🛡️Internship Report

Intern ID: 210

Name: Sahil Anil Patil

⚒️Tool Name: Shodan

History

Shodan, an acronym for "Sentient Hyper-Optimized Data Access Network," was created by John Matherly in 2009. It was designed to be a search engine for internet-connected devices, rather than websites. The idea originated from the frustration of not being able to easily find specific types of devices or services exposed to the internet.

Description:

Shodan is a search engine that lets users find specific types of devices connected to the internet using a variety of filters. While typical search engines crawl the web, Shodan crawls the Internet's services, looking for banners and metadata from servers, routers, webcams, industrial control systems, and more. This allows it to identify open ports, services running on those ports, and even default credentials or vulnerabilities.

📌What Is This Tool About?

Shodan is fundamentally a "search engine for hackers" or, more accurately, a "search engine for the Internet of Things (IoT) and operational technology (OT)." It discovers devices based on their banners, which are metadata that servers send back to clients. These banners often reveal information about the software running, its version, and other details that can be crucial for security professionals, researchers, and penetration testers. It essentially provides a real-time inventory of internet-facing devices and services globally.

⭐Key Characteristics / Features:

- **Banner Grabbing:** Collects information from network banners to identify services and versions.
- **Device Discovery:** Locates a wide range of devices including servers, routers, cameras, and SCADA systems.
- **Filter Options:** Allows detailed searches using filters like port, country, OS, organization, and more.
- **Vulnerability Information:** Often highlights known vulnerabilities associated with discovered services.
- **Exploit Database Integration:** Links to exploit databases for identified vulnerabilities.

- **API Access:** Provides an API for programmatic access and integration with other tools.
- **Network Intelligence:** Offers insights into global network infrastructure and trends.
- **Alerting:** Can set up alerts for specific types of devices or vulnerabilities.
- **Maps:** Visualizes the geographic location of discovered devices.
- **Shodan Monitor:** A service to track an organization's own internet-facing assets.
- **Command-Line Interface (CLI):** Provides command-line access for scripting and automation.
- **Real-time Data:** Continuously scans the internet, providing up-to-date information.

🛠️Types / Modules Available:

- **Shodan Search:** The core search functionality for devices and services.
- **Shodan Exploits:** A database of exploits relevant to findings on Shodan.
- **Shodan Images:** Search for screenshots of vulnerable webcams or VNC servers.
- **Shodan Maps:** Geographical visualization of discovered devices.
- **Shodan Command Line Interface (CLI):** For direct interaction and scripting.
- **Shodan API:** For integration into custom scripts and applications.
- **Shodan Monitor:** For continuous monitoring of an organization's network perimeter.

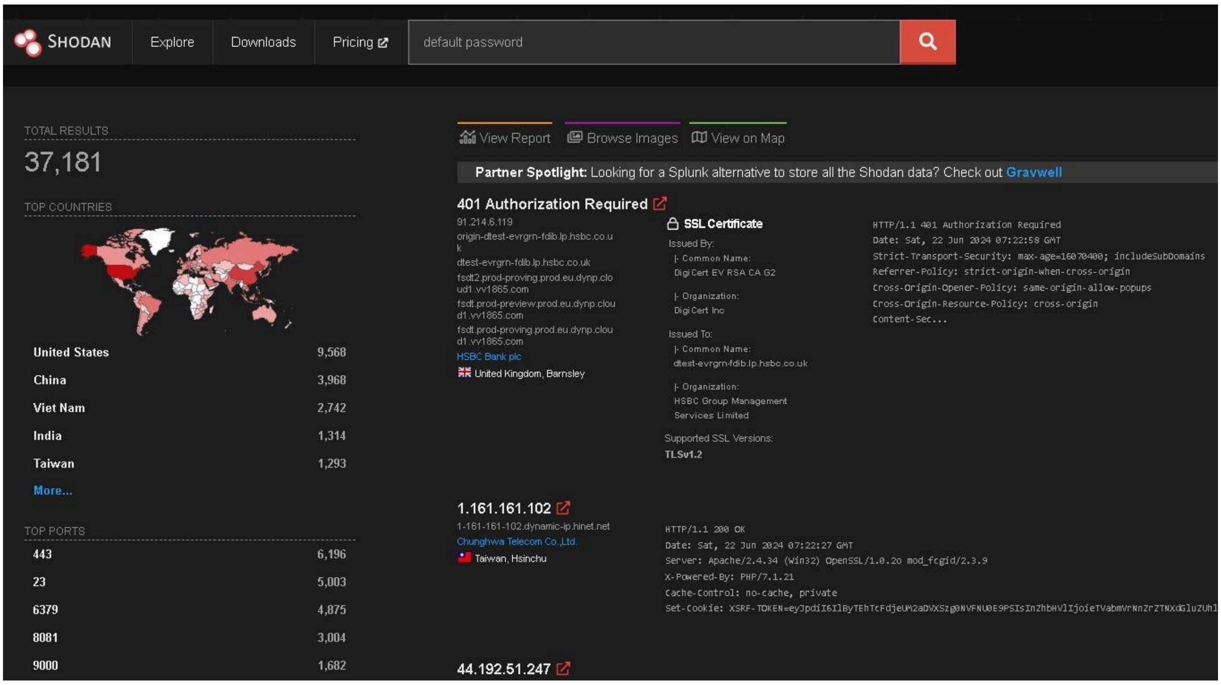
🎯How Will This Tool Help?

