KRAKEN IO

Kraken IO Sentinel: **Hunting C2 Operation**

Workshop Goal:

To provide participants with a comprehensive understanding of how to effectively recognize, identify, and report on Command and Control (C2) servers using Censys.

---

1. Introduction to Command and Control (C2) Servers:

- **Definition**: Central servers utilized by attackers to manage compromised devices remotely, sending commands, and exfiltrating data.
- **Significance**:
  - A linchpin in advanced persistent threats (APTs).
  - Essential component in major cyber-espionage and cybercrime campaigns.
- **C2 Behavior**:
  - Common signs of C2 traffic in networks.
  - Typical patterns and anomalies associated with C2 communications.

---

2. Censys: The Internet's Search Engine for Security Researchers:

- **Overview**:
  - Origin and development of Censys.
  - Its critical role in the cybersecurity ecosystem.
- **Key Features**:
  - Device indexing and digital certificate tracking.
  - Observing real-time and historical network data.
  - Advanced query capabilities for pinpointing potential threats.
- **Limitations & Best Practices**:
  - Ethical considerations when using Censys.
  - Avoiding false positives and understanding rate limits.

2.5. Advanced Threat Intelligence and Fingerprinting:

- **Understanding Fingerprinting**:
  - Differentiating between device, service, and network fingerprints.
  - Importance in attribution and malware tracking.
- **Introduction to JA3S Fingerprinting**:
  - Definition: A method for creating SSL/TLS client fingerprints in an easily sharable format.
  - Significance: Enables detection of encrypted malware traffic without decryption.
  - Usage: How to incorporate JA3S in network monitoring and threat hunting.

---

3. Diving Deep into the Query Structure: **Query**: `(Directory listing for msf4) and http://services.software.vendor='Python Software Foundation'`

- **Query Components**:
  - `Directory listing for msf4`: Scours for evidence of directories or systems associated with msf4. This placeholder can be swapped with other malicious tool signatures.
  - `http://services.software.vendor='Python Software Foundation'`: Filters results to services linked to the Python Software Foundation, indicating potential service misuse or impersonation.

---

4. Expanding the Search: Identifying Malicious Infrastructure:

- **Strategy**:
  - Leveraging known malicious tool signatures.
  - Incorporating additional criteria like geolocation, associated domains, or known bad actors to refine search results.
  - Using JA3S fingerprinting to identify encrypted traffic patterns associated with malware or C2 activity.

Examples of malicious tool signatures:

1. **DarkComet**: A Remote Access Trojan (RAT) used for remote administration.
2. **njRAT**: A Remote Access Trojan originating from the Middle East, often used in cyber espionage.
3. **Emotet**: Originally a banking Trojan, it evolved into a versatile botnet.
4. **Ryuk**: Ransomware is often delivered as a payload by other malware.
5. **TrickBot**: A modular banking Trojan known to drop other malware.
6. **Nmap**: A network scanning tool for discovery and vulnerability detection.
7. **Metasploit (msf4)**: An open-source framework for developing, testing, and executing exploit code.
8. **Mimikatz**: A tool to extract plaintext passwords, hashes, and PINs from memory.
9. **Cobalt Strike**: A commercial penetration testing tool often used by attackers for its stealthy capabilities.
10. **PoisonIvy**: A famous RAT known for its customizable features.
11. **LOIC (Low Orbit Ion Cannon)**: A DoS attacking tool.
12. **HOIC (High Orbit Ion Cannon)**: An upgraded version of LOIC with more attack vectors.
13. **Hydra**: A fast and flexible password-cracking tool.
14. **John the Ripper**: Password cracking software.
15. **Gh0st RAT**: A Remote Access Tool used to control infected systems.
16. **NanoCore RAT**: A general-purpose RAT.
17. **BlackEnergy**: Malware used in a series of cyberattacks.
18. **Zeus**: A Trojan horse malware package known for stealing banking information.
19. **Stuxnet**: A worm targeting SCADA systems, notably used against Iranian nuclear facilities.
20. **Duqu**: A collection of malware discovered to be related to Stuxnet.
21. **Flame**: Advanced malware used in Middle Eastern countries for cyber espionage.
22. **Red October**: An advanced cyber-espionage campaign targeting diplomatic and governmental agencies.
23. **Carbanak**: Malware targeting banks, allowing for money transfer and manipulation of balances.
24. **Dridex**: Banking malware that steals credentials.
25. **JexBoss**: A tool for testing and exploiting JBoss application servers.
26. **PowerShell Empire**: A post-exploitation agent built on cryptologically-secure communications.
27. **BeEF (Browser Exploitation Framework)**: A penetration testing tool focusing on web browsers.
28. **SQLmap**: A tool that automates detecting and exploiting SQL injection flaws.
29. **Netcat**: Networking utility for reading and writing data across network connections.
30. **CAIN & ABEL**: Password recovery tool for Microsoft Operating Systems.
31. **APT28 (Fancy Bear tools)**: Cyber-espionage group associated with various cyber attacks.
32. **APT29 (Cozy Bear tools)**: Another cyber-espionage group known for attacks against governmental agencies.

