(source="WinEventLog:Security" EventCode="4704" (Message="*SeEnableDelegationPrivilege*"))
```

```
(source="WinEventLog:Security" (EventCode="4625" OR EventCode="4776") (Status="0xC0000072" OR Status
   ="0xC000006F" OR Status="0xC0000070" OR Status="0xC0000413" OR Status="0xC000018C" OR Status
   ="0xC000015B"))
```

```
((CommandLine="*taskkill *" CommandLine="*RaccineSettings.exe*") OR (CommandLine="*reg.exe*" CommandLine="
   *delete*" CommandLine="*Raccine Tray*") OR (CommandLine="*schtasks*" CommandLine="*/DELETE*"
   CommandLine="*Raccine Rules Updater*"))
```

```
((eventName="CreateInstanceExportTask" eventSource="ec2.amazonaws.com") (errorMessage="*" OR errorCode="*" OR
   responseElements="*Failure*"))
```

```
index=__your_sysmon_index__ Image="C:\\Windows\\*\\at.exe"|stats values(CommandLine) as "Command Lines" by
   ComputerName
```

```
index=__your_sysmon_index__ EventCode=1 (Image="C:\\Windows\\*\\hostname.exe" OR Image="C:\\Windows\\*\\ipconfig.exe" OR Image="C:\\Windows\\*\\net.exe" OR Image="C:\\Windows\\*\\quser
   .exe" OR Image="C:\\Windows\\*\\qwinsta.exe" OR (Image="C:\\Windows\\*\\sc.exe" AND (CommandLine="* query *" OR CommandLine="* qc *")) OR Image="C:\\Windows\\*\\systeminfo.exe" OR
   Image="C:\\Windows\\*\\tasklist.exe" OR Image="C:\\Windows\\*\\whoami.exe")|stats values(Image) as "Images" values(CommandLine) as "Command Lines" by ComputerName
```

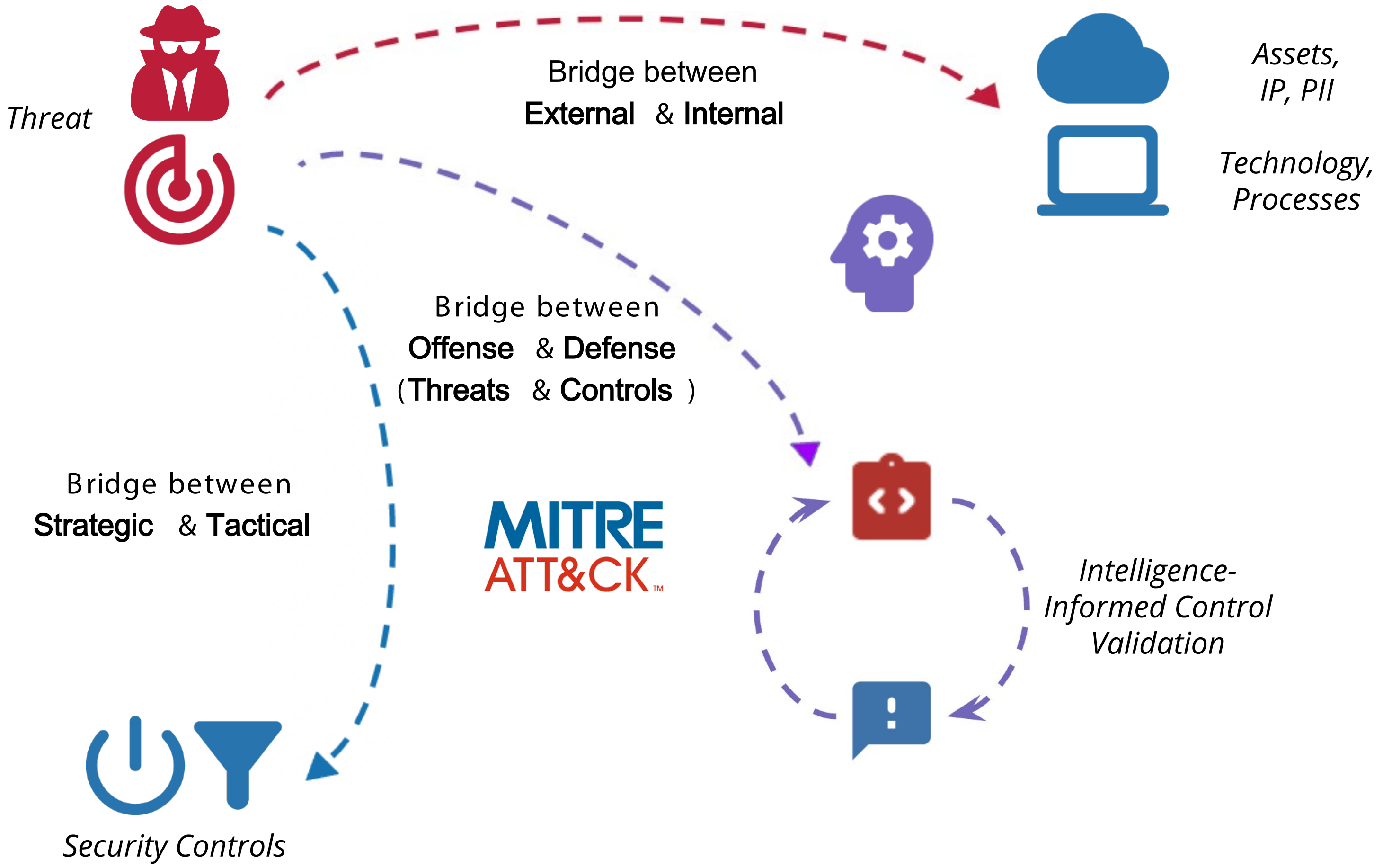