- **Vulnerability Assessment:** Helps identify exposed services and potential vulnerabilities in an organization's infrastructure or other targets.
- **Asset Discovery:** Maps an organization's attack surface by revealing all internet-facing devices.
- **Threat Intelligence:** Provides insights into global threat landscape, common vulnerabilities, and exposed services.
- **Compliance Auditing:** Assists in ensuring that systems comply with security policies by identifying misconfigurations.
- **Cybercrime Investigation:** Can be used to locate Command & Control (C2) servers, vulnerable devices used in botnets, or compromised systems.
- **Research:** Enables security researchers to study internet-wide trends, common misconfigurations, and the prevalence of specific technologies.
- **Penetration Testing:** Aids in reconnaissance by quickly identifying potential entry points into a target network.

📷Proof of Concept (PoC) Images: Shodan

(Insert 5 screenshots showing:

1. A Shodan search result page for a common service (e.g., "Apache" or "nginx").



TOTAL RESULTS

37,181

TOP COUNTRIES

United States	9,568
China	3,968
Viet Nam	2,742
India	1,314
Taiwan	1,293
More...	

TOP PORTS

443	6,196
23	5,003
6379	4,875
8081	3,004
9000	1,682

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

401 Authorization Required

91.214.6.119
origin-dtest-evrgrn-fdib.lp.hsbc.co.uk
dtest-evrgrn-fdib.lp.hsbc.co.uk
fsdt2.prod-proving.prod.eu.dynp.cloud1.vv1865.com
fsdt.prod-preview.prod.eu.dynp.cloud1.vv1865.com
fsdt.prod-proving.prod.eu.dynp.cloud1.vv1865.com
HSBC Bank plc
United Kingdom, Barnsley

SSL Certificate

```
Issued By:
 |- Common Name:
 Digi Cert EV RSA CA G2

 |- Organization:
 Digi Cert Inc

Issued To:
 |- Common Name:
 dtest-evrgrn-fdib.lp.hsbc.co.uk

 |- Organization:
 HSBC Group Management
 Services Limited

Supported SSL Versions:
TLSv1.2
```

```
HTTP/1.1 401 Authorization Required
Date: Sat, 22 Jun 2024 07:22:58 GMT
Strict-Transport-Security: max-age=16070400; includeSubDomains
Referrer-Policy: strict-origin-when-cross-origin
Cross-Origin-Opener-Policy: same-origin-allow-popups
Cross-Origin-Resource-Policy: cross-origin
Content-Sec...
```

1.161.161.102

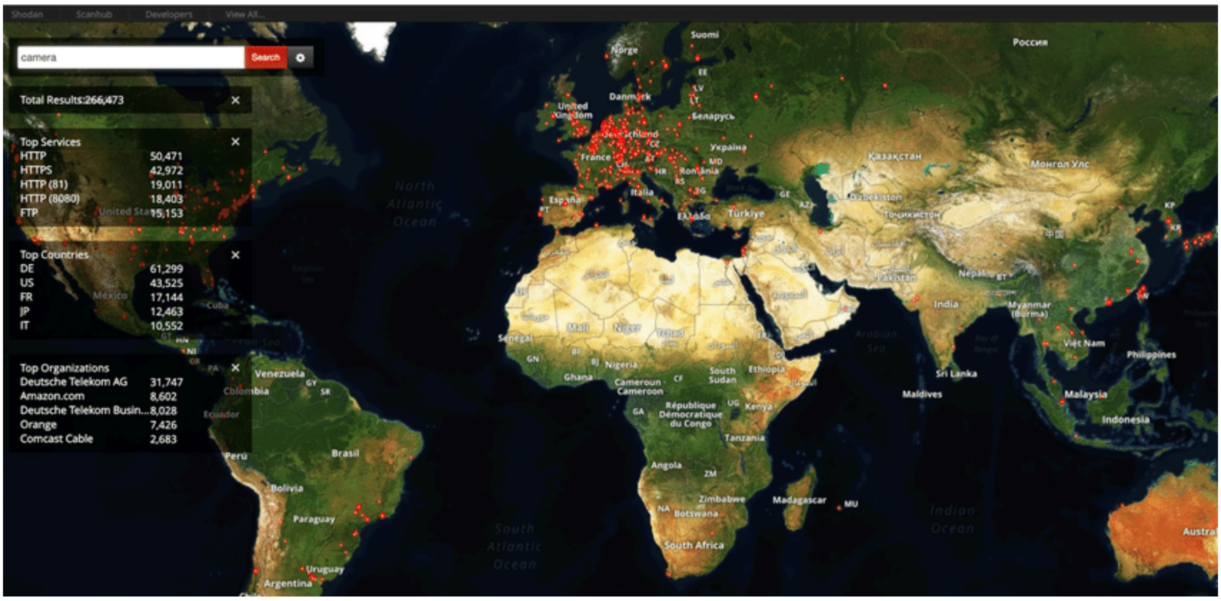
1-161-161-102.dynamic-ip.hinet.net
Chunghwa Telecom Co.,Ltd.
Taiwan, Hsinchu

```
HTTP/1.1 200 OK
Date: Sat, 22 Jun 2024 07:22:27 GMT
Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o mod_fcgid/2.3.9
X-Powered-By: PHP/7.1.21
Cache-Control: no-cache, private
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlByTEhTcFdjeUM2aDVXSzg0NVFNU0E9PSIsInZhbHVlIjoieTVabmVrNnZrZTNXdGluZUhl
```

