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/)
2. docker pull splunk/splunk:latest
3.
```
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
```
4. 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

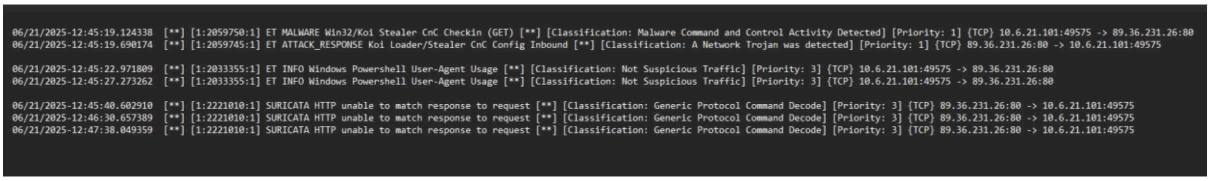
21/6/2025 – 12:45:40.602910 = Generic Protocol Command Decode

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

Log Evidence(s):

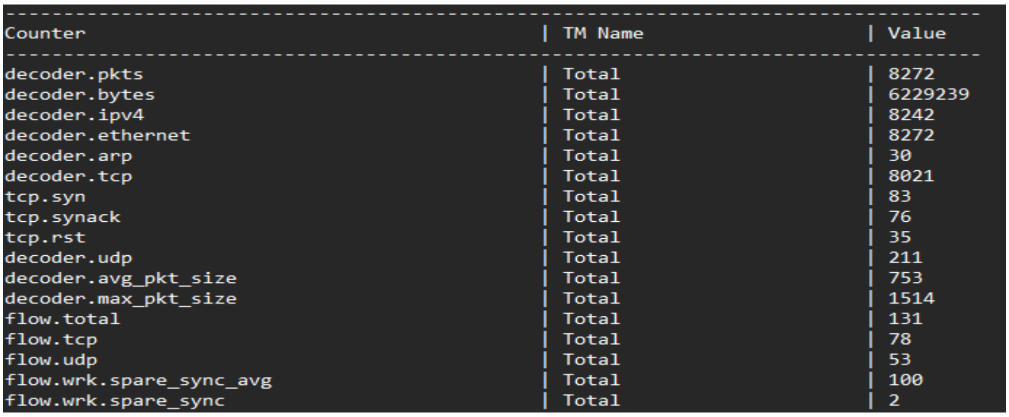
Using the Suricata we going to perform the analyses on the Splunk for hunting threat from the alerts produced by the SURICATA alerts

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



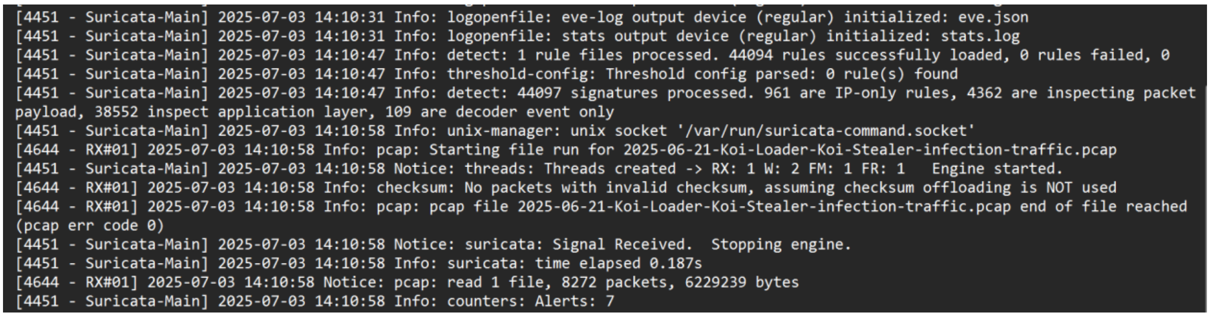
```
06/21/2025-12:45:19.124338  [**] [1:2059750:1] ET MALWARE Win32/Koi Stealer CnC Checkin (GET) [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] {TCP} 10.6.21.101:49575 -> 89.36.231.26:80
06/21/2025-12:45:19.690174  [**] [1:2059745:1] ET ATTACK_RESPONSE Koi Loader/Stealer CnC Config Inbound [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 89.36.231.26:80 -> 10.6.21.101:49575

06/21/2025-12:45:22.971809  [**] [1:2033355:1] ET INFO Windows Powershell User-Agent Usage [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.6.21.101:49575 -> 89.36.231.26:80
06/21/2025-12:45:27.273262  [**] [1:2033355:1] ET INFO Windows Powershell User-Agent Usage [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.6.21.101:49575 -> 89.36.231.26:80

06/21/2025-12:45:40.602910  [**] [1:2221010:1] SURICATA HTTP unable to match response to request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 89.36.231.26:80 -> 10.6.21.101:49575
06/21/2025-12:46:30.657389  [**] [1:2221010:1] SURICATA HTTP unable to match response to request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 89.36.231.26:80 -> 10.6.21.101:49575
06/21/2025-12:47:38.049359  [**] [1:2221010:1] SURICATA HTTP unable to match response to request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 89.36.231.26:80 -> 10.6.21.101:49575
```