# Background

For defenders, deciding where to start when implementing behavioral detections can be daunting

Ideally, a “best practice” approach involves closing the gap between existing controls and relevant threats - but this is easier said than done

# Intelligence as a Bridge

# Intelligence as a Bridge



Threat

Bridge between
**External** & **Internal**

*Assets,*
*IP, PII*

*Technology,*
*Processes*

Bridge between
**Offense** & **Defense**
(**Threats** & **Controls**)

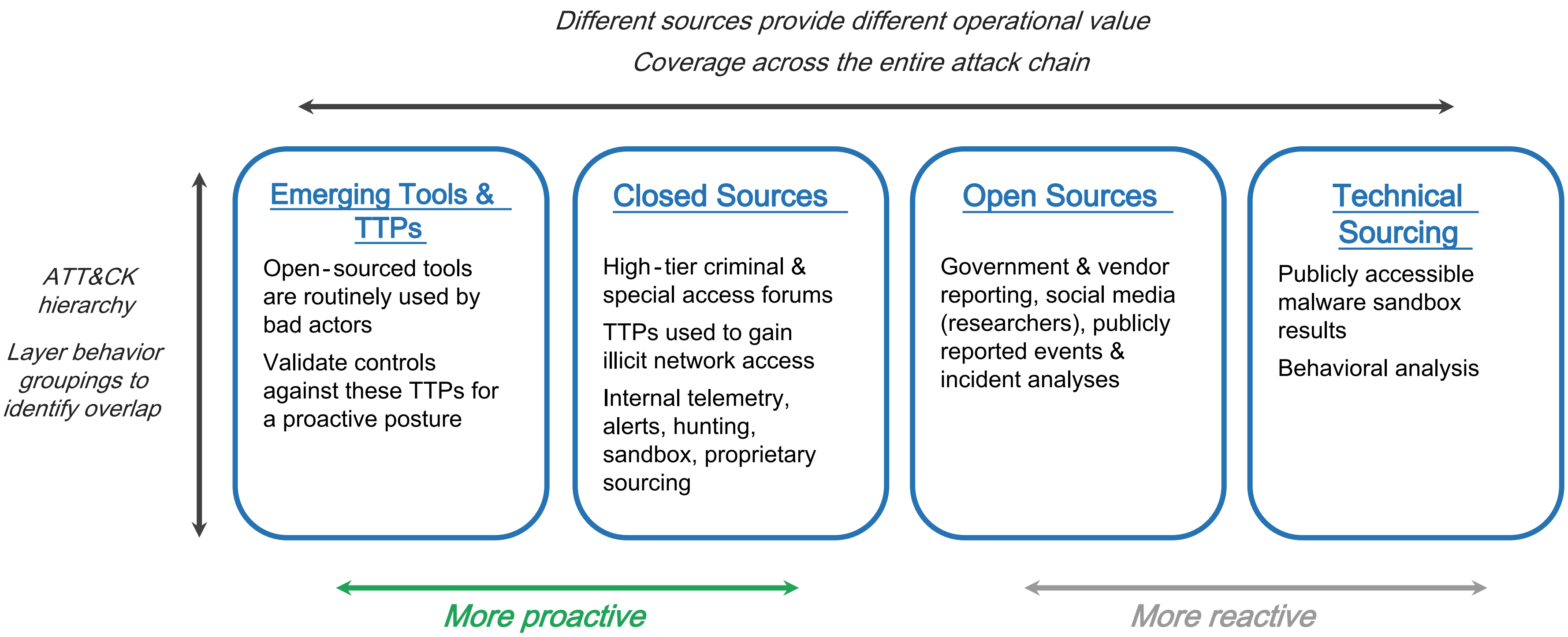
Bridge between
**Strategic** & **Tactical**

MITRE
ATT&CK™

*Intelligence-*
*Informed Control*
*Validation*

*Security Controls*

# Sourcing TTP - Focused Intelligence



*Different sources provide different operational value*

*Coverage across the entire attack chain*

*ATT&CK hierarchy*

*Layer behavior groupings to identify overlap*

## Emerging Tools & TTPs

Open-sourced tools are routinely used by bad actors

Validate controls against these TTPs for a proactive posture

## Closed Sources

High-tier criminal & special access forums

TTPs used to gain illicit network access

Internal telemetry, alerts, hunting, sandbox, proprietary sourcing

## Open Sources

Government & vendor reporting, social media (researchers), publicly reported events & incident analyses

## Technical Sourcing

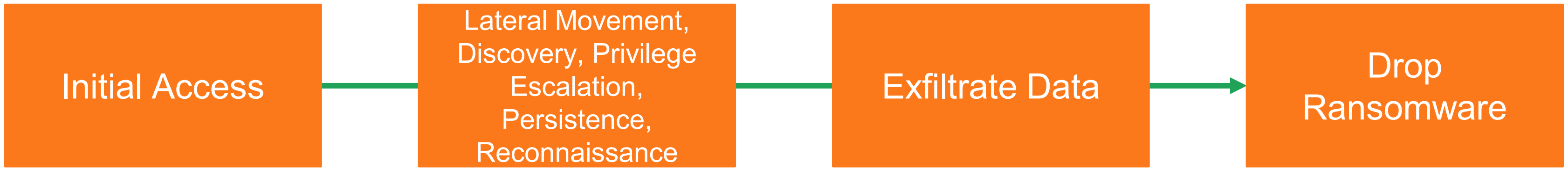
Publicly accessible malware sandbox results

Behavioral analysis

*More proactive*

