**Splunk**

Project Overview:

* Title : Mini SOC using the Splunk and wireshark Dataset
* Goal: Simulate real-world SOC operations, perform threat hunting and incident response using Splunk and the wireshark dataset.

Tools & Setup:

* Splunk – Dockerized instance
* Dataset – 2025-06-21-Koi-Loader-Koi-Stealer-infection-traffic.pcap
* OS - Windows 11 (host), Docker Environment.
* VirusTotal and other tools

Suricata:   
Suricata is an open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that monitors network traffic for threats and can block malicious activity. It is developed by the Open Information Security Foundation (OISF) and is known for its flexibility and ability to analyze network packets in detail.

Splunk setup:

1. Docker installation required

(<https://docs.docker.com/engine/install/>)

1. docker pull splunk/splunk:latest
2. docker run -d --name splunk -p 8000:8000 -p 8088:8088 \

-p 9997:9997 -e SPLUNK\_START\_ARGS="--accept-license" \

-e SPLUNK\_PASSWORD="YOURPASSWORD" splunk/splunk:latest

1. Open in browser <http://localhost:8080>

**Executive Summary**

This report documents the simulation of a Security Operations Center (SOC) environment using Splunk and Suricata with a malware-infected network traffic dataset. The objective was to detect, analyze, and respond to threats within a controlled environment by ingesting Suricata logs into Splunk for investigation. The investigation revealed a malicious communication involving the "Koi Stealer" malware contacting a Command and Control (C2) server. Using MITRE ATT&CK mapping, threat intelligence tools, and Splunk's powerful analytics, we validated the threat, confirmed the indicators of compromise (IOCs), and assessed the incident's severity. Recommendations for containment and further action were provided above.

**Timeline of Events:**

21/6/2025 – 12:45:19.124338 = Malware Command and Control Activity Detected

21/6/2025 – 12:45:19. 690174 = A Network Trojan was detected

21/6/2025 – 12:45:22.971809 = Not Suspicious Traffic

21/6/2025 – 12:45:27.273262 = Repeated Not Suspicious Traffic

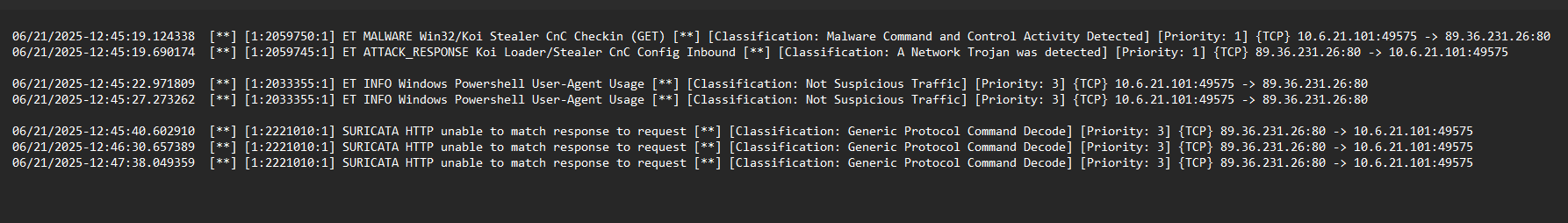
21/6/2025 – 12:45:40.602910 = Generic Protocol Command Decode

21/6/2025 – 12:46:30.657389 = Repeated Generic Protocol Command Decode

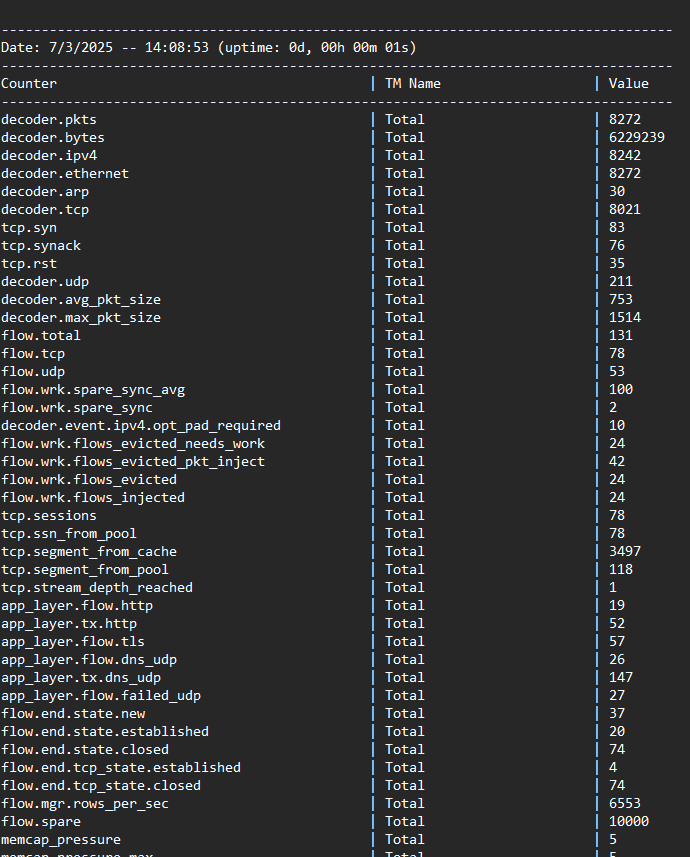
**Log Evidence(s):**

Using the Suricata we going to perform the analyses on the Splunk for hunting threat from the alerts produced by the SURICATA alerts