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



```
------------------------------------------------------------------------------------
Counter                                      | TM Name                   | Value
------------------------------------------------------------------------------------
decoder.pkts                                 | Total                     | 8272
decoder.bytes                                | Total                     | 6229239
decoder.ipv4                                 | Total                     | 8242
decoder.ethernet                             | Total                     | 8272
decoder.arp                                  | Total                     | 30
decoder.tcp                                  | Total                     | 8021
tcp.syn                                      | Total                     | 83
tcp.synack                                   | Total                     | 76
tcp.rst                                      | Total                     | 35
decoder.udp                                  | Total                     | 211
decoder.avg_pkt_size                         | Total                     | 753
decoder.max_pkt_size                         | Total                     | 1514
flow.total                                   | Total                     | 131
flow.tcp                                     | Total                     | 78
flow.udp                                     | Total                     | 53
flow.wrk.spare_sync_avg                      | Total                     | 100
flow.wrk.spare_sync                          | Total                     | 2
```

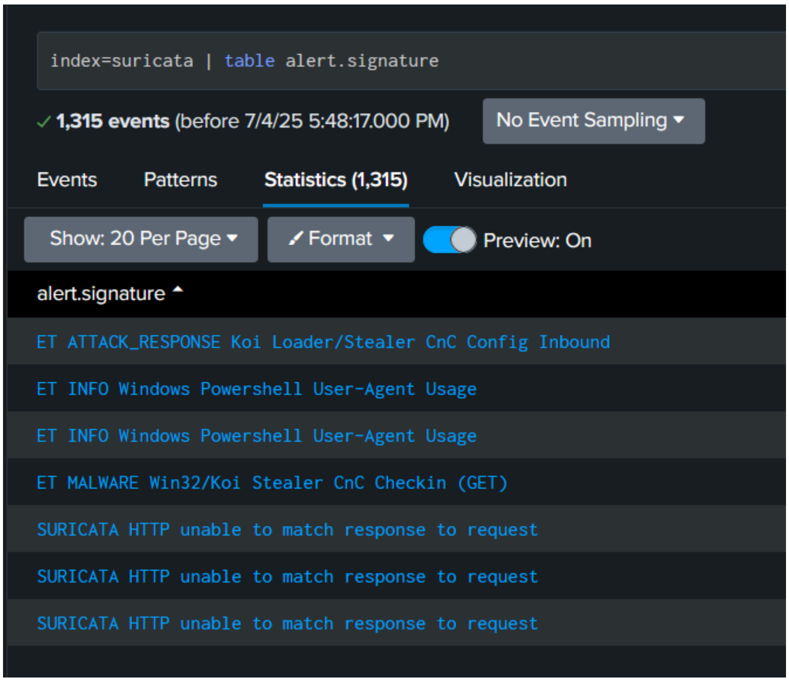
3. suricata.log – It is a log file that captures various informational and error messages generated by the Suricata IDS/IPS during its operation.



```
[4451 - Suricata-Main] 2025-07-03 14:10:31 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[4451 - Suricata-Main] 2025-07-03 14:10:31 Info: logopenfile: stats output device (regular) initialized: stats.log
[4451 - Suricata-Main] 2025-07-03 14:10:47 Info: detect: 1 rule files processed. 44094 rules successfully loaded, 0 rules failed, 0
[4451 - Suricata-Main] 2025-07-03 14:10:47 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[4451 - Suricata-Main] 2025-07-03 14:10:47 Info: detect: 44097 signatures processed. 961 are IP-only rules, 4362 are inspecting packet
payload, 38552 inspect application layer, 109 are decoder event only
[4451 - Suricata-Main] 2025-07-03 14:10:58 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
[4644 - RX#01] 2025-07-03 14:10:58 Info: pcap: Starting file run for 2025-06-21-Koi-Loader-Koi-Stealer-infection-traffic.pcap
[4451 - Suricata-Main] 2025-07-03 14:10:58 Notice: threads: Threads created -> RX: 1 W: 2 FM: 1 FR: 1   Engine started.
[4644 - RX#01] 2025-07-03 14:10:58 Info: checksum: No packets with invalid checksum, assuming checksum offloading is NOT used
[4644 - RX#01] 2025-07-03 14:10:58 Info: pcap: pcap file 2025-06-21-Koi-Loader-Koi-Stealer-infection-traffic.pcap end of file reached
(pcap err code 0)
[4451 - Suricata-Main] 2025-07-03 14:10:58 Notice: suricata: Signal Received.  Stopping engine.
[4451 - Suricata-Main] 2025-07-03 14:10:58 Info: suricata: time elapsed 0.187s
[4644 - RX#01] 2025-07-03 14:10:58 Notice: pcap: read 1 file, 8272 packets, 6229239 bytes
[4451 - Suricata-Main] 2025-07-03 14:10:58 Info: counters: Alerts: 7
```