44.192.51.247

2. A detailed view of a specific host's banner information.

3. A Shodan map showing device locations.



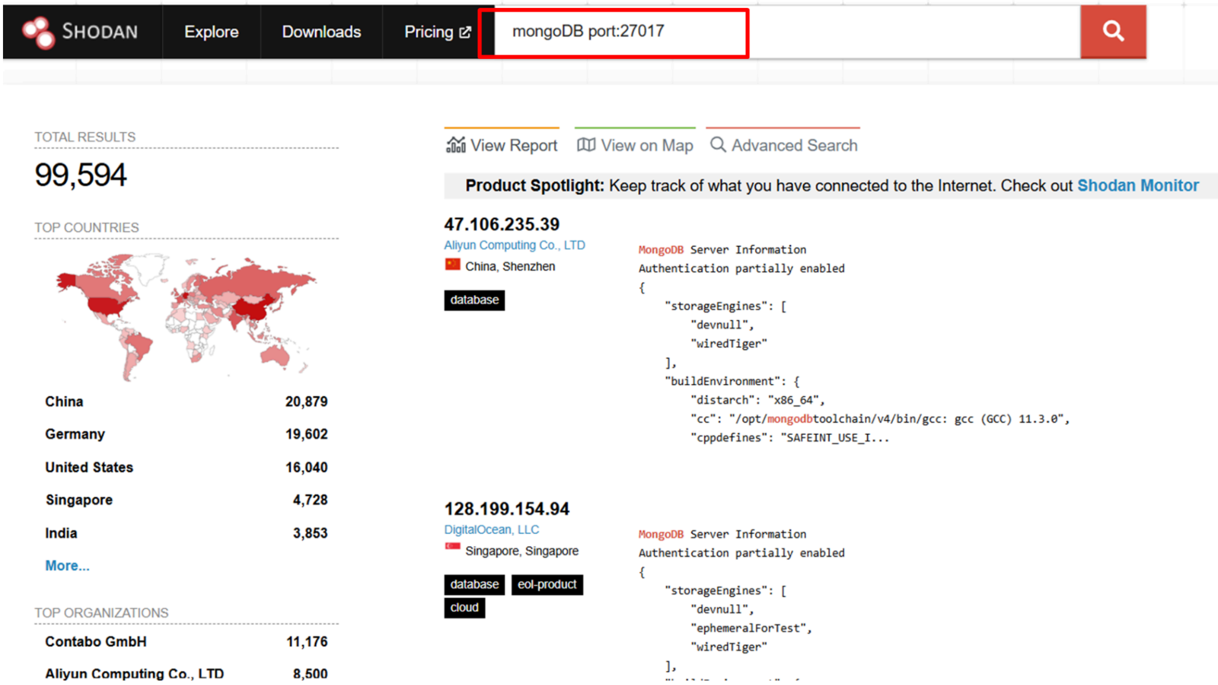
Total Results:266,473

Top Services	
HTTP	50,471
HTTPS	42,972
HTTP (81)	19,011
HTTP (8080)	18,403
FTP	15,153

Top Countries	
DE	61,299
US	43,525
FR	17,144
JP	12,463
IT	10,552

Top Organizations	
Deutsche Telekom AG	31,747
Amazon.com	8,602
Deutsche Telekom Busin...	8,028
Orange	7,426
Comcast Cable	2,683

4. A search using a filter like "port:22 country:US"



TOTAL RESULTS

99,594

TOP COUNTRIES

China	20,879
Germany	19,602
United States	16,040
Singapore	4,728
India	3,853

More...