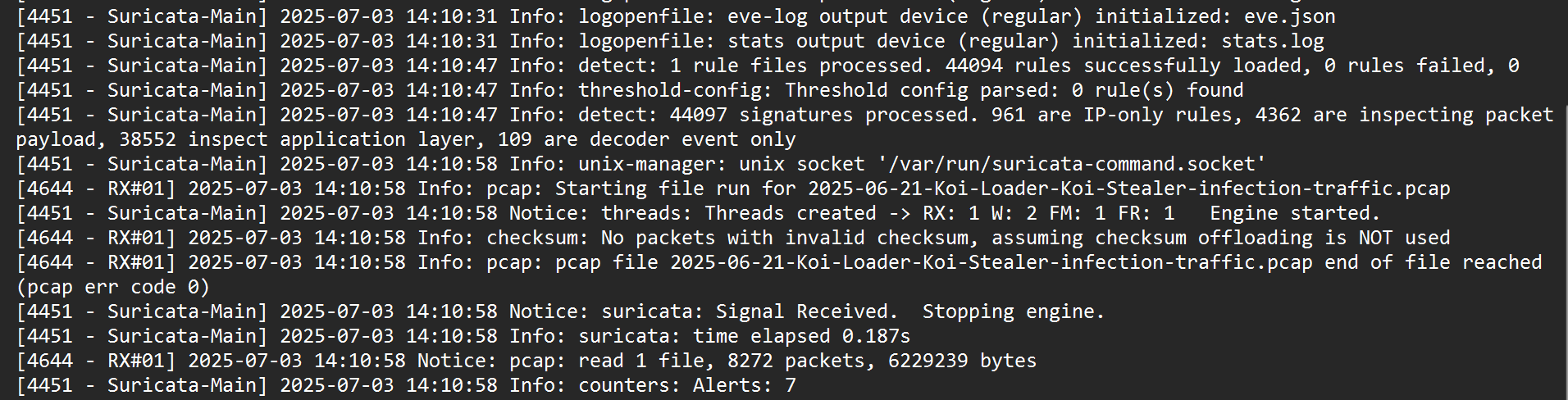
1. fast.log – Summary of alerts generated by suricata IDS/IPS.



1. stats.log – It is a log file that provides statistical information about the performance and activity of the Suricata IDS/IPS.

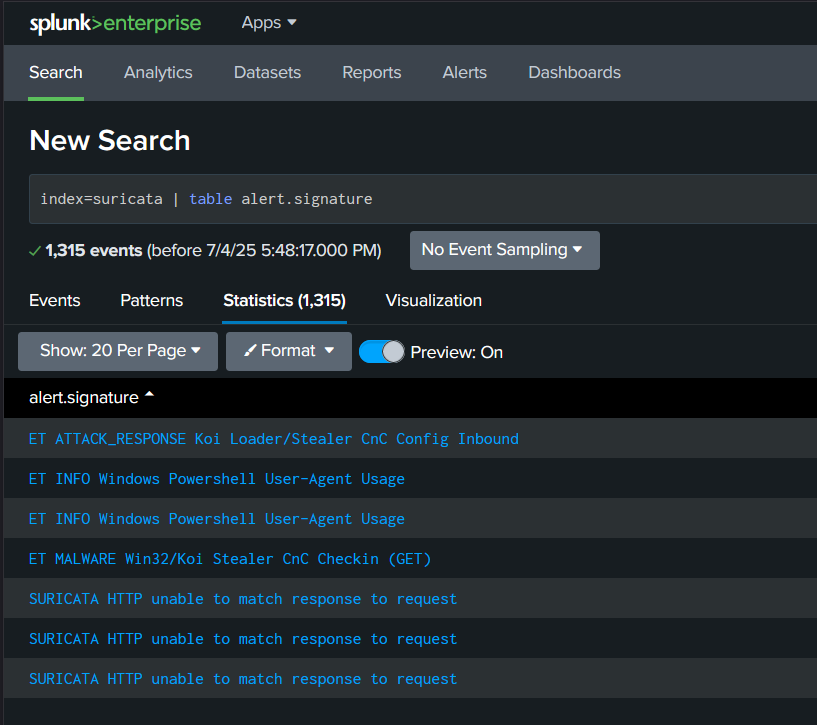


1. suricata.log – It is a log file that captures various informational and error messages generated by the Suricata IDS/IPS during its operation.