Splunk Investigation:

1. Alert signature verifying

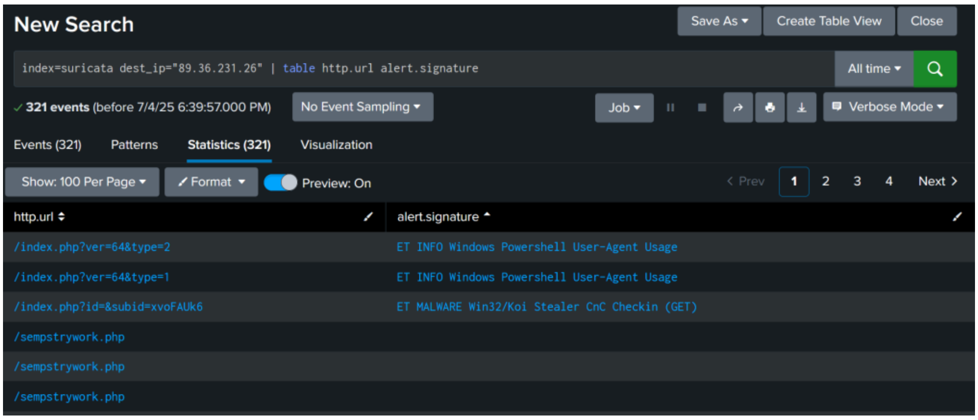


```
index=suricata | table alert.signature
```

✓ **1,315 events** (before 7/4/25 5:48:17.000 PM)

alert.signature
ET ATTACK_RESPONSE Koi Loader/Stealer CnC Config Inbound
ET INFO Windows Powershell User-Agent Usage
ET INFO Windows Powershell User-Agent Usage
ET MALWARE Win32/Koi Stealer CnC Checkin (GET)
SURICATA HTTP unable to match response to request
SURICATA HTTP unable to match response to request
SURICATA HTTP unable to match response to request

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

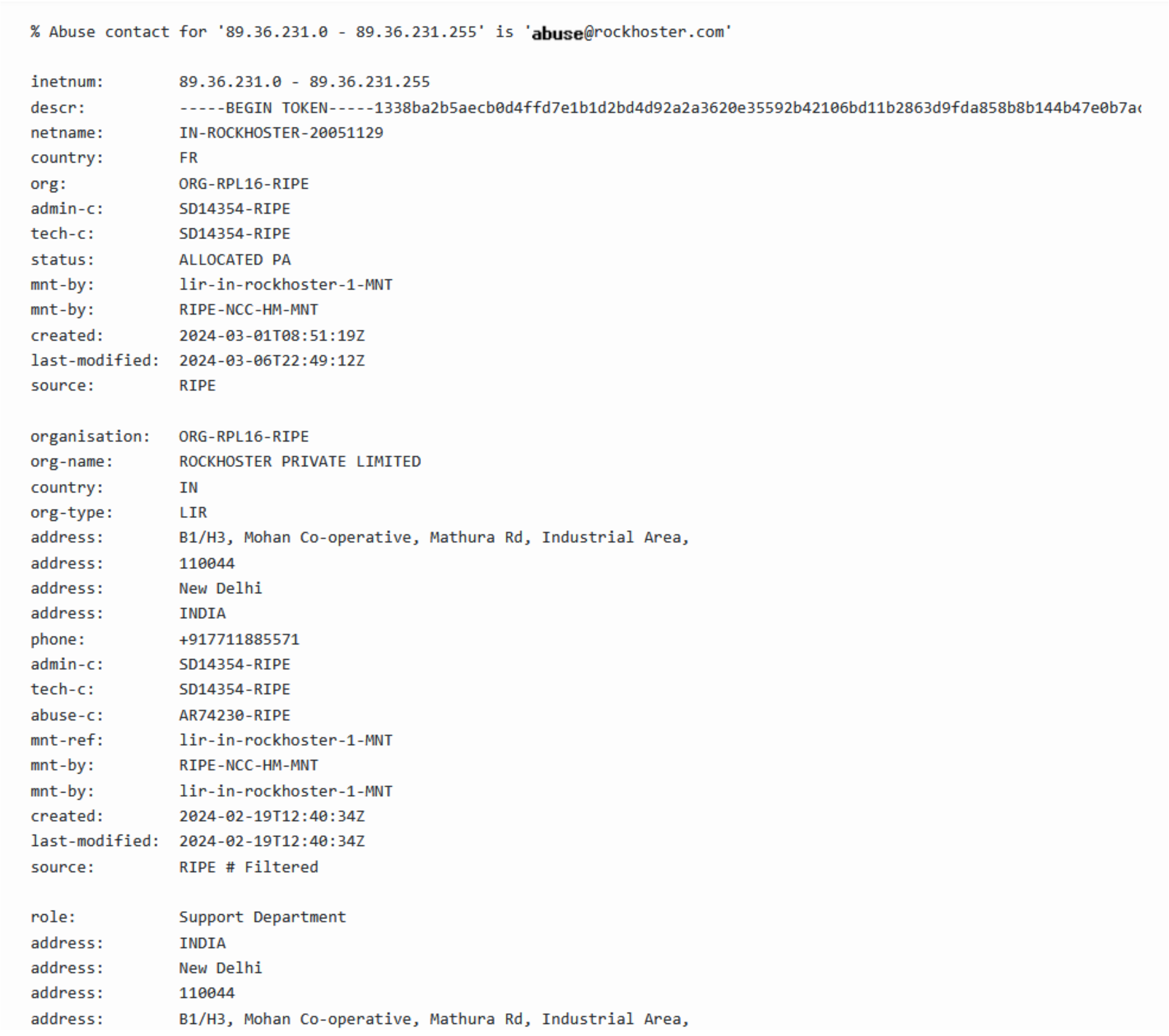


```
index=suricata dest_ip="89.36.231.26" | table http.url alert.signature
```