*More reactive*

# Case Study: Anatomy of a Ransomware Attack



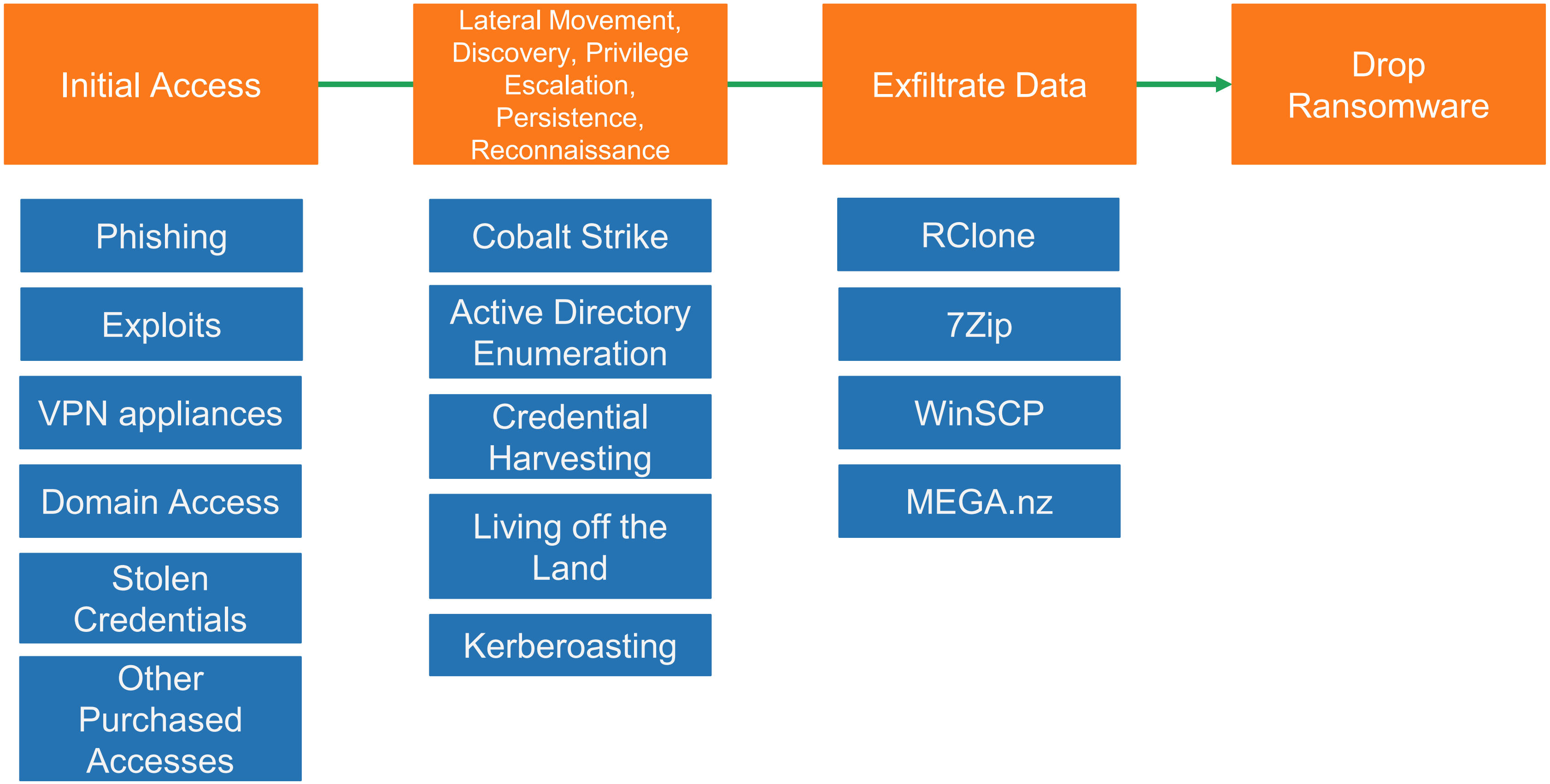
Initial Access

Lateral Movement, Discovery, Privilege Escalation, Persistence, Reconnaissance

Exfiltrate Data

Drop Ransomware

# Case Study: Anatomy of a Ransomware Attack



Initial Access

- Phishing
- Exploits
- VPN appliances
- Domain Access
- Stolen Credentials
- Other Purchased Accesses

Lateral Movement, Discovery, Privilege Escalation, Persistence, Reconnaissance

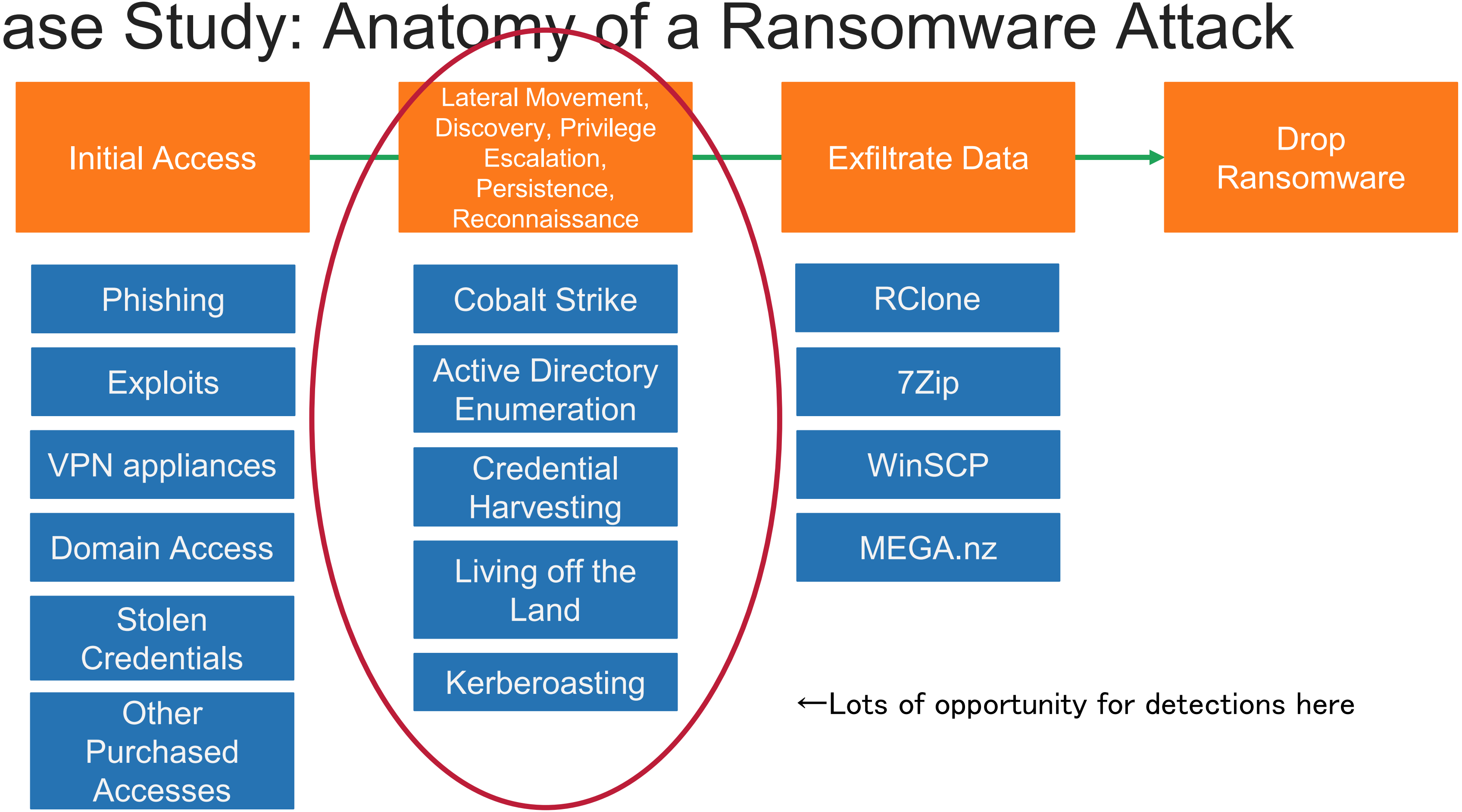
- Cobalt Strike
- Active Directory Enumeration
- Credential Harvesting
- Living off the Land
- Kerberoasting

Exfiltrate Data

- RClone
- 7Zip
- WinSCP
- MEGA.nz

Drop Ransomware

# Case Study: Anatomy of a Ransomware Attack



**Initial Access**

- Phishing
- Exploits
- VPN appliances
- Domain Access
- Stolen Credentials
- Other Purchased Accesses

**Lateral Movement, Discovery, Privilege Escalation, Persistence, Reconnaissance**

- Cobalt Strike
- Active Directory Enumeration
- Credential Harvesting
- Living off the Land
- Kerberoasting

**Exfiltrate Data**

- RClone
- 7Zip
- WinSCP
- MEGA.nz

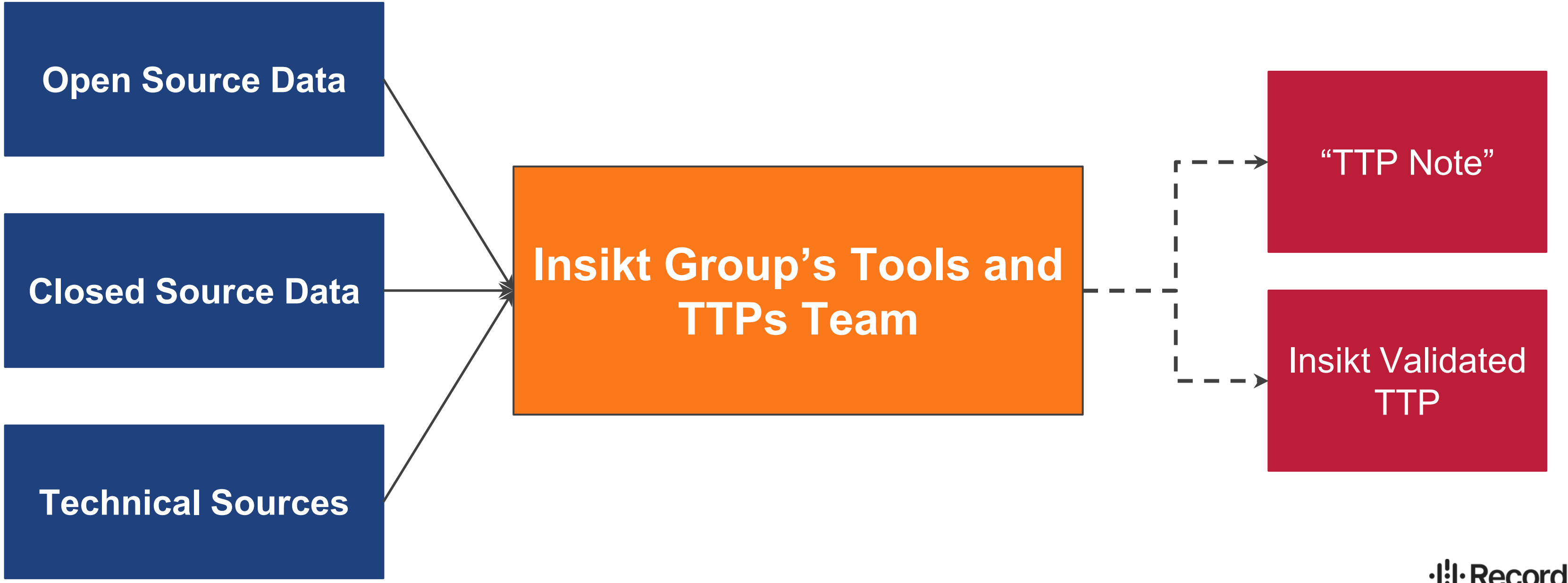
**Drop Ransomware**

←Lots of opportunity for detections here

Recorded Future

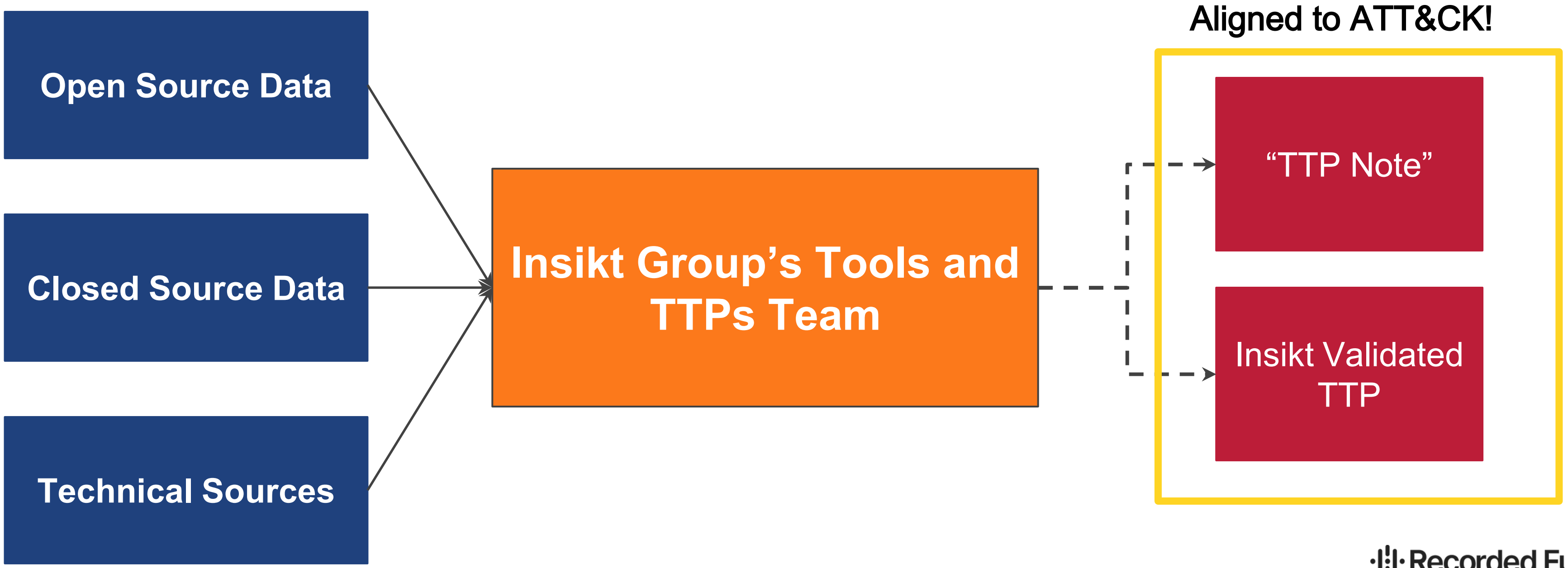
# Intel driving rule development (Insikt's process)

ATT&CK serves as a common language between highly technical concepts or reports and defenders'/operators' needs