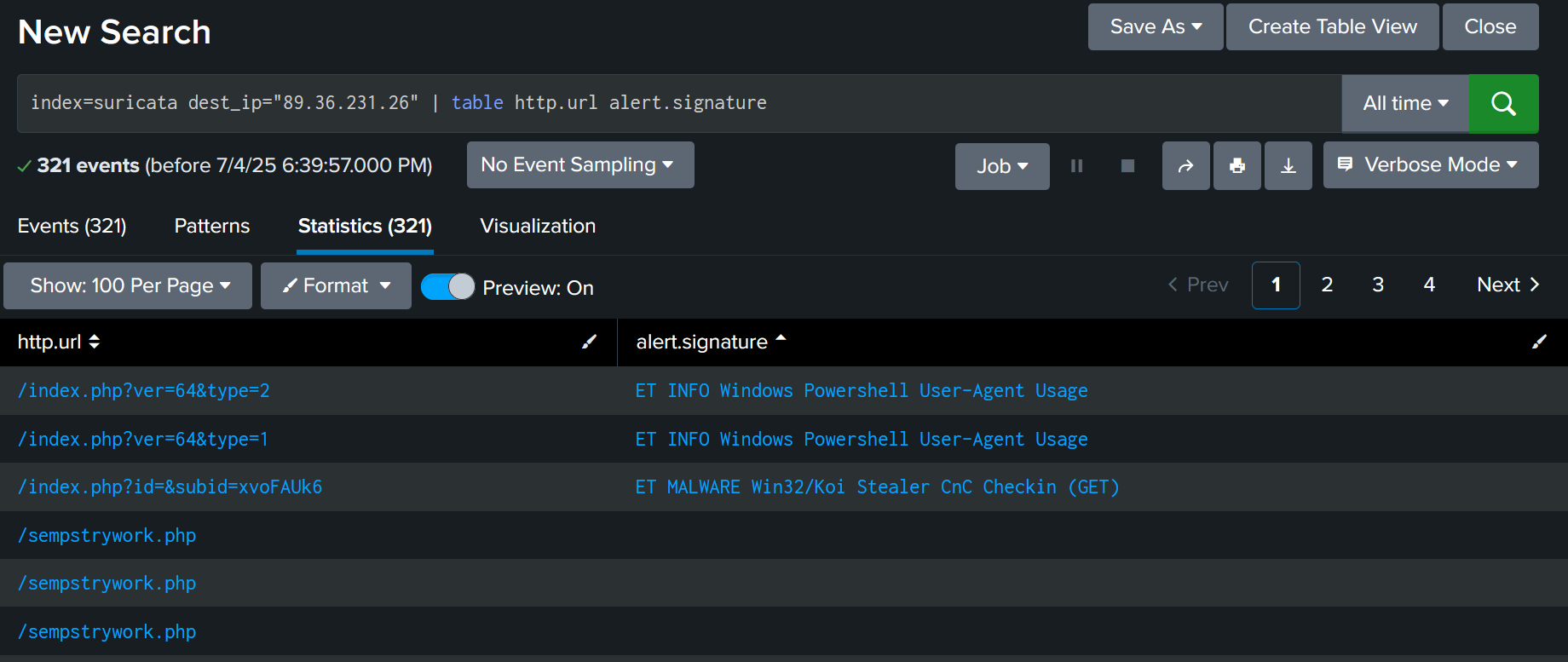


**Splunk Investigation:**

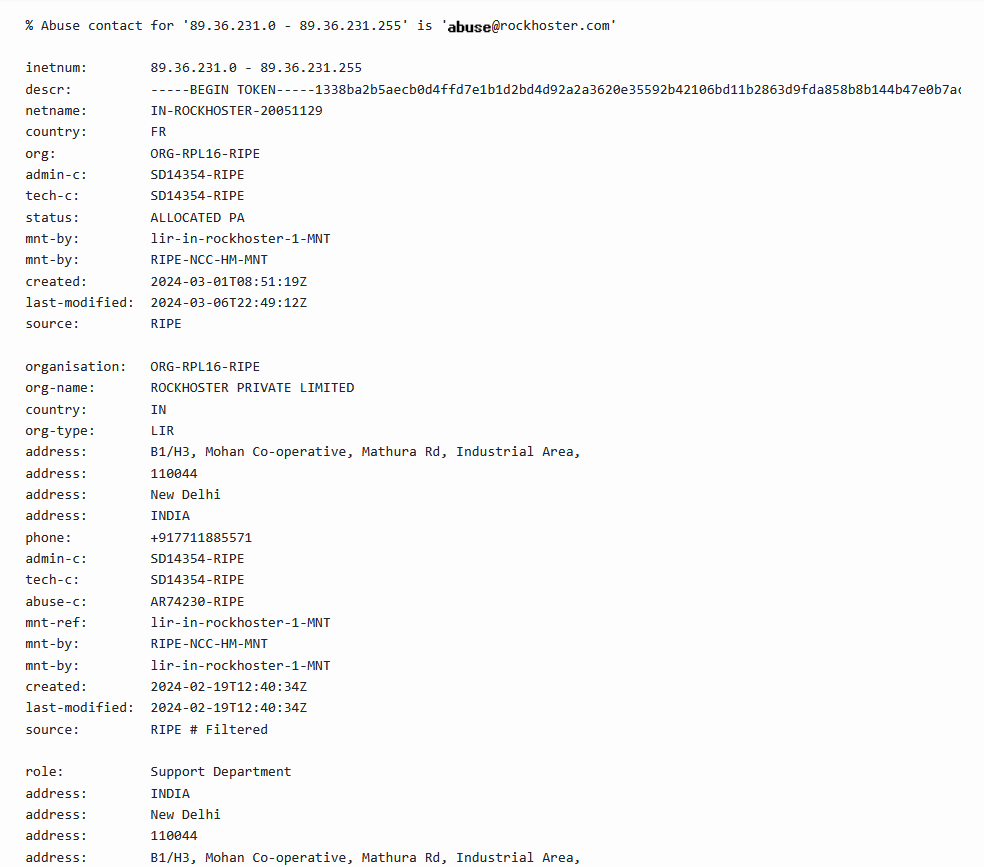
1. Alert signature verifying



1. Using the IP from the fast.log identified the alert signatures and http.url + files

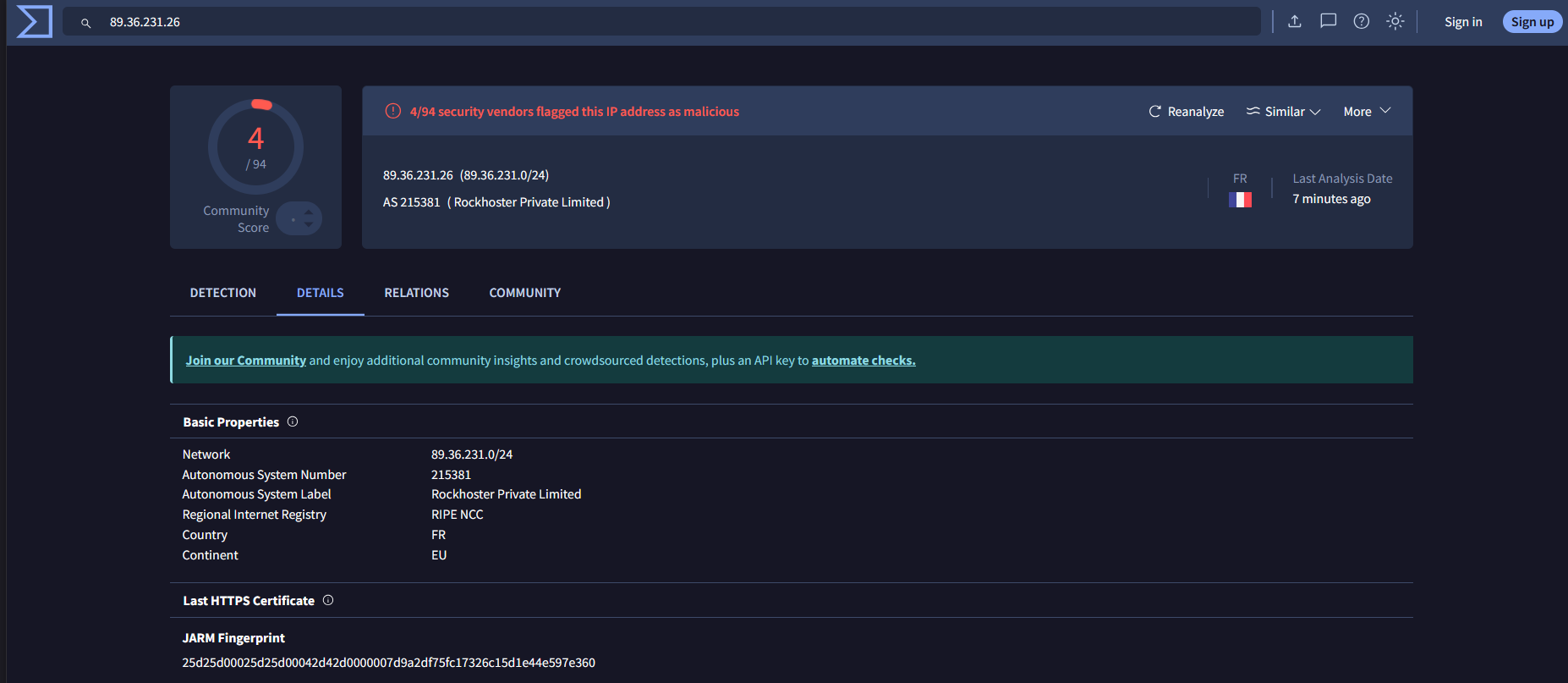


1. “whois” lookup for destination IP : 89.36.231.26



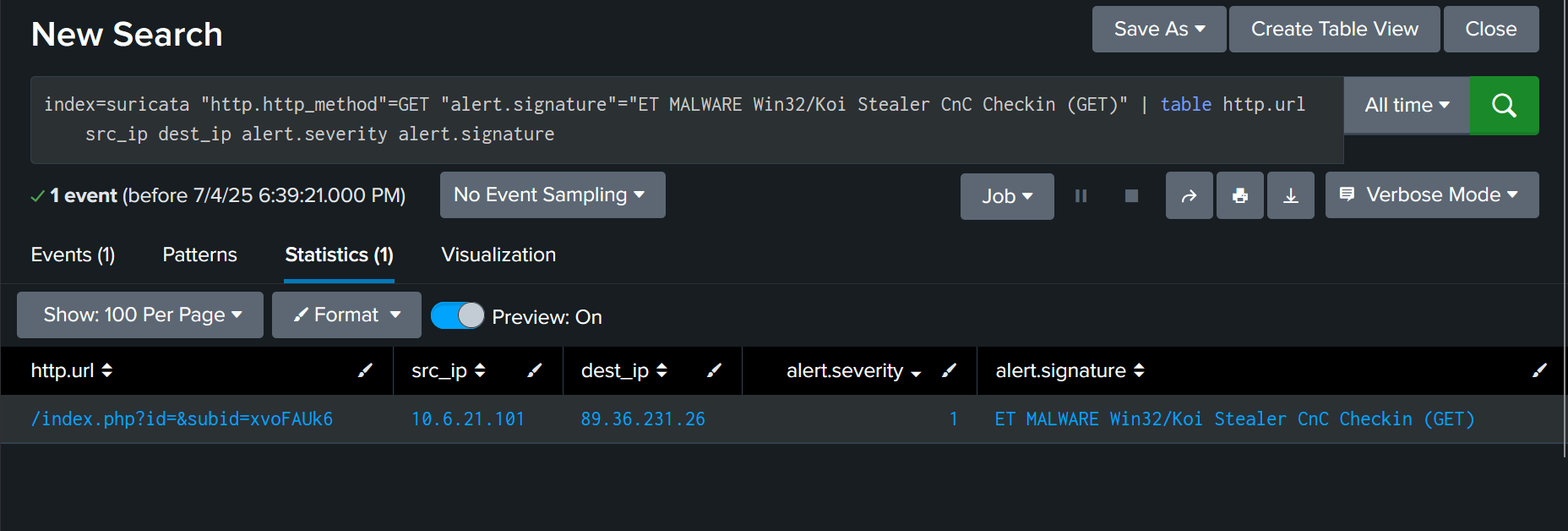
1. Virustotal :

https://www.virustotal.com/gui/ip-address/89.36.231.26/details



1. Investigating the “ET MALWARE Win32/Koi Stealer CnC Checkin (GET)”

“index=suricata "http.http\_method"=GET "alert.signature"="ET MALWARE Win32/Koi Stealer CnC Checkin (GET)" | table http.url src\_ip dest\_ip alert.severity alert.signature”