33. **Equation Group Tools**: A collection of tools from the Equation Group linked to the NSA.
34. **Turla**: A Russian-based threat group known for its stealthy operations.
35. **FinFisher**: Governmental-grade spyware used for surveillance.
36. **Pegasus**: Mobile spyware that provides comprehensive surveillance.
37. **Regin**: Malware platform with a structure designed for espionage.
38. **EternalBlue**: An exploit developed by the NSA, later used by the WannaCry ransomware.
39. **DoublePulsar**: A backdoor implant tool developed by the NSA.
40. **BadUSB**: An attack that turns USB devices into attack platforms.
41. **NotPetya**: A ransomware strain that caused global disruptions.
42. **WannaCry**: Ransomware that exploited the EternalBlue vulnerability for propagation.
43. **Shellshock**: A family of security bugs in the Unix Bash shell.
44. **Heartbleed**: A security bug in the OpenSSL cryptography library.
45. **QuasarRAT**: An open-source RAT used in various cyber-attacks.
46. **Adwind RAT**: A cross-platform malware distributed as a service.
47. **XAgent**: Malware used by APT28, targeting multiple platforms.
48. **Destover**: Destructive malware used in the Sony Pictures attack.
49. **Blackshades**: RAT used to hijack computers and webcams.
50. **PlugX**: A remote access tool associated with Chinese APTs.
51. **Cerber**: A ransomware-as-a-service platform.
52. **XOR DDoS**: Linux-based botnet for distributed denial-of-service attacks.
53. **Sodinokibi (REvil)**: Ransomware is often spread via supply chain attacks or malspam.
54. **QakBot (QBot)**: Banking Trojan is known for its worm-like capabilities.
55. **Mirai**: Malware that turns networked devices into bots for large-scale network attacks.
56. **RATANKBA**: A banking Trojan with several variants.
57. **Havex**: Malware targeting industrial control systems.
58. **ZeroAccess**: A peer-to-peer botnet known for bitcoin mining and click fraud.
59. **IcedID**: Banking Trojan that uses web injection attacks.
60. **BazarLoader**: Malware loader known for its stealth and ability to deliver subsequent payloads.
61. **PwnyExpress**: A device that provides remote access to the user, often used for penetration testing but can be misused maliciously.
62. **Radmin**: A legitimate remote access tool often misused by attackers for unauthorized access.
63. **Buhtrap**: A group and malware known for targeting financial institutions in Russia.
64. **Bancos**: A Trojan that targets online banking users primarily in Brazil but has variants affecting other regions.
65. **Kazuar**: A multi-platform backdoor Trojan with ties to the Turla APT.
66. **Vawtrak (NeverQuest)**: Banking malware is known for its sophistication and evasion techniques.
67. **AndroRAT**: A RAT (Remote Access Tool) for Android devices.
68. **LokiBot**: An information-stealing malware that transforms into ransomware under certain conditions.
69. **Ursnif (Gozi)**: A Trojan and one of the most active banking Trojans known for stealing financial information.

70. **DanaBot**: Banking Trojan that has evolved with a range of functionalities, from keylogging to ransomware.

5. Analyst Framework: A Deep Dive into Cybersecurity Analysis

---

Introduction to the Analyst Framework:

- Definition: An organized methodology for cybersecurity professionals to detect, analyze, and respond to threats.
- Significance: Provides a structured approach to handle myriad cyber threats and incidents efficiently.