✓ **321 events** (before 7/4/25 6:39:57.000 PM)

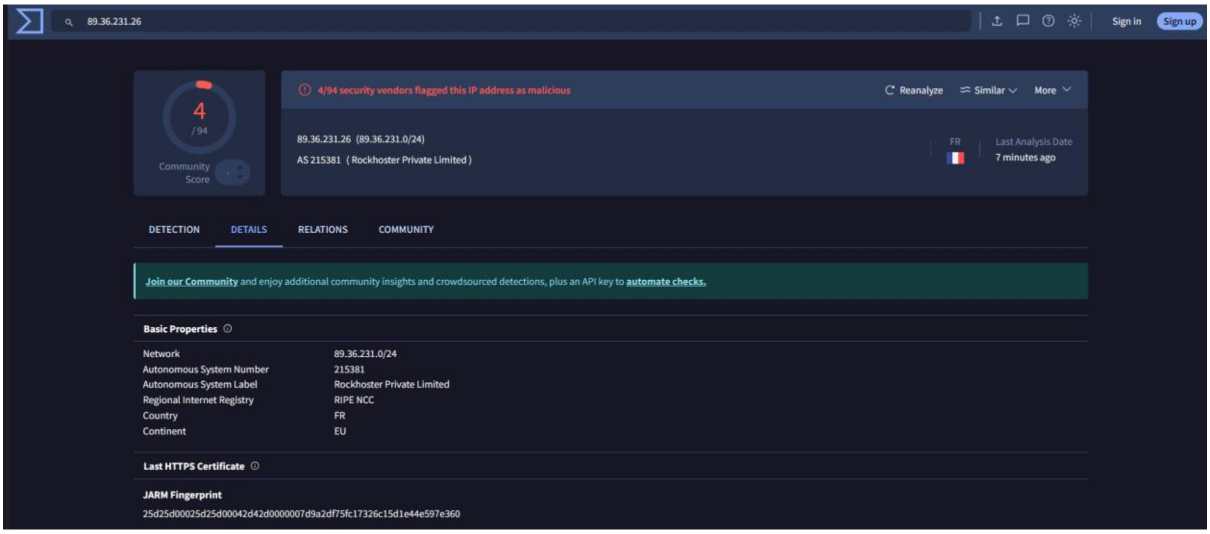
http.url	alert.signature
/index.php?ver=64&type=2	ET INFO Windows Powershell User-Agent Usage
/index.php?ver=64&type=1	ET INFO Windows Powershell User-Agent Usage
/index.php?id=&subid=xvoFAUk6	ET MALWARE Win32/Koi Stealer CnC Checkin (GET)
/sempstrywork.php	
/sempstrywork.php	
/sempstrywork.php	