TOP ORGANIZATIONS

Contabo GmbH	11,176
Aliyun Computing Co., LTD	8,500

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

47.106.235.39
Aliyun Computing Co., LTD
China, Shenzhen
database

```
MongoDB Server Information
Authentication partially enabled
{
    "storageEngines": [
        "devnull",
        "wiredTiger"
    ],
    "buildEnvironment": {
        "distarch": "x86_64",
        "cc": "/opt/mongodbtoolchain/v4/bin/gcc: gcc (GCC) 11.3.0",
        "cppdefines": "SAFEINT_USE_I...
```

128.199.154.94
DigitalOcean, LLC
Singapore, Singapore
database eol-product cloud

```
MongoDB Server Information
Authentication partially enabled
{
    "storageEngines": [
        "devnull",
        "ephemeralForTest",
        "wiredTiger"
    ],
```

5. A screenshot of Shodan Monitor dashboard if applicable.)

📚15-Liner Summary: Shodan

1. Indexes internet-connected devices and services.
2. Uses banner grabbing to gather information.
3. Allows searches based on various filters (port, country, OS).
4. Identifies exposed services and potential vulnerabilities.
5. Provides a comprehensive view of the internet's attack surface.
6. Offers an API for automation and integration.
7. Useful for asset discovery and vulnerability assessment.
8. Helps track C2 servers and compromised systems.
9. Can visualize device locations on a map.
10. Supports both GUI and CLI interactions.
11. Continuously scans for real-time data.
12. Offers Shodan Monitor for organizational asset tracking.
13. Valuable for penetration testers and security researchers.
14. Helps in compliance auditing by identifying misconfigurations.
15. A powerful tool for global threat intelligence.

⏱️Time to Use / Best Case Scenarios: Shodan

- **Initial Reconnaissance:** Before launching a penetration test or vulnerability scan.
- **Threat Hunting:** To identify specific types of vulnerable devices globally.
- **Incident Response:** To quickly assess external exposure of an affected organization.
- **Security Audits:** To verify proper configuration of internet-facing systems.
- **Competitive Intelligence:** To understand the technology stack of competitors.

- **When to Use During Investigation: Shodan**
- **External Attack Surface Mapping:** To understand what an attacker sees from the outside.
- **Malware Analysis:** To identify potential C2 infrastructure or distribution points.
- **Phishing Campaign Analysis:** To find servers hosting malicious content or phishing kits.
- **Compliance Checks:** To ensure no unauthorized services are exposed.

- **Supply Chain Risk Assessment:** To identify vulnerabilities in third-party services.

Best Person to Use This Tool & Required Skills: Shodan

- **Best User:** Penetration Tester / Security Analyst / Cyber Threat Intelligence Analyst
- **Required Skills:**
    - Understanding of networking concepts (ports, protocols).
    - Familiarity with common services and their banners.
    - Ability to interpret search results and identify anomalies.
    - Knowledge of common vulnerabilities (CVEs) is beneficial.
    - Basic scripting skills (e.g., Python) for API interaction is a plus.

Flaws / Suggestions to Improve: Shodan

- **Limited Deep Scanning:** Primarily relies on banner grabbing; does not perform active vulnerability exploitation.
- **False Positives/Negatives:** Can sometimes misidentify services or miss obscure ones.
- **Historical Data:** While it scans continuously, historical snapshots of specific devices might be limited.
- **Legality Concerns:** Can be misused for malicious purposes if not handled responsibly.
- **API Rate Limits:** Free API usage is limited, requiring a paid subscription for extensive use.
- **Visualization Improvements:** Could benefit from more interactive and customizable dashboards for complex queries.

Good About the Tool: Shodan

- **Comprehensive Coverage:** Scans a vast range of internet-connected devices.
- **Rich Data:** Provides detailed information beyond just open ports.
- **Ease of Use:** Intuitive search interface with powerful filtering options.
- **API Availability:** Allows for extensive automation and integration.
- **Valuable for Reconnaissance:** Excellent for initial information gathering.
- **Continuously Updated:** Provides near real-time data on internet-facing assets.

Tool Name: Malcore

History

Malcore is a more recent addition to the cybersecurity toolset, focusing on automating the analysis of malicious files and URLs. It's built to streamline the often-complex process of malware analysis, providing rapid insights into potential threats without requiring deep technical expertise from the user. Its development stems from the increasing volume and sophistication of malware, necessitating quicker and more accessible analysis capabilities.

Description:

Malcore is an automated malware analysis platform that provides in-depth reports on suspicious files, URLs, and network indicators. It leverages a combination of static and dynamic analysis techniques to identify malicious behaviors, network communications, and artifact drops. Its primary goal is to provide actionable intelligence for security professionals to quickly assess and respond to threats.

What Is This Tool About?

Malcore is essentially a sandboxing and threat intelligence platform rolled into one. When a suspicious file or URL is submitted, Malcore executes it in a controlled virtual environment (sandbox) to observe its behavior. It then collects various indicators of compromise (IOCs) such as network connections, dropped files, registry modifications, and process injections. This behavioral analysis is combined with static analysis (examining the file's structure without execution) and often integrates with external threat intelligence feeds to provide a comprehensive risk assessment and detailed report.