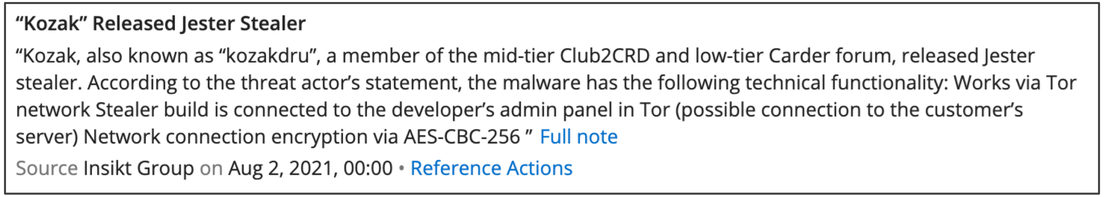
# Intel driving rule development (Insikt's process)

ATT&CK serves as a common language between highly technical concepts or reports and defenders'/operators' needs



Recorded Future®

# Case Study: Intelligence Driving Rule Development



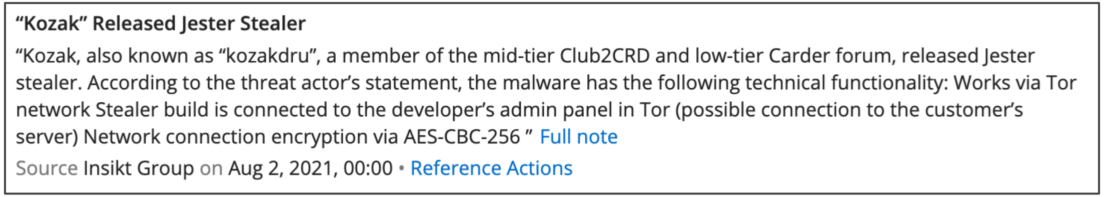
**“Kozak” Released Jester Stealer**

“Kozak, also known as “kozakdru”, a member of the mid-tier Club2CRD and low-tier Carder forum, released Jester stealer. According to the threat actor’s statement, the malware has the following technical functionality: Works via Tor network Stealer build is connected to the developer’s admin panel in Tor (possible connection to the customer’s server) Network connection encryption via AES-CBC-256 ” Full note

Source Insikt Group on Aug 2, 2021, 00:00 • Reference Actions

We saw a threat actor “release” Jester Stealer on the dark web in August 2021 - produced a “note”

# Case Study: Intelligence Driving Rule Development

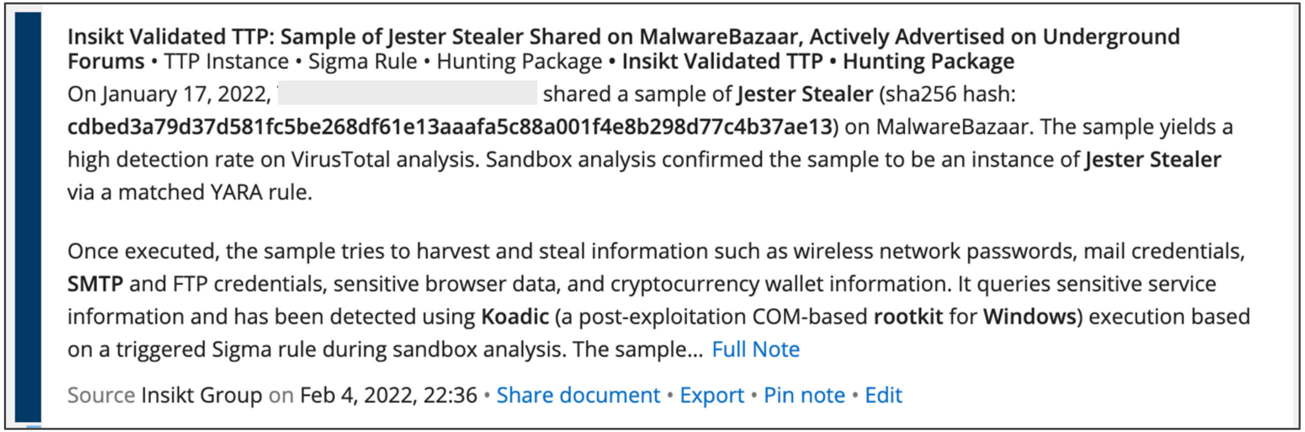


**"Kozak" Released Jester Stealer**

"Kozak, also known as "kozakdru", a member of the mid-tier Club2CRD and low-tier Carder forum, released Jester stealer. According to the threat actor's statement, the malware has the following technical functionality: Works via Tor network Stealer build is connected to the developer's admin panel in Tor (possible connection to the customer's server) Network connection encryption via AES-CBC-256 " Full note