3. “whois” lookup for destination IP : 89.36.231.26



```
% Abuse contact for '89.36.231.0 - 89.36.231.255' is 'abuse@rockhoster.com'

inetnum:        89.36.231.0 - 89.36.231.255
descr:          -----BEGIN TOKEN-----1338ba2b5aecb0d4ffd7e1b1d2bd4d92a2a3620e35592b42106bd11b2863d9fda858b8b144b47e0b7a
netname:        IN-ROCKHOSTER-20051129
country:        FR
org:            ORG-RPL16-RIPE
admin-c:        SD14354-RIPE
tech-c:         SD14354-RIPE
status:         ALLOCATED PA
mnt-by:         lir-in-rockhoster-1-MNT
mnt-by:         RIPE-NCC-HM-MNT
created:        2024-03-01T08:51:19Z
last-modified:  2024-03-06T22:49:12Z
source:         RIPE

organisation:   ORG-RPL16-RIPE
org-name:       ROCKHOSTER PRIVATE LIMITED
country:        IN
org-type:       LIR
address:        B1/H3, Mohan Co-operative, Mathura Rd, Industrial Area,
address:        110044
address:        New Delhi
address:        INDIA
phone:          +917711885571
admin-c:        SD14354-RIPE
tech-c:         SD14354-RIPE
abuse-c:        AR74230-RIPE
mnt-ref:        lir-in-rockhoster-1-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         lir-in-rockhoster-1-MNT
created:        2024-02-19T12:40:34Z
last-modified:  2024-02-19T12:40:34Z
source:         RIPE # Filtered

role:           Support Department
address:        INDIA
address:        New Delhi
address:        110044
address:        B1/H3, Mohan Co-operative, Mathura Rd, Industrial Area,
```

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



4/94 security vendors flagged this IP address as malicious

89.36.231.26 (89.36.231.0/24)
AS 215381 (Rockhoster Private Limited)

FR

Last Analysis Date
7 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

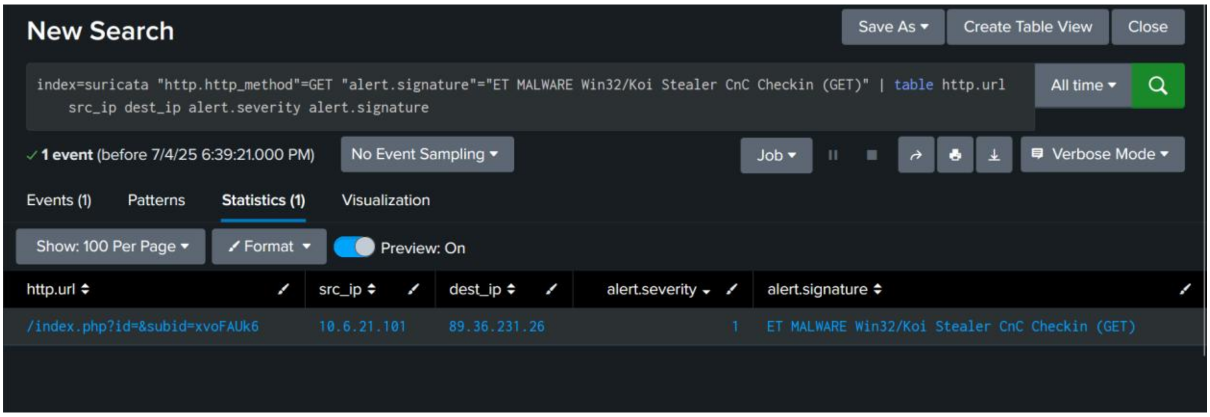
Network	89.36.231.0/24
Autonomous System Number	215381
Autonomous System Label	Rockhoster Private Limited
Regional Internet Registry	RIPE NCC
Country	FR
Continent	EU

Last HTTPS Certificate

JARM Fingerprint
25d25d00025d25d00042d42d0000007d9a2df75fc17326c15d1e44e597e360

5. 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"



```
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
```

✓ **1 event** (before 7/4/25 6:39:21.000 PM)

http.url	src_ip	dest_ip	alert.severity	alert.signature
/index.php?id=&subid=xvoFAUk6	10.6.21.101	89.36.231.26	1	ET MALWARE Win32/Koi Stealer CnC Checkin (GET)

