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.
Nearly 600 techniques & sub-techniques. Countless implementations of 9,000+ detection rules, 2,100+ tests.
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

Bridge between External & Internal

Bridge between Offense & Defense (Threats & Controls)

Bridge between Strategic & Tactical

Security Controls

Assets, IP, PII
Technology, Processes

Intelligence-Informed Control Validation
Different sources provide different operational value
Coverage across the entire attack chain

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

AT&T&CK hierarchy
Layer behavior groupings to identify overlap

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
- Kerberroasting

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
Intel driving rule development (Insikt’s process)

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

- Open Source Data
- Closed Source Data
- Technical Sources

Insikt Group’s Tools and TTPs Team

“TTP Note”

Insikt Validated TTP
Intel driving rule development (Insikt’s process)

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

Open Source Data
Closed Source Data
Technical Sources

Insikt Group’s Tools and TTPs Team

Aligned to ATT&CK!
“TTP Note”
Insikt Validated TTP
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, someone shared a sample of Jester Stealer (sha256 hash: cdbed3a79d377d581f5be268df61e13aaaf5e8a001fae8b2b98d77c4b37ae13) 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:
    "refresh-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

Visibility (Data Sources)
Resources, Maturity, & Bandwidth (affects validation frequency)

Actual Control Coverage

MITRE ATT&CK™
Prioritizing Detections: A Compass to Guide You

Control Validation Compass

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

Lookup by Technique  Lookup by Controls  Threat Alignment  Resources

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

Advanced Options

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.

<table>
<thead>
<tr>
<th>Soft Low-to-High by:</th>
<th>Rules &amp; Tests Total</th>
<th>Rules Total</th>
<th>Tests Total</th>
<th>Identifier</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Soft High-to-Low by:</th>
<th>Rules &amp; Tests Total</th>
<th>Rules Total</th>
<th>Tests Total</th>
<th>Identifier</th>
</tr>
</thead>
</table>

Detection Rules
- T1109.001 (PowerShell): 225
- T1109.003 (Windows Command Shell): 172
- T1162.001 (Process or Module Hook): 111

Offensive Tests
- T1109.001 (PowerShell): 60
- T1109.003 (Windows Command Shell): 35
- T1162.001 (Windows Hook): 37

Control Compass
controlcompass.github.io
Threat Intelligence

Jester Stealer

ACTINUM targets Ukrainian organizations
Microsoft Threat Intelligence Center (MSTIC)
Microsoft Digital Security Unit (DSU)

8 Stealer Malware (Combined)

Policy/Process Controls
- T1059.001 (PowerShell): 26
- T1098.003 (Windows Command Shell): 14
- T1162.001 (Disable or Modify Tools): 22
- T1106 (Process Tool Transfer): 22
- T1112 (Modify Registry): 7
- T1047 (Windows Management Instrumentation): 35
- T1548.002 (Bypass User Account Control): 26
- T1053.005 (Scheduled Task): 22
- T1082 (System Information Discovery): 6
- T1204.002 (Malicious File): 21

Detection Rules
- T1059.001 (PowerShell): 264
- T1098.003 (Windows Command Shell): 185
- T1162.001 (Disable or Modify Tools): 182
- T1106 (Process Tool Transfer): 109
- T1112 (Modify Registry): 138
- T1047 (Windows Management Instrumentation): 93
- T1548.002 (Bypass User Account Control): 82
- T1053.005 (Scheduled Task): 69
- T1082 (System Information Discovery): 31
- T1204.002 (Malicious File): 69

Offensive Tests
- T1059.001 (PowerShell): 60
- T1098.003 (Windows Command Shell): 37
- T1162.001 (Disable or Modify Tools): 40
- T1106 (Process Tool Transfer): 66
- T1112 (Modify Registry): 48
- T1047 (Windows Management Instrumentation): 25
- T1548.002 (Bypass User Account Control): 20
- T1053.005 (Scheduled Task): 56
- T1082 (System Information Discovery): 85
- T1204.002 (Malicious File): 12

Operational takeaways (Controls)
Thank You!