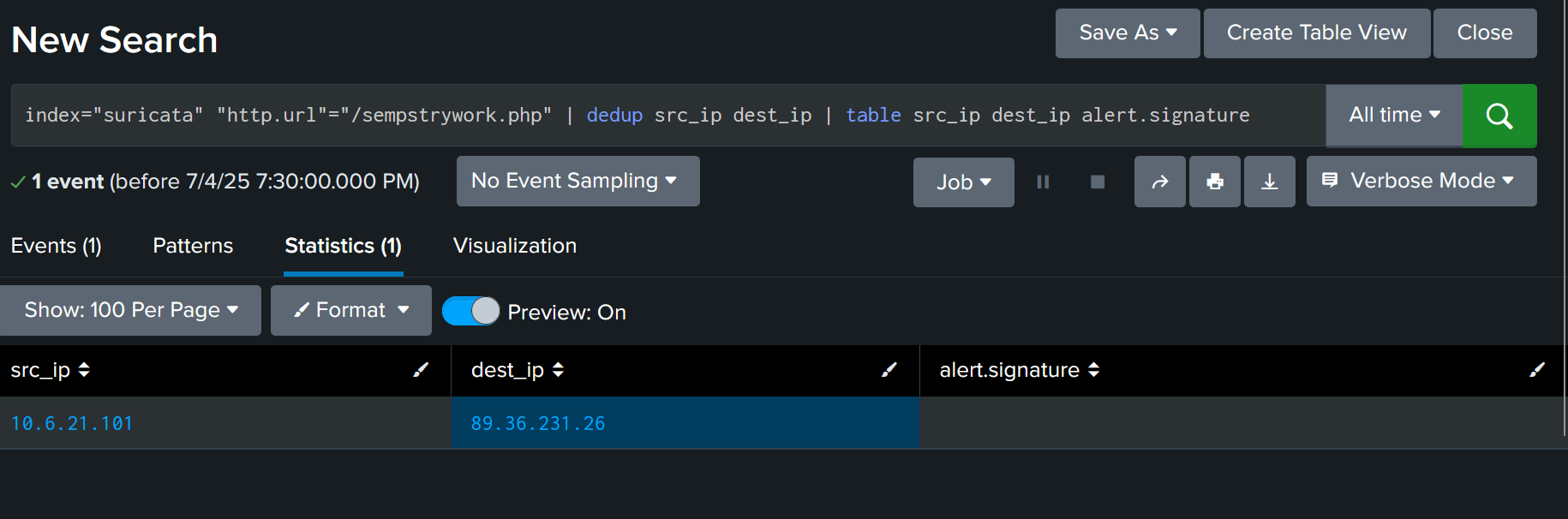
Let investigate what it is “/index.php?id=&subid=xvoFAUk6”

I got:

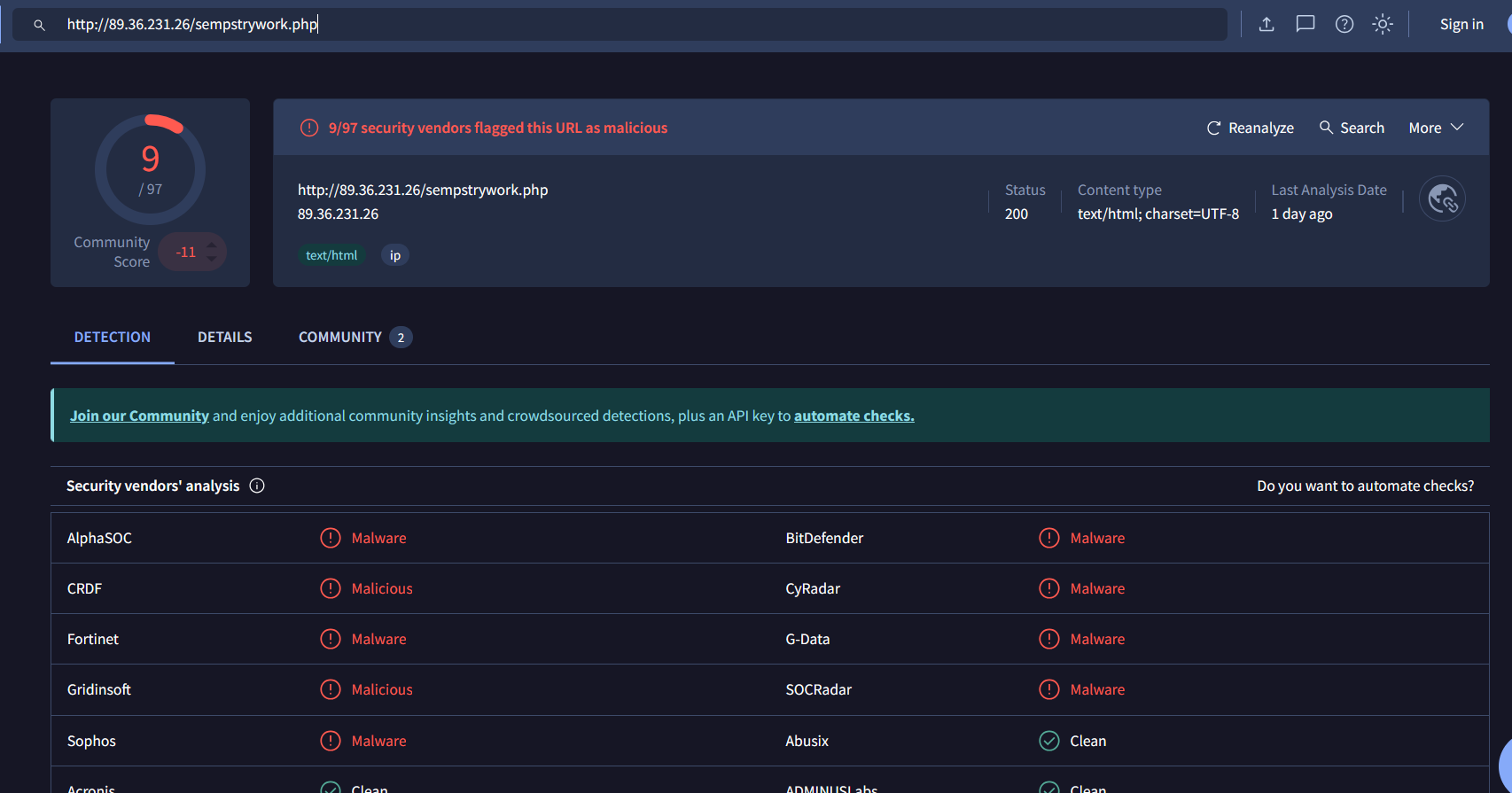
1. Affected product : Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit
2. Malware family: Koi-Stealer
3. Mitre Att&ck
4. Tactic\_id : TA0011
5. Tactic\_name : Command\_And\_Control
6. Technique\_id: T1105
7. Technique\_name : Ingree\_Tool\_Transfer
8. Created at : 2025\_01\_29
9. Source : 89.36.231.26 : 80
10. Target : 10.6.21.101 : 49575

--------------------------------------------------------------------------------------------------------------------------------------

1. Investigating the “/sempstrywork.php”



Reference (hybrid-analysis): <https://hybrid-analysis.com/sample/36475886fdf01aaa9c51cc1beac108e58d5cbc07c4868aebcbb4923c879fcd3a/6859d11184c8cb916f06387e>



Details:

IOC: hxxp://89.36.231.26/sempstrywork.php

IOC Type: url

Threat Type: botnet\_cc

Malware: Koi Stealer

Confidence Level: 100%

Reference:hxxps://bazaar.abuse.ch/sample/84577db0b164c06ef9628a94eb693150dc2101332ed526f4d431ddb56b3a7c4c/

ThreatFox: <https://threatfox.abuse.ch/ioc/1548411/>

**Threat Hunting Hypotheses:**

We hypothesized that the traffic observed in the PCAP file represented an active malware infection involving C2 communication. To validate this, we focused on HTTP GET requests, analyzed suspicious URL patterns and endpoints, and enriched the IOCs with threat intelligence platforms such as VirusTotal, Hybrid Analysis, and ThreatFox.

**Detection Rules:**

1. Suricata Alert:

1:2059750:1 : ET MALWARE Win32/Koi Stealer CnC Checkin (GET)

1:2059745:1 : ET ATTACK\_RESPONSE Koi Loader/Stealer CnC Config Inbound

1:2033355:1 : ET INFO Windows Powershell User-Agent Usage

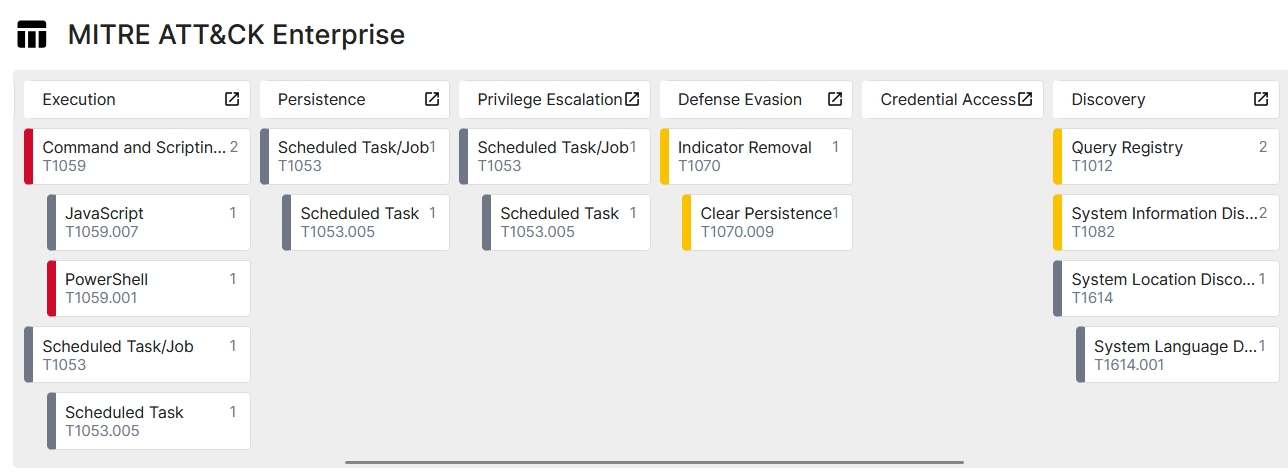
1:2221010:1 : SURICATA HTTP unable to match response to request