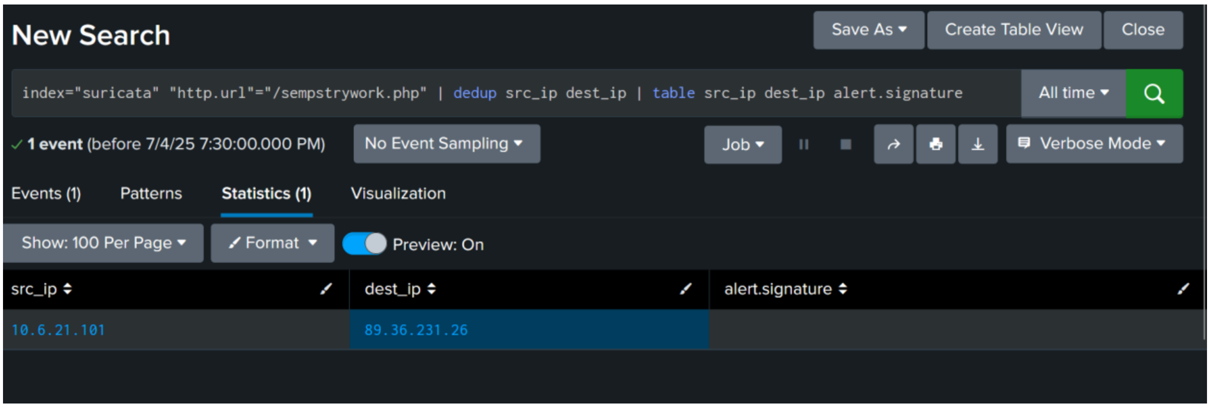
Let investigate what it is "/index.php?id=&subid=xvoFAUk6"

I got:

1. Affected product : Windows_XP_Vista_7_8_10_Server_32_64_Bit
2. Malware family: Koi-Stealer
3. Mitre Att&ck
    1. Tactic_id : TA0011
    2. Tactic_name : Command_And_Control
    3. Technique_id: T1105
    4. Technique_name : Ingree_Tool_Transfer
4. Created at : 2025_01_29
5. Source : 89.36.231.26 : 80
6. Target : 10.6.21.101 : 49575

----

6. Investigating the "/sempstrywork.php"

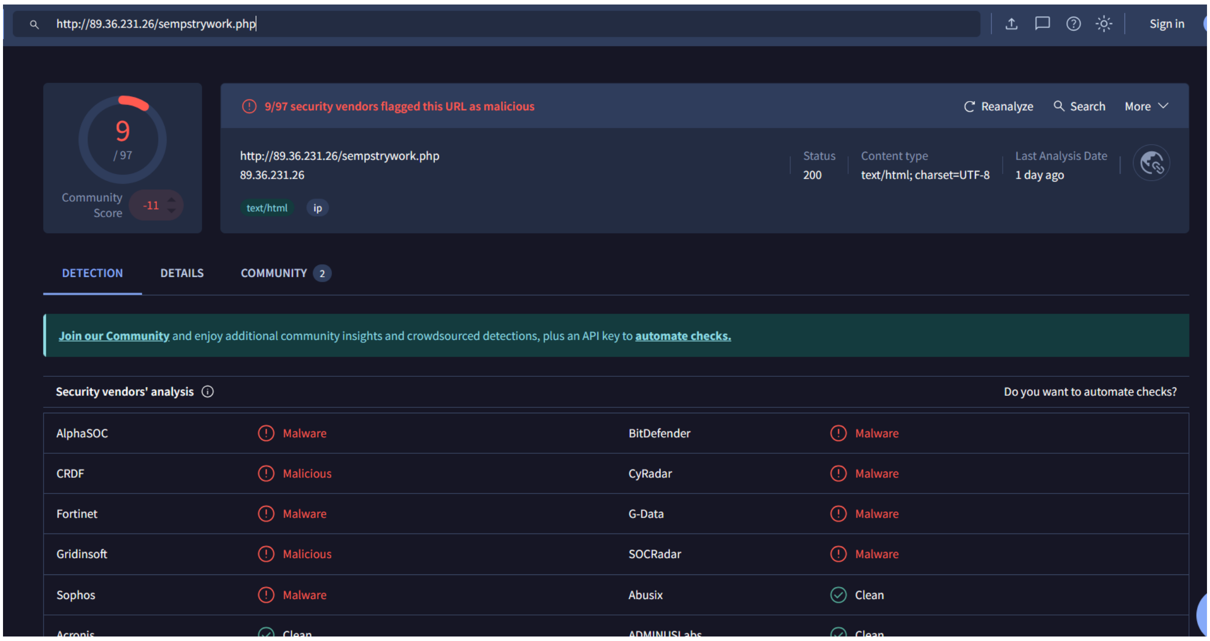


```
index="suricata" "http.url"="/sempstrywork.php" | dedup src_ip dest_ip | table src_ip dest_ip alert.signature
```