Key Characteristics / Features:

- **Automated Sandbox Analysis:** Executes suspicious files/URLs in a safe environment.
- **Static Analysis:** Examines file properties, headers, strings, and metadata without execution.
- **Dynamic Analysis:** Monitors runtime behavior (network activity, file system changes, process creation).
- **IOC Extraction:** Automatically extracts Indicators of Compromise (IPs, domains, hashes, URLs).
- **Threat Scoring:** Provides a risk score or verdict on the analyzed sample.
- **Detailed Reports:** Generates comprehensive reports with timelines, network graphs, and system changes.
- **API Integration:** Offers an API for automated submission and retrieval of analysis results.
- **URL Analysis:** Scans URLs for malicious content, redirects, and phishing indicators.
- **File Type Support:** Supports various file formats (PE, PDF, Office documents, scripts).
- **Network Traffic Analysis (PCAP):** Captures and analyzes network traffic generated during execution.
- **Screenshot Capture:** Takes screenshots of the sandboxed environment during execution.
- **Memory Dumps:** Can provide memory dumps for deeper forensic analysis.
- **Community/Private Sandboxing:** May offer options for public or private analysis environments.
- **YARA Rule Detection:** Identifies samples matching specific YARA rules.

Types / Modules Available:

- **File Analysis Module:** For submitting and analyzing suspicious executable files, documents, etc.
- **URL Analysis Module:** For analyzing potentially malicious web links.
- **Network Indicator Analysis:** For investigating IPs, domains, and hash values.
- **Threat Intelligence Feed Integration:** Connects with external sources for enriched data.
- **Reporting Module:** Generates and presents analysis results in various formats.
- **API Module:** For programmatic interaction and integration into security workflows.

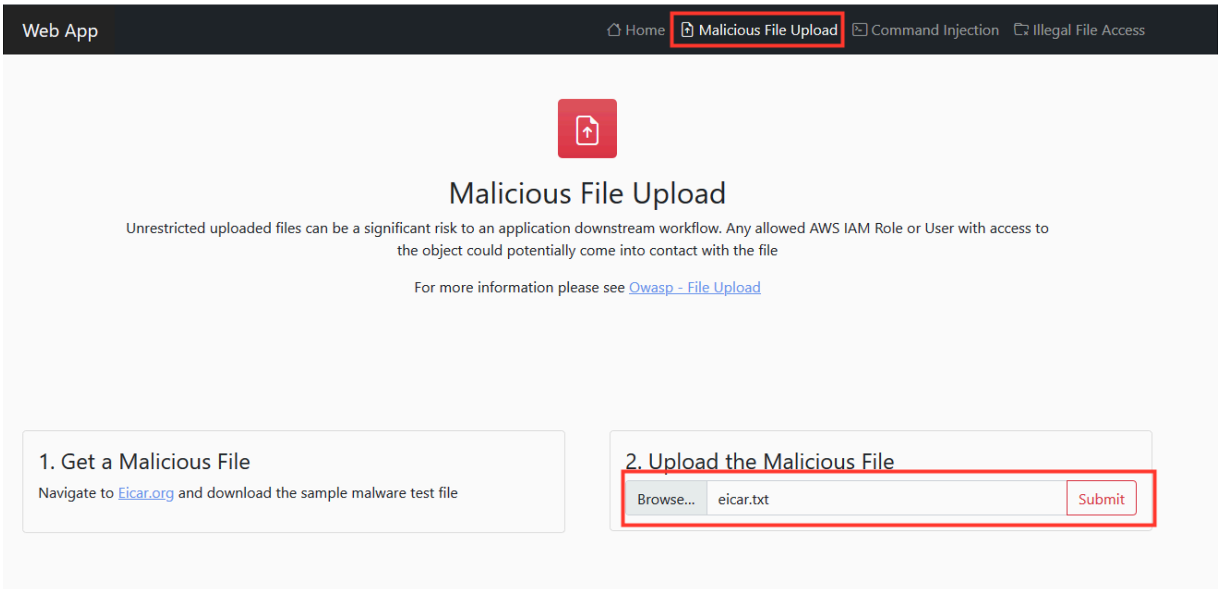
How Will This Tool Help?

- **Rapid Malware Triage:** Quickly determines if a file or URL is malicious, speeding up incident response.
- **Threat Intelligence Generation:** Provides actionable IOCs and behavioral insights into new threats.
- **Security Operations Efficiency:** Automates a significant portion of malware analysis, freeing up analysts.
- **Phishing Detection:** Analyzes suspicious URLs and attachments in phishing campaigns.
- **Vulnerability Exploitation Analysis:** Helps understand the behavior of exploits and their payloads.
- **Incident Response Support:** Provides critical data for containment, eradication, and recovery efforts.
- **Malware Research:** Aids researchers in understanding new malware families and attack techniques.
- **Automated Investigations:** Can be integrated into SIEM or SOAR platforms for automated alert enrichment.