1. Splunk Queries:

* index = "suricata" | table src\_ip dest\_ip alert.signature
* index = "suricata" http.http\_method="GET" | table src\_ip dest\_ip alert.signature http.http\_method
* index = "suricata" "alert.signature"="ET MALWARE Win32/Koi Stealer CnC Checkin (GET)" | table src\_ip dest\_ip http.url
* index = "suricata" "alert.signature"="ET ATTACK\_RESPONSE Koi Loader/Stealer CnC Config Inbound" | table src\_ip dest\_ip http.url
* index = "suricata" | dedup http.url | table src\_ip dest\_ip http.url
* index = "suricata" "alert.signature"="ET INFO Windows Powershell User-Agent Usage" | table src\_ip dest\_ip http.url
* index = "suricata" "alert.signature"="SURICATA HTTP unable to match response to request" | table src\_ip dest\_ip http.url
* index=suricata "http.url"="/sempstrywork.php" | table src\_ip, dest\_ip, alert.signature

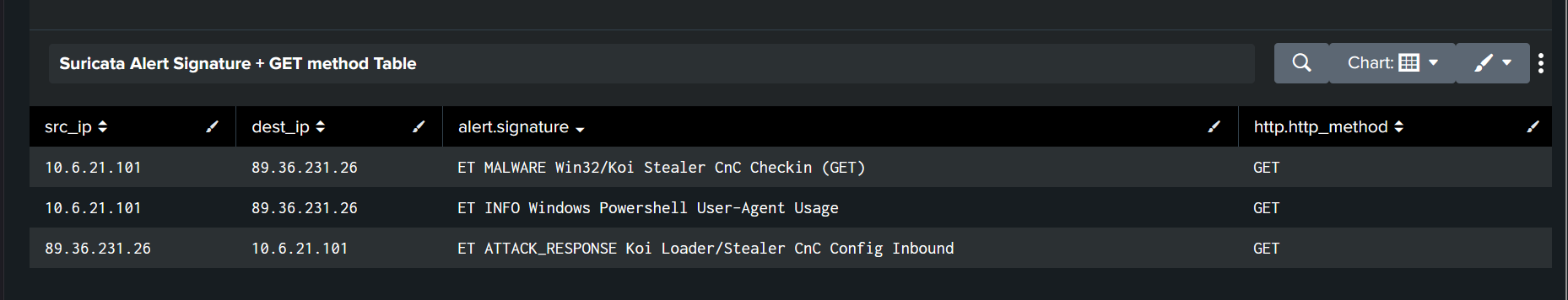
MITRE ATT&CK Mapping:

|  |  |
| --- | --- |
| Defense Evasion | Hide Artifacts (T1564),  Indirect Command Execution (T1202)  Indicator Removal(T1070) |
| Execution | Scheduled Task/Job (T1053),  Command and Scripting Interpreter (T1059) |
| Persistence | Scheduled Task/Job (T1053) |
| Privilege Escalation | Scheduled Task/Job (T1053) |
| Reconnaissance | Active Scanning (T1595) |
| Impact | System Shutdown/Reboot (T1529) |



C2 connection using the network packets

The Logs are generated by suricata



**Incident Classification and Severity**

Classification: Malware Command and Control Activity Detected

Severity: 1

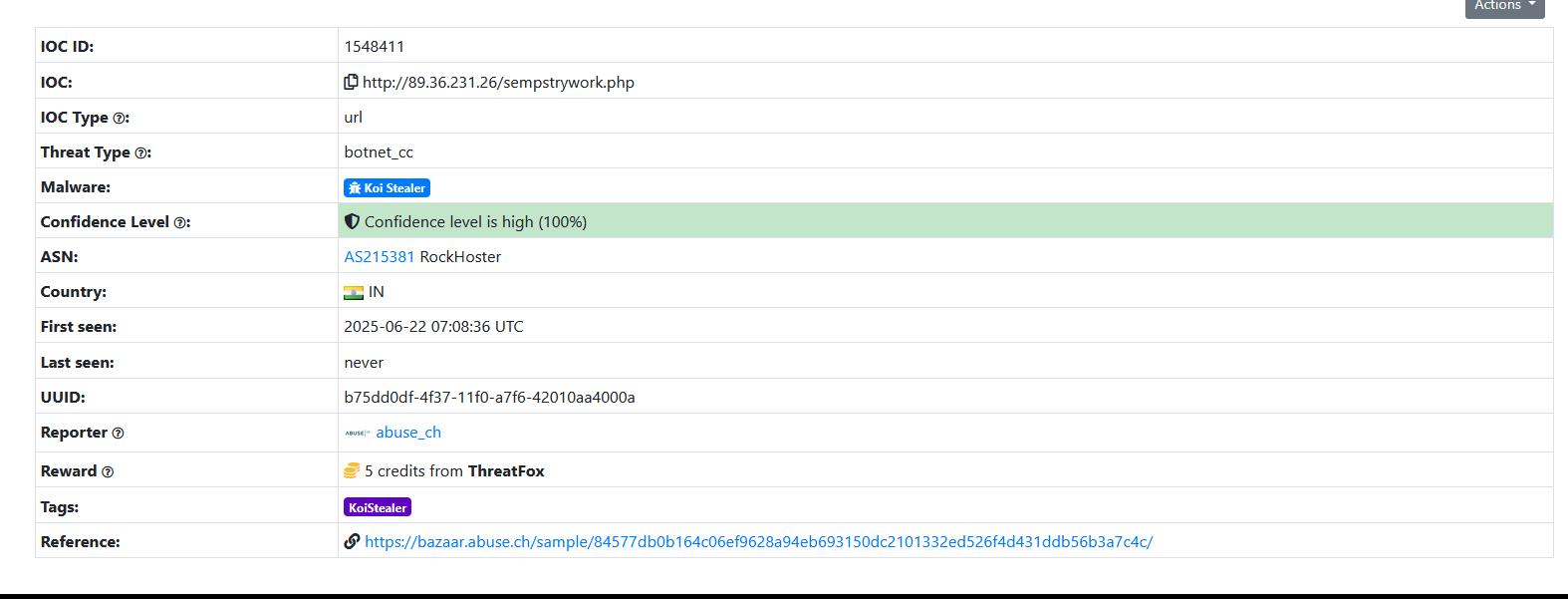
Connections: 10.6.21.101:49575 -> 89.36.231.26:80