✓ **1 event** (before 7/4/25 7:30:00.000 PM)

src_ip	dest_ip	alert.signature
10.6.21.101	89.36.231.26	

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



9/97 security vendors flagged this URL as malicious

http://89.36.231.26/sempstrywork.php
89.36.231.26

Status	Content type	Last Analysis Date
200	text/html; charset=UTF-8	1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

AlphaSOC	Malware	BitDefender	Malware
CRDF	Malicious	CyRadar	Malware
Fortinet	Malware	G-Data	Malware
Gridinsoft	Malicious	SOCRadar	Malware
Sophos	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

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:

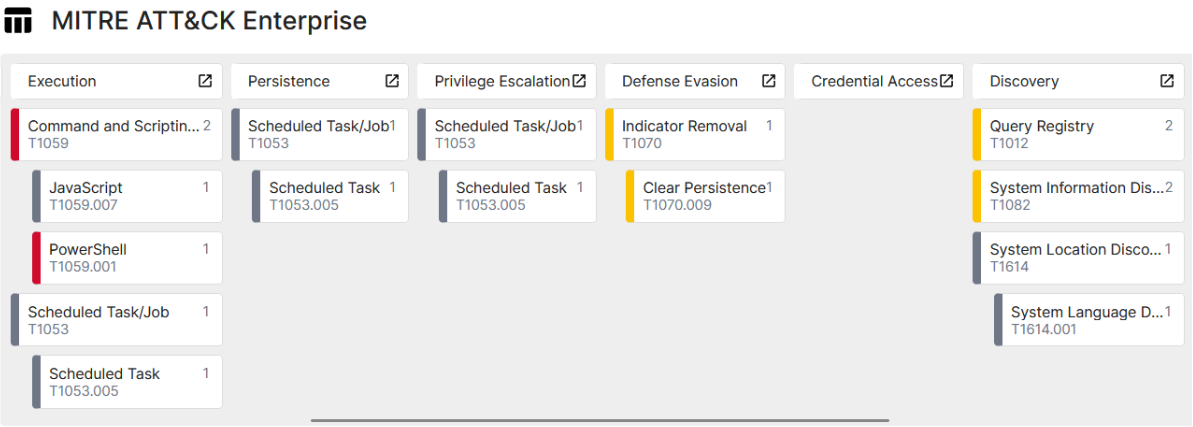
1. Suricata Alert:
   1:2059750:1 : ET MALWARE Win32/Koi Stealer CnC Checkin (GET)
   1:2059745:1 : ET ATTACK_RESPONSE Koi Loader/Stealer CnC Config Inbound
   1:2033355:1 : ET INFO Windows Powershell User-Agent Usage
   1:2221010:1 : SURICATA HTTP unable to match response to request

2. 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:

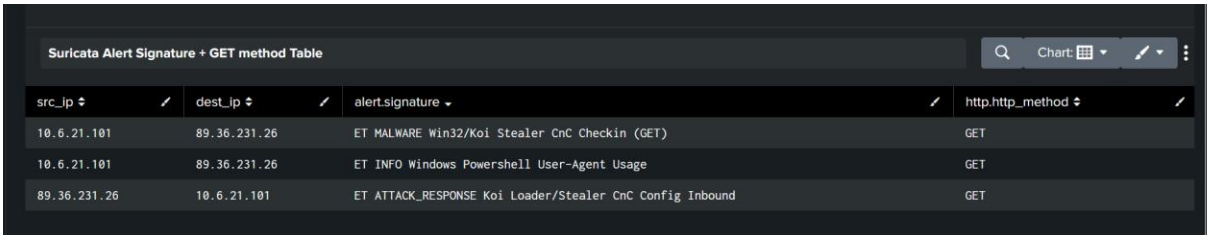
Defense Evasion	Hide Artifacts (T1564), Indirect Command Execution (T1202) Indicator Removal(T1070)
Execution	Scheduled Task/Job (T1053), Command and Scripting Interpreter (T1059)
Persistence	Scheduled Task/Job (T1053)
Privilege Escalation	Scheduled Task/Job (T1053)
Reconnaissance	Active Scanning (T1595)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



MITRE ATT&CK Enterprise

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Command and Scriptin... 2 T1059	Scheduled Task/Job 1 T1053	Scheduled Task/Job 1 T1053	Indicator Removal 1 T1070		Query Registry 2 T1012
JavaScript 1 T1059.007	Scheduled Task 1 T1053.005	Scheduled Task 1 T1053.005	Clear Persistence 1 T1070.009		System Information Dis... 2 T1082
PowerShell 1 T1059.001					System Location Disco... 1 T1614
Scheduled Task/Job 1 T1053					System Language D... 1 T1614.001
Scheduled Task 1 T1053.005					