Source Insikt Group on Aug 2, 2021, 00:00 • Reference Actions

We saw a threat actor "release" Jester Stealer on the dark web in August 2021 - produced a "note"



**Insikt Validated TTP: Sample of Jester Stealer Shared on MalwareBazaar, Actively Advertised on Underground Forums** • TTP Instance • Sigma Rule • Hunting Package • **Insikt Validated TTP • Hunting Package**

On January 17, 2022, [redacted] shared a sample of **Jester Stealer** (sha256 hash: **cdbed3a79d37d581fc5be268df61e13aaafa5c88a001f4e8b298d77c4b37ae13**) on MalwareBazaar. The sample yields a high detection rate on VirusTotal analysis. Sandbox analysis confirmed the sample to be an instance of **Jester Stealer** via a matched YARA rule.

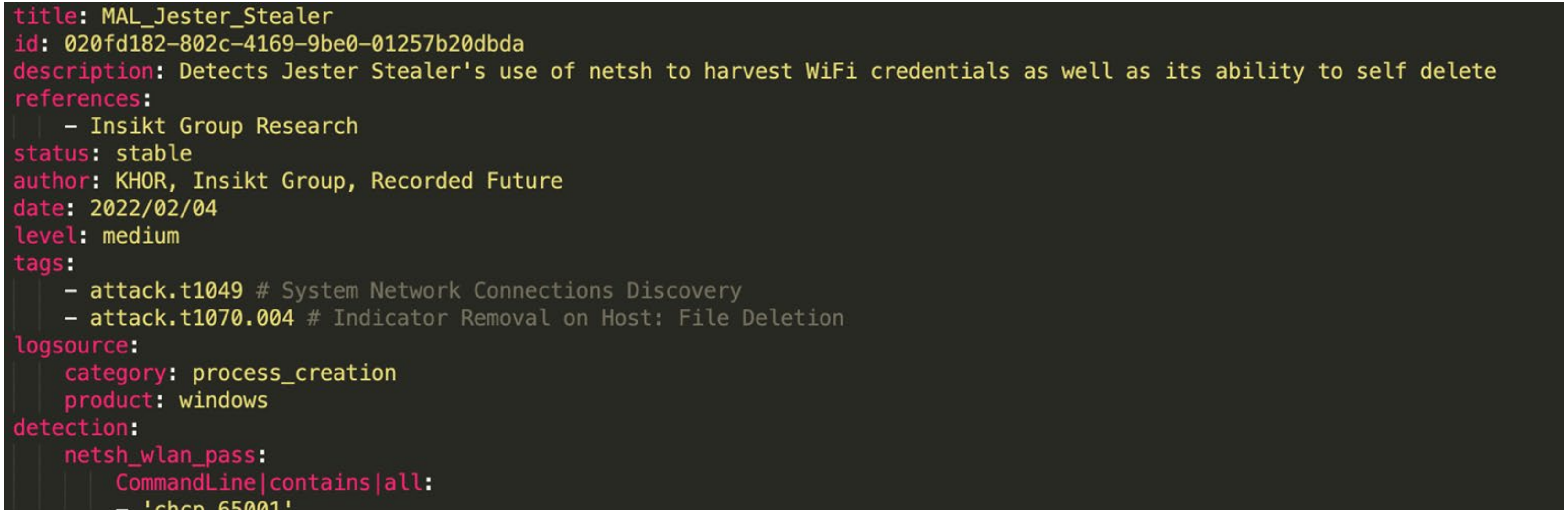
Once executed, the sample tries to harvest and steal information such as wireless network passwords, mail credentials, **SMTP** and FTP credentials, sensitive browser data, and cryptocurrency wallet information. It queries sensitive service information and has been detected using **Koadic** (a post-exploitation COM-based **rootkit** for **Windows**) execution based on a triggered Sigma rule during sandbox analysis. The sample... Full Note

Source Insikt Group on Feb 4, 2022, 22:36 • Share document • Export • Pin note • Edit

Then, in January 2022, we saw a user on social media shared a sample of Jester Stealer on MalwareBazaar….