Suricata Alert Dataset: ET MALWARE Win32/Koi Stealer CnC Checkin (GET)

Dataset rule No: 2059750

Justification: ­

1. Spawns new processes and Dropped files for persistence
2. Accessed the “.php” file from the IP -> <http://89.36.231.26/sempstrywork.php>
3. Known Malware : Koi-Stealer
4. Target : Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit
5. IOC: hxxp://89.36.231.26/sempstrywork.php
6. IOC Type: url
7. Threat Type: botnet\_cc
8. Confidence Level: 100%
9. Payload\_url : hxxps[:]//vuelaviajero[.]com/wp-includes/images
10. Process Analysis : <https://cyber-fortress.com/docs/result/index.php?id=6857a7b9b06783b9ebd692b4>



sha256 : 84577db0b164c06ef9628a94eb693150dc2101332ed526f4d431ddb56b3a7c4c

Creation Time - 2025-06-16 01:17:03 UTC

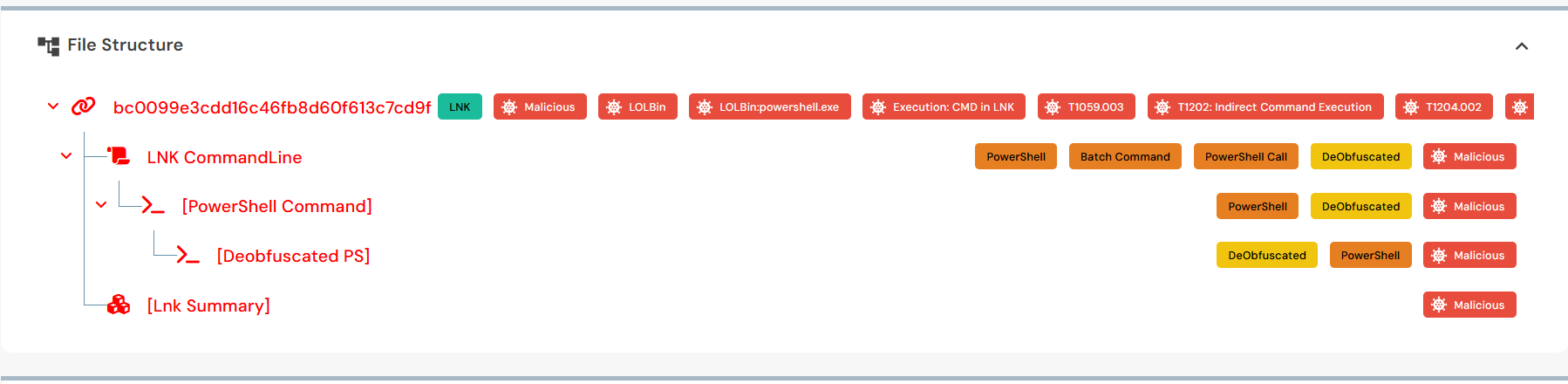
First Seen In The Wild - 2025-06-22 10:02:21 UTC

First Submission - 2025-06-22 06:53:30 UTC

Last Submission - 2025-06-26 09:43:37 UTC

Last Analysis - 2025-06-23 06:00:50 UTC

File Structure of Infection

­­­

**Recommendations & Response Plan**

Immediate Actions:

* Block outbound traffic to 89.36.231.26
* Isolate the affected host (10.6.21.101) from the network
* Notify the incident response team
* Investigation:
* Perform endpoint forensic analysis
* Check for persistence mechanisms or dropped executables
* Analyze full packet capture for potential lateral movement

Prevention:

* Update IDS/IPS rules
* Harden firewall rules to restrict untrusted HTTP traffic
* Deploy EDR and behavior-based detection mechanisms
* Monitoring:
* Continue monitoring for related IOCs
* Add detected signatures to Splunk alerts

­

**Appendix**

IOC: <http://89.36.231.26/sempstrywork.php>

VT Report: <https://www.virustotal.com/gui/ip-address/89.36.231.26/details>

<https://www.virustotal.com/gui/file/84577db0b164c06ef9628a94eb693150dc2101332ed526f4d431ddb56b3a7c4c/details>

Hybrid Analysis: <https://hybrid-analysis.com/sample/36475886fdf01aaa9c51cc1beac108e58d5cbc07c4868aebcbb4923c879fcd3a/6859d11184c8cb916f06387e>

ThreatFox: <https://threatfox.abuse.ch/ioc/1548411/>