Foundations of Cybersecurity Analysis:

- **Data Collection**:
    - Sources: Network logs, endpoint telemetry, threat intelligence feeds, and external tools like Censys.
    - Importance: Establishing a broad data set for in-depth analysis.
- **Threat Identification**:
    - Techniques: Signature-based detection, behavior analytics, and anomaly detection.
    - Role of Censys: Using specific queries to identify potential C2 servers and malicious infrastructure.
- **Analysis & Investigation**:
    - Tools & Techniques: SIEM, data visualization, threat hunting platforms.
    - Correlation: Making connections between different data sources to identify patterns.

The Lifecycle of an Analyst's Investigation:

1. **Alert Triage**:
    - Initial assessment of alerts to determine urgency and potential impact.
    - Filtering out false positives.
2. **In-depth Analysis**:
    - Diving deeper into suspicious activities.
    - Using tools like Censys to gather more data about potential threats.
3. **Threat Verification**:
    - Confirming if a threat is genuine.

    - Evaluating its potential impact and severity.
4. **Response & Mitigation**:
    - Formulating and executing a plan to contain and neutralize the threat.
    - Ensuring lessons are learned for future prevention.
5. **Communication & Reporting**:
    - Keeping stakeholders informed.
    - Producing detailed reports for documentation and future reference.

Integration of External Tools with the Analyst Framework:

- **Censys**: For external threat intelligence and to identify potential malicious infrastructure.
- **Threat Intelligence Platforms**: To gather data on the latest threat actors, TTPs (Tactics, Techniques, and Procedures), and IOCs (Indicators of Compromise).
- **Endpoint Detection and Response (EDR) Tools**: To monitor endpoint activities and detect malicious activities.

Case Studies & Practical Application:

- Real-world examples of how the analyst framework has been applied to handle major cyber threats.
- Hands-on exercises for participants to apply the framework using simulated data.

6. The Art of Reporting: Crafting Comprehensive & Actionable Threat Intelligence on IP Investigation

---

Introduction to Cybersecurity Reporting on IP Investigation:

- **Definition**: A systematic document detailing the findings, implications, and recommendations from investigating suspicious IP addresses and their associated activities.
- **Significance**: Empowers organizations to proactively dissect and interpret traffic from or to suspicious IP addresses, facilitating timely response and mitigation.

Critical Components of an Effective Cybersecurity Report on IP Investigation:

1. **Title & Metadata**:
    - Setting the specific context: "IP Investigation Report: [Suspicious IP Address]."
    - Date of the investigation, lead analyst's name, and report iteration/version.
2. **Executive Summary**:
    - Brief overview of the suspicious IP: Geographical location, associated domains, known activities, etc.
    - Key takeaways for C-level executives and decision-makers.
3. **Methodology**:
    - Tools and platforms used: Censys, Wireshark, and other threat intelligence platforms.
    - Techniques: Passive DNS analysis, traffic pattern analysis, historical data review, etc.
    - Approach: Sequential steps taken from the initial flagging of the IP to the end of the investigation.
4. **Detailed Findings**:
    - **Timeline**: Chronological breakdown of the IP's activity.
    - **Associated Domains**: Any domains linked to the IP.
    - **Nature of Traffic**: Whether the IP was the source of scanning activities, involved in data exfiltration, part of a botnet, etc.
    - **Visuals**: Network graphs, pie charts (for types of traffic), tables with timestamped activities.
5. **Implications & Risk Assessment**:
    - **Potential Targets**: Systems or networks that might have been compromised or targeted.
    - **Data at Risk**: Data that could have been accessed or exfiltrated.
    - **Threat Actor Profile**: If any attribution can be made or if the IP address matches known profiles of cybercriminals or APT groups.
    - **Risk Scoring**: Using frameworks like CVSS (Common Vulnerability Scoring System) to assign a severity level.

6. **Recommendations & Action Plan**:
    - **Immediate Actions** include blocking the IP, alerting affected parties, or enhancing monitoring.
    - **Long-Term Strategies**: Enhancing network security, continuous monitoring, threat intelligence subscription, etc.
    - **Educational Recommendations**: Training modules or awareness sessions for staff to prevent future breaches.
7. **Annex & References**:
    - **Raw Data**: Logs or data extracts that provide evidence (can be redacted for sensitive info).
    - **Threat Intelligence Sources**: Cited sources, threat intelligence feeds, or databases that provided data or corroborated findings.
    - **Further Reading**: If applicable, extended studies or reports on similar incidents.