Proof of Concept (PoC) Images: Malcore

(Insert 5 screenshots showing:

1. The Malcore submission interface (upload file/paste URL)



Web App

Home | Malicious File Upload | Command Injection | Illegal File Access

Malicious File Upload

Unrestricted uploaded files can be a significant risk to an application downstream workflow. Any allowed AWS IAM Role or User with access to the object could potentially come into contact with the file

For more information please see Owasp - File Upload

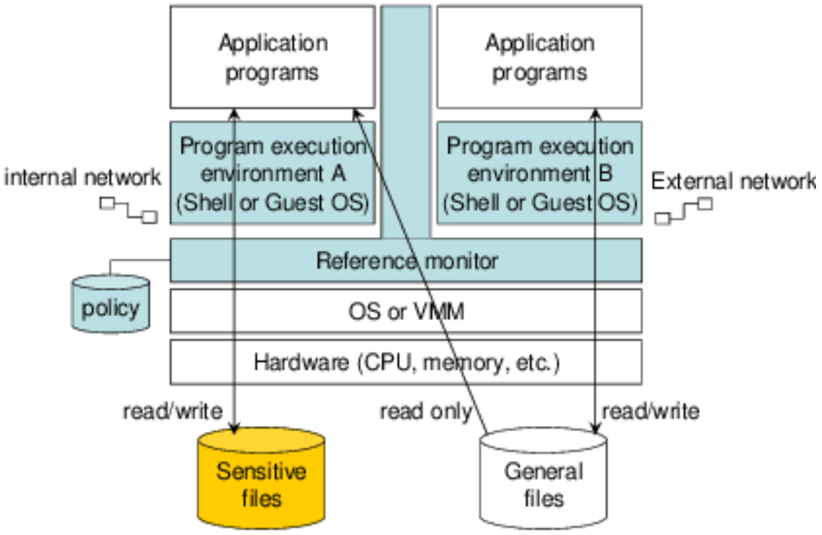
1. Get a Malicious File

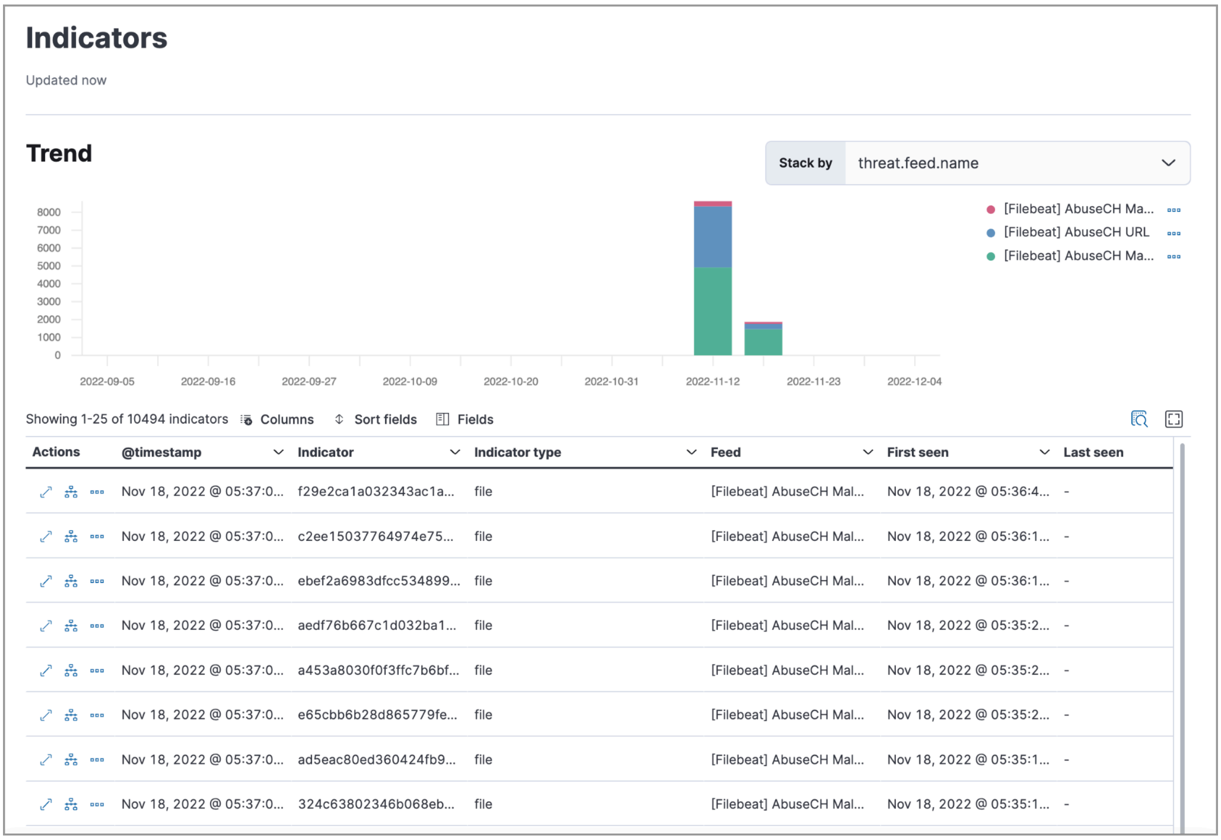
Navigate to Eicar.org and download the sample malware test file