# Case Study: Intelligence Driving Rule Development

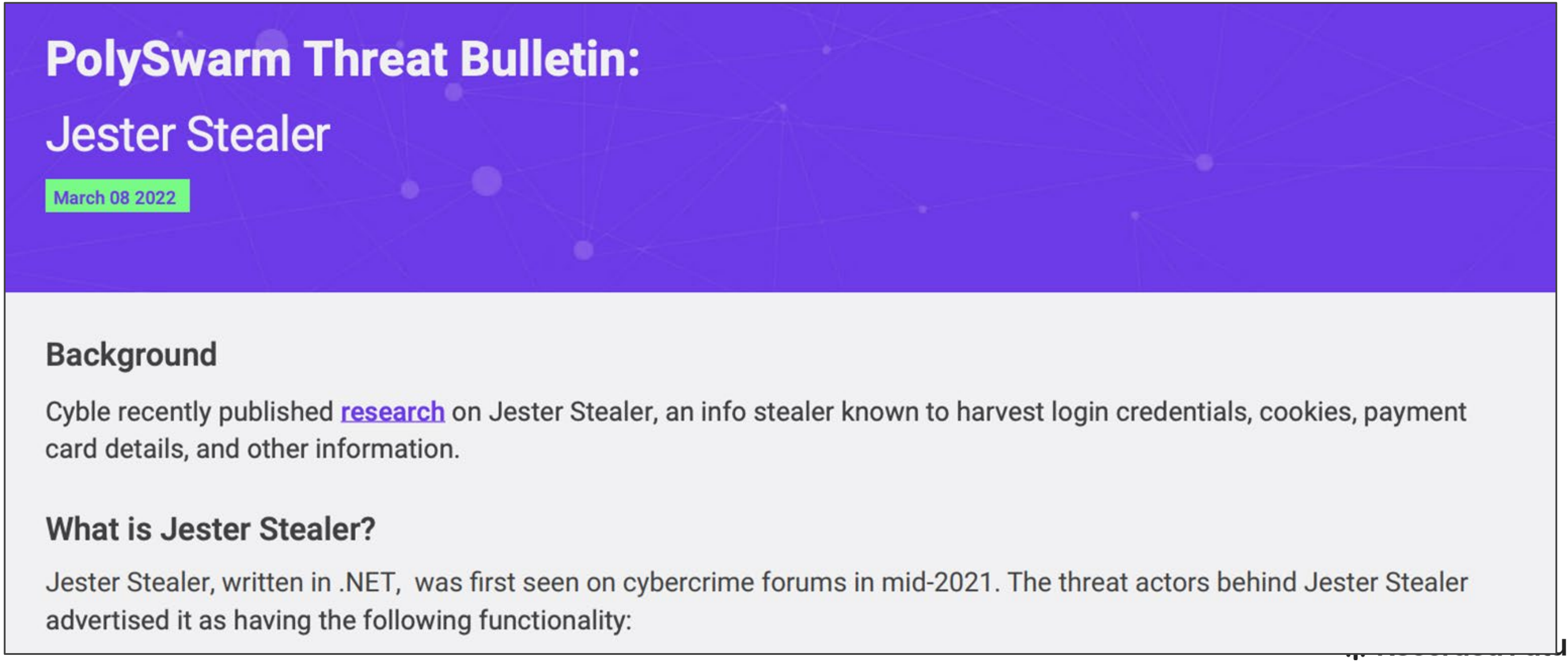
Now that Jester Stealer was openly in use, an Insikt Validated TTP was created to provide a Sigma rule to our clients, to help detect the malware



```
title: MAL_Jester_Stealer
id: 020fd182-802c-4169-9be0-01257b20dbda
description: Detects Jester Stealer's use of netsh to harvest WiFi credentials as well as its ability to self delete
references:
    - Insikt Group Research
status: stable
author: KHOR, Insikt Group, Recorded Future
date: 2022/02/04
level: medium
tags:
    - attack.t1049 # System Network Connections Discovery
    - attack.t1070.004 # Indicator Removal on Host: File Deletion
logsource:
    category: process_creation
    product: windows
detection:
    netsh_wlan_pass:
        CommandLine|contains|all:
            - 'chcp 65001'
```

# Case Study: Intelligence Driving Rule Development

One month later, other vendors identified Jester Stealer as a priority threat



## PolySwarm Threat Bulletin:

Jester Stealer

March 08 2022

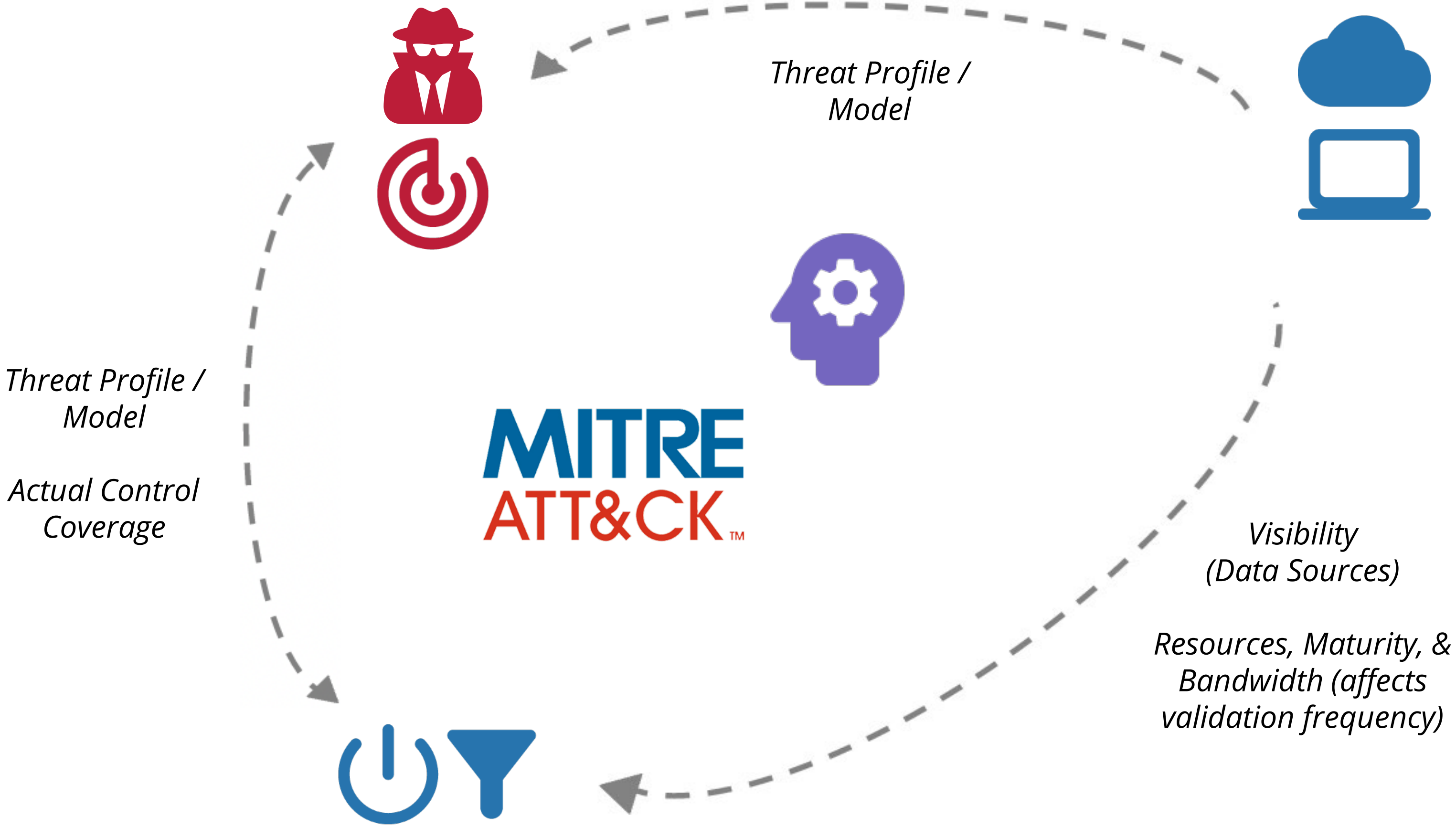
### Background

Cyble recently published research on Jester Stealer, an info stealer known to harvest login credentials, cookies, payment card details, and other information.