C2 connection using the network packets
The Logs are generated by suricata



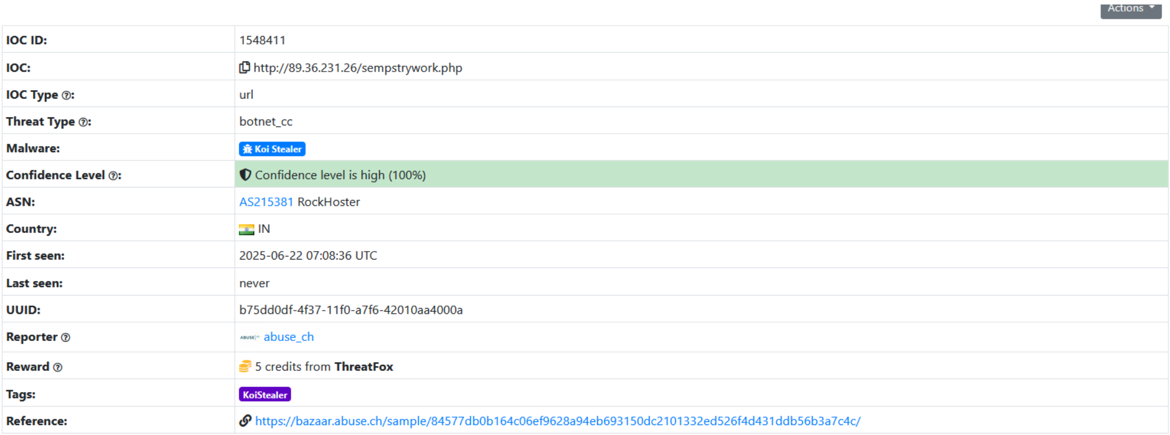
Suricata Alert Signature + GET method Table

src_ip	dest_ip	alert.signature	http.http_method
10.6.21.101	89.36.231.26	ET MALWARE Win32/Koi Stealer CnC Checkin (GET)	GET
10.6.21.101	89.36.231.26	ET INFO Windows Powershell User-Agent Usage	GET
89.36.231.26	10.6.21.101	ET ATTACK_RESPONSE Koi Loader/Stealer CnC Config Inbound	GET

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:

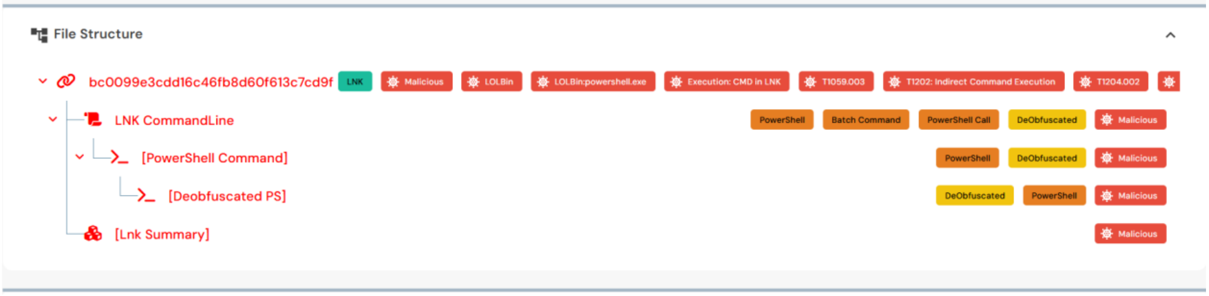
1. Spawns new processes and Dropped files for persistence
2. Accessed the ".php" file from the IP -> http://89.36.231.26/sempstrywork.php
3. Known Malware : Koi-Stealer
4. Target : Windows_XP_Vista_7_8_10_Server_32_64_Bit
5. IOC: hxxp://89.36.231.26/sempstrywork.php
6. IOC Type: url
7. Threat Type: botnet_cc
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



IOC ID:	1548411
IOC:	http://89.36.231.26/sempstrywork.php
IOC Type ⓘ:	url
Threat Type ⓘ:	botnet_cc
Malware:	Koi Stealer
Confidence Level ⓘ:	Confidence level is high (100%)
ASN:	AS215381 RockHoster
Country:	IN
First seen:	2025-06-22 07:08:36 UTC
Last seen:	never
UUID:	b75dd0df-4f37-11f0-a7f6-42010aa4000a
Reporter ⓘ	abuse_ch
Reward ⓘ	5 credits from **ThreatFox**
Tags:	KoiStealer
Reference:	https://bazaar.abuse.ch/sample/84577db0b164c06ef9628a94eb693150dc2101332ed526f4d431ddb56b3a7c4c/

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/