Conclusion of the IP Investigation Report:

In the ever-evolving landscape of cyber threats, IP investigation plays a pivotal role in preemptive defense. This report outlines the investigated IP's suspicious activities and provides actionable insights to fortify against future threats. We can stay one step ahead of cyber adversaries through continuous learning and vigilance.

Link:
https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=%28Directory+listing+for+cobaltstrike%29+and+services.software.vendor%3D%60Python+Software+Foundation%60

Example Report:

Critical Components of an Effective Cybersecurity Report on IP Investigation:

---

1. Title & Metadata:

- **Context**: IP Investigation Report: 43.129.239.195
- **Date**: Sep 01, 2023
- **Analyst**: Operator K.
- **Report Version**: 1.0
- **Location**: Hong Kong, Asia (Latitude: 22.27832, Longitude: 114.17469)
- **Autonomous System**: TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue (ASN: 132203)

---

2. Executive Summary:

- **IP Address**: 43.129.239.195, hosted on Ubuntu Linux 20.04.
- **Network Provider**: TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN.
- **Key Observations**: The IP showcases multiple open ports, a known malicious tool signature "cobalt strike", and several associated services. The presence of the "rikka" image-sharing service, "SimpleHTTP" with a potential beaconing file, and a TLS service linked to "cobaltstrike" are of particular concern.

---

3. Methodology:

- **Tools Used**: Censys for initial data extraction, followed by auxiliary tools for further analysis.
- **Techniques**: Passive DNS analysis, traffic pattern analysis, service probing, and JA3S fingerprinting.
- **Approach**: Initial flagging of IP based on "cobaltstrike" signature, followed by a deep dive into associated services, open ports, and related metadata.

---

4. Detailed Findings:

- **Open Ports and Services**:
  - **SSH (22)**: Used for remote administration. OpenSSH 8.2 on Ubuntu Linux 20.04 detected.
  - **DNS (53)**: Can be misused for data exfiltration or C2 operations.
  - **HTTP (80)**: Serving a default nginx page.
  - **COBALT_STRIKE Ports (4433, 9999)**: Known malicious tool signature detected.
  - **Rikka Service on Port 8080**: A personal image share system, not inherently malicious but warrants scrutiny on this IP.
  - **SimpleHTTP on Port 8999**: Directory listing reveals a file named "beacon.bin", suggesting potential beaconing activity.
  - **TLS Service on Port 61111**: TLS activity with a leaf certificate associated with "cobaltstrike" indicates potential encrypted C2 operations.

---

5. Implications & Risk Assessment:

- **Potential Targets**: The IP might have compromised or targeted systems or networks.
- **Data at Risk**: Unknown, but the presence of beaconing suggests potential exfiltration.
- **Threat Actor Profile**: The use of "cobaltstrike" and beaconing activity suggests sophisticated actors. However, exact attribution remains inconclusive.
- **Risk Scoring**: High.

---

6. Recommendations & Action Plan:

- **Immediate Actions**:
  - Block IP 43.129.239.195 at the firewall.
  - Monitor traffic for communication to/from this IP.
- **Long-Term Strategies**:
  - Improve network monitoring.
  - Regularly update threat intelligence feeds.
- **Educational Recommendations**: Organize security awareness sessions emphasizing system and software updates.

---

7. Annex & References:

- **Raw Data**: Data from Censys, detailed port and service data, and associated banners.
- **Contact Information**: qcloud_net_duty@tencent.com (Note: marked as invalid), +8613923479936 (Phone number associated with ASHEVILLE PTE LTD).
- **Network Information**: CIDR 43.129.192.0/18, Registry via APNIC.

Conclusion:

The IP 43.129.239.195 presents several red flags:

1. The presence of **"cobalt strike"** on specific ports indicates potential C2 activity.
2. The **"rikka"** service on port 8080 might be leveraged for data storage or exfiltration.
3. The **SimpleHTTP** service on port 8999, especially with the "beacon.bin", indicates potential beaconing activity.
4. The **TLS Service** on port 61111, associated with "cobaltstrike", suggests encrypted C2 operations.

Given these findings and the IP's location, it's evident that this IP poses a significant threat. Immediate actions are crucial to mitigate potential risks.