### What is Jester Stealer?

Jester Stealer, written in .NET,  was first seen on cybercrime forums in mid-2021. The threat actors behind Jester Stealer advertised it as having the following functionality:

# Prioritizing Detections: Risk Profiling



*Threat Profile / Model*

*Threat Profile / Model*

*Actual Control Coverage*

*Visibility (Data Sources)*

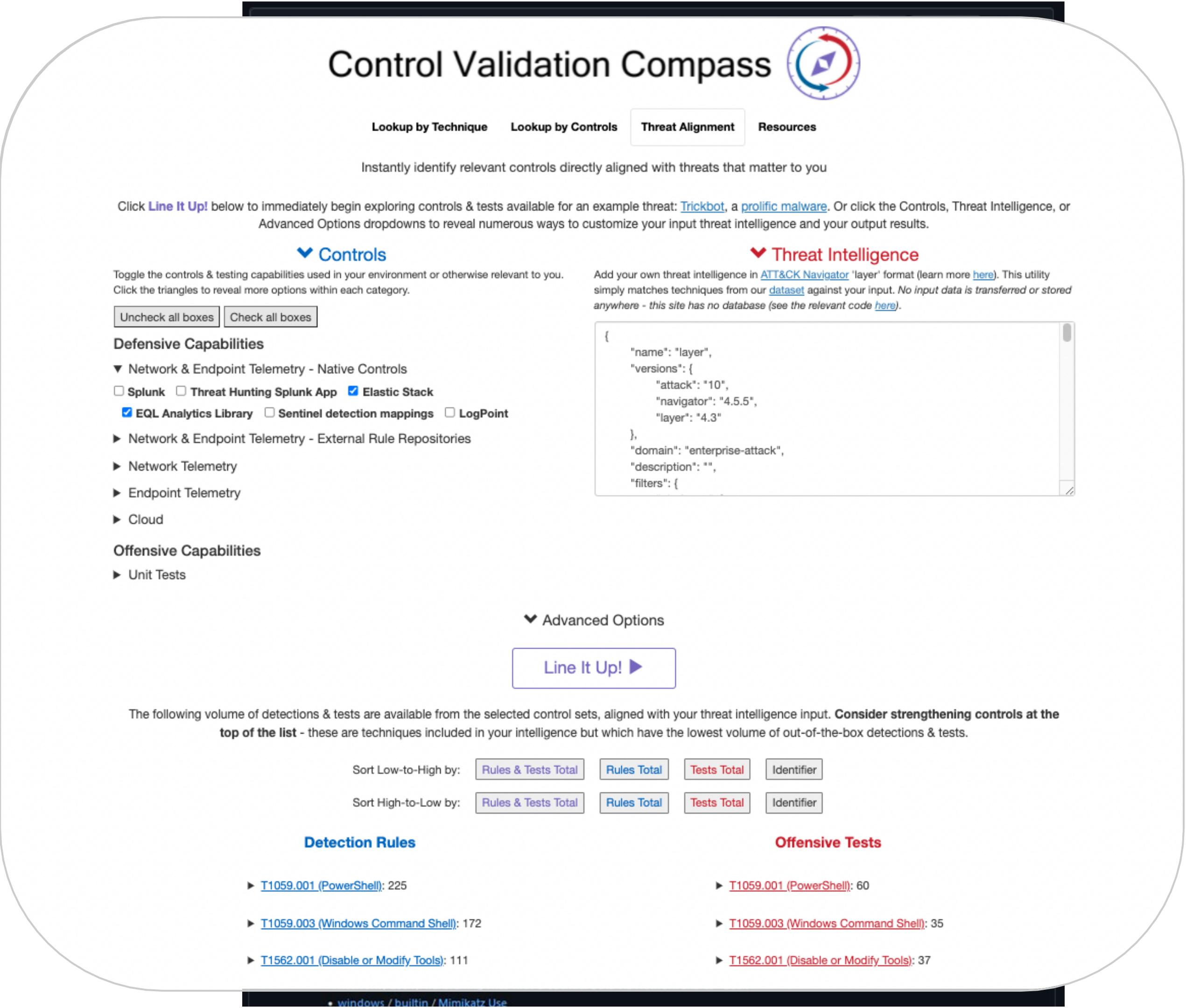
*Resources, Maturity, & Bandwidth (affects validation frequency)*

# Prioritizing Detections: A Compass to Guide You

## Control Validation Compass

[controlcompass.github.io](controlcompass.github.io)

Open source tool pointing cybersecurity teams to **9,000+** publicly-accessible technical and policy controls and **2,100+** offensive security tests, aligned with over **500** ATT&CK (sub)techniques



# Control Validation Compass

Instantly identify relevant controls directly aligned with threats that matter to you

Click **Line It Up!** below to immediately begin exploring controls & tests available for an example threat: Trickbot, a prolific malware. Or click the Controls, Threat Intelligence, or Advanced Options dropdowns to reveal numerous ways to customize your input threat intelligence and your output results.

## Controls

Toggle the controls & testing capabilities used in your environment or otherwise relevant to you. Click the triangles to reveal more options within each category.

### Defensive Capabilities

▼ Network & Endpoint Telemetry - Native Controls

□ **Splunk** □ **Threat Hunting Splunk App** ☑ **Elastic Stack**
☑ **EQL Analytics Library** □ **Sentinel detection mappings** □ **LogPoint**

▶ Network & Endpoint Telemetry - External Rule Repositories

▶ Network Telemetry

▶ Endpoint Telemetry

▶ Cloud

### Offensive Capabilities

▶ Unit Tests

## Threat Intelligence

Add your own threat intelligence in ATT&CK Navigator 'layer' format (learn more here). This utility simply matches techniques from our dataset against your input. *No input data is transferred or stored anywhere - this site has no database (see the relevant code here).*

```
{
    "name": "layer",
    "versions": {
        "attack": "10",
        "navigator": "4.5.5",
        "layer": "4.3"
    },
    "domain": "enterprise-attack",
    "description": "",
    "filters": {
```

The following volume of detections & tests are available from the selected control sets, aligned with your threat intelligence input. **Consider strengthening controls at the top of the list** - these are techniques included in your intelligence but which have the lowest volume of out-of-the-box detections & tests.