2. Upload the Malicious File

Browse... eicar.txt Submit

2. A summary report page after a file analysis, showing verdict and key IOCs.





Indicators

Updated now

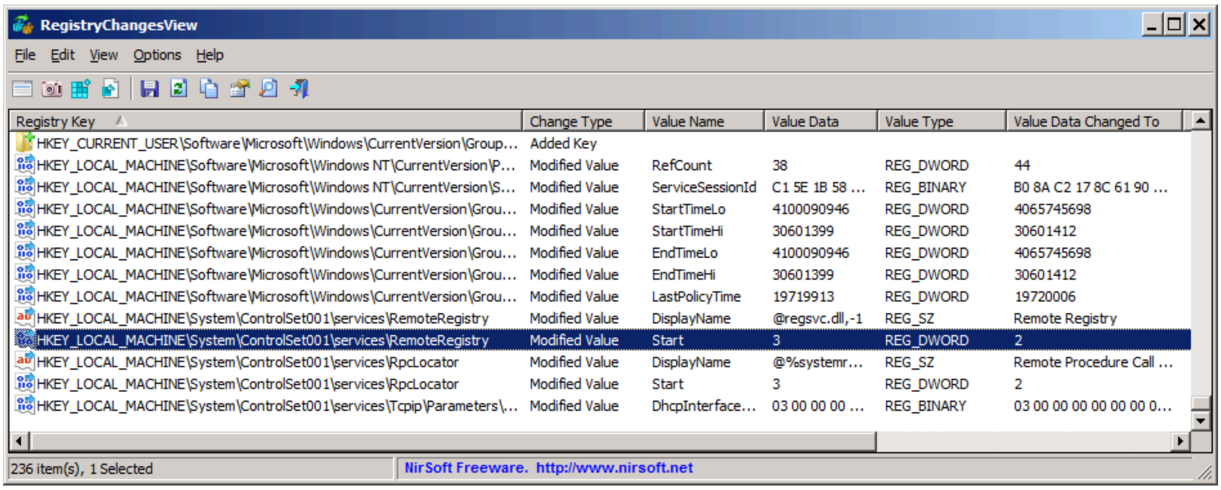
Trend

Stack by: threat.feed.name

Showing 1-25 of 10494 indicators   Columns   Sort fields   Fields

Actions	@timestamp	Indicator	Indicator type	Feed	First seen	Last seen
	Nov 18, 2022 @ 05:37:0...	f29e2ca1a032343ac1a...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:36:4...	-
	Nov 18, 2022 @ 05:37:0...	c2ee15037764974e75...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:36:1...	-
	Nov 18, 2022 @ 05:37:0...	ebef2a6983dfcc534899...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:36:1...	-
	Nov 18, 2022 @ 05:37:0...	aedf76b667c1d032ba1...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:35:2...	-
	Nov 18, 2022 @ 05:37:0...	a453a8030f0f3ffc7b6bf...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:35:2...	-
	Nov 18, 2022 @ 05:37:0...	e65cbb6b28d865779fe...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:35:2...	-
	Nov 18, 2022 @ 05:37:0...	ad5eac80ed360424fb9...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:35:1...	-
	Nov 18, 2022 @ 05:37:0...	324c63802346b068eb...	file	[Filebeat] AbuseCH Mal...	Nov 18, 2022 @ 05:35:1...	-

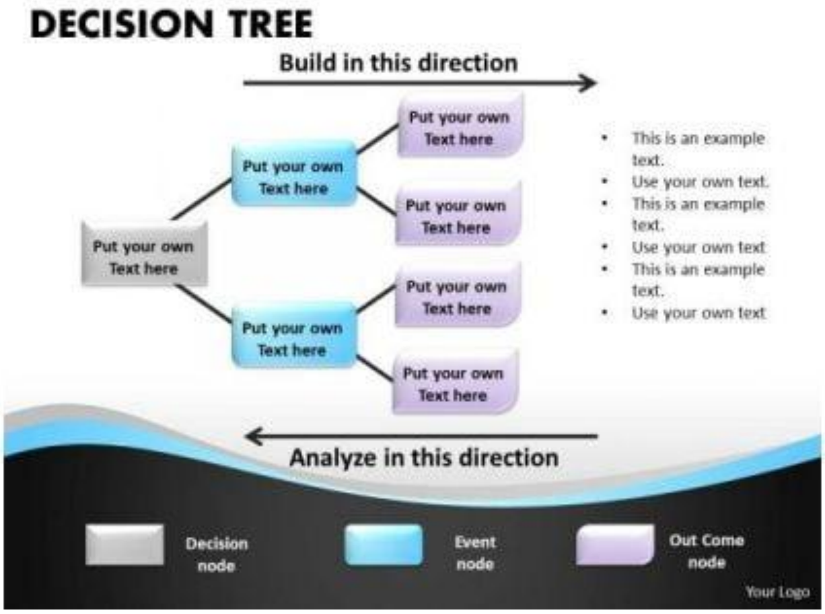
3. A detailed view of network connections made during sandbox execution.
4. A screenshot of system changes (registry, files) identified.