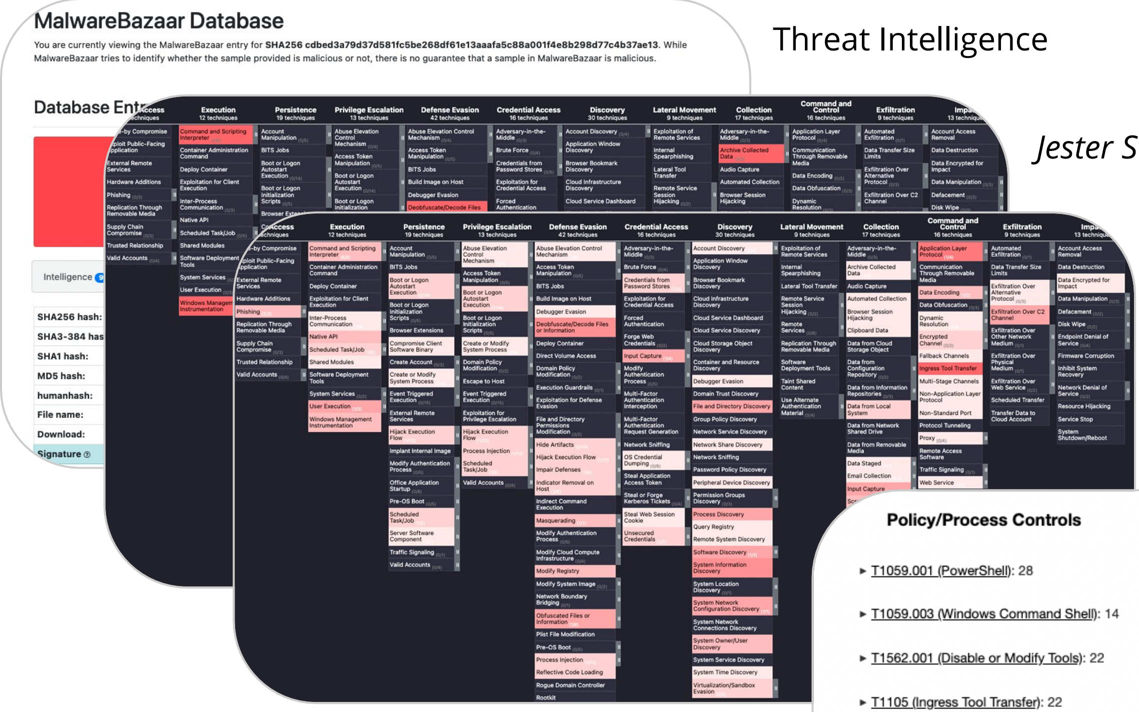
Sort Low-to-High by: Rules & Tests Total | Rules Total | Tests Total | Identifier
Sort High-to-Low by: Rules & Tests Total | Rules Total | Tests Total | Identifier

| Detection Rules | Offensive Tests |
|---|---|
| ▶ T1059.001 (PowerShell): 225 | ▶ T1059.001 (PowerShell): 60 |
| ▶ T1059.003 (Windows Command Shell): 172 | ▶ T1059.003 (Windows Command Shell): 35 |
| ▶ T1562.001 (Disable or Modify Tools): 111 | ▶ T1562.001 (Disable or Modify Tools): 37 |

- windows / builtin / Mimikatz Use

controlcompass.github.io

# Threat Intelligence



## MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 cdbed3a79d37d581fc5be268df61e13aaafa5c88a001f4e8b298d77c4b37ae13**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Ent

Intelligence

**SHA256 hash:**
**SHA3-384 has**
**SHA1 hash:**
**MD5 hash:**
**humanhash:**
**File name:**
**Download:**
**Signature**

Initial Access
Execution 12 techniques
Persistence 19 techniques
Privilege Escalation 13 techniques
Defense Evasion 42 techniques
Credential Access 16 techniques
Discovery 30 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 16 techniques
Exfiltration 9 techniques
Impact 13 techniques

*Jester Stealer*

*8 Stealer Malware (Combined)*

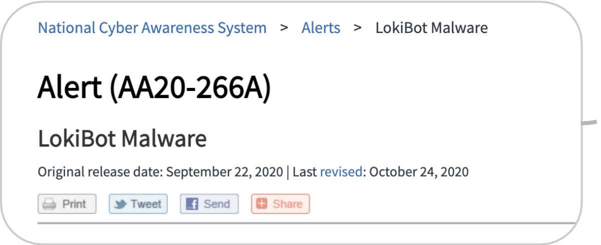
February 4, 2022 • 19 min read

## ACTINIUM targets Ukrainian organizations

Microsoft Threat Intelligence Center (MSTIC)

Microsoft Digital Security Unit (DSU)

[github.com/tropChaud/Cyber-Adversary-Heatmaps](https://github.com/tropChaud/Cyber-Adversary-Heatmaps)



National Cyber Awareness System > Alerts > LokiBot Malware

## Alert (AA20-266A)

### LokiBot Malware

Original release date: September 22, 2020 | Last revised: October 24, 2020

| **Policy/Process Controls** | **Detection Rules** | **Offensive Tests** |
|---|---|---|
| ▸ T1059.001 (PowerShell): 28 | ▸ T1059.001 (PowerShell): 284 | ▸ T1059.001 (PowerShell): 60 |
| ▸ T1059.003 (Windows Command Shell): 14 | ▸ T1059.003 (Windows Command Shell): 185 | ▸ T1059.003 (Windows Command Shell): 37 |
| ▸ T1562.001 (Disable or Modify Tools): 22 | ▸ T1562.001 (Disable or Modify Tools): 162 | ▸ T1562.001 (Disable or Modify Tools): 40 |
| ▸ T1105 (Ingress Tool Transfer): 22 | ▸ T1105 (Ingress Tool Transfer): 109 | ▸ T1105 (Ingress Tool Transfer): 66 |
| ▸ T1112 (Modify Registry): 7 | ▸ T1112 (Modify Registry): 138 | ▸ T1112 (Modify Registry): 48 |
| ▸ T1047 (Windows Management Instrumentation): 35 | ▸ T1047 (Windows Management Instrumentation): 93 | ▸ T1047 (Windows Management Instrumentation): 25 |
| ▸ T1548.002 (Bypass User Account Control): 26 | ▸ T1548.002 (Bypass User Account Control): 82 | ▸ T1548.002 (Bypass User Account Control): 40 |
| ▸ T1053.005 (Scheduled Task): 22 | ▸ T1053.005 (Scheduled Task): 69 | ▸ T1053.005 (Scheduled Task): 56 |
| ▸ T1082 (System Information Discovery): 6 | ▸ T1082 (System Information Discovery): 31 | ▸ T1082 (System Information Discovery): 85 |
| ▸ T1204.002 (Malicious File): 21 | ▸ T1204.002 (Malicious File): 69 | ▸ T1204.002 (Malicious File): 12 |

Operational takeaways (Controls)

# Thank You!