Registry Key	Change Type	Value Name	Value Data	Value Type	Value Data Changed To
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group...	Added Key				
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\P...	Modified Value	RefCount	38	REG_DWORD	44
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\S...	Modified Value	ServiceSessionId	C1 5E 1B 58 ...	REG_BINARY	B0 8A C2 17 8C 61 90 ...
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	StartTimeLo	4100090946	REG_DWORD	4065745698
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	StartTimeHi	30601399	REG_DWORD	30601412
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	EndTimeLo	4100090946	REG_DWORD	4065745698
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	EndTimeHi	30601399	REG_DWORD	30601412
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Grou...	Modified Value	LastPolicyTime	19719913	REG_DWORD	19720006
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RemoteRegistry	Modified Value	DisplayName	@regsvc.dll,-1	REG_SZ	Remote Registry
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RemoteRegistry	Modified Value	Start	3	REG_DWORD	2
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RpcLocator	Modified Value	DisplayName	@%systemr...	REG_SZ	Remote Procedure Call ...
HKEY_LOCAL_MACHINE\System\ControlSet001\services\RpcLocator	Modified Value	Start	3	REG_DWORD	2
HKEY_LOCAL_MACHINE\System\ControlSet001\services\Tcpip\Parameters\...	Modified Value	DhcpInterface...	03 00 00 00 ...	REG_BINARY	03 00 00 00 00 00 00 0...

236 item(s), 1 Selected   NirSoft Freeware. http://www.nirsoft.net

5. A view of the process tree or timeline generated during analysis.)



15-Liner Summary: Malcore

1. Automates static and dynamic malware analysis.
2. Executes suspicious files/URLs in a sandbox.
3. Extracts Indicators of Compromise (IOCs).
4. Provides detailed analysis reports.
5. Supports various file types and URLs.
6. Captures network traffic (PCAP).
7. Generates threat scores and verdicts.
8. Offers API for automation and integration.
9. Aids in rapid malware triage.
10. Enhances threat intelligence capabilities.
11. Improves SOC efficiency by automating analysis.
12. Useful for phishing and exploit analysis.
13. Captures screenshots of execution environment.
14. Supports both community and private analysis.
15. Crucial for incident response and malware research.

Time to Use / Best Case Scenarios: Malcore

- **During Incident Triage:** When an alert is triggered about a suspicious file or URL.
- **Email Analysis:** To safely analyze suspicious attachments or links in emails.
- **Threat Intelligence Gathering:** To understand new malware samples and extract IOCs.
- **Endpoint Detection & Response (EDR) Alerts:** To get quick insights into suspicious executables.
- **Security Awareness Training:** To demonstrate malware behavior safely.

When to Use During Investigation: Malcore

- **Initial Malware Analysis:** To determine the nature and capabilities of a suspicious sample.
- **Phishing Incident Response:** To analyze malicious links or attached documents.
- **Compromise Assessment:** To investigate suspicious files found on compromised systems.
- **IOC Enrichment:** To extract and validate IOCs from unknown threats.
- **Post-Breach Analysis:** To understand the specific TTPs (Tactics, Techniques, and Procedures) of malware used.

Best Person to Use This Tool & Required Skills: Malcore

- **Best User:** Malware Analyst / SOC Analyst / Incident Responder
- **Required Skills:**
  - Basic understanding of malware types and behaviors.
  - Familiarity with network protocols and common artifacts.
  - Ability to interpret analysis reports and identify relevant IOCs.
  - Knowledge of common operating system internals is beneficial.
  - Understanding of threat intelligence concepts.

Flaws / Suggestions to Improve: Malcore

- **Evasion Techniques:** Sophisticated malware can sometimes detect and evade sandbox environments.
- **Zero-Day Exploits:** May not fully understand or detect truly novel, unknown threats without specific signatures.
- **Context Limitations:** Sandbox analysis might not capture the full attack chain if it relies on specific environmental factors not present in the sandbox.
- **Resource Intensive:** Running many complex analyses can be resource-intensive for the platform.
- **Data Privacy Concerns:** Public sandboxes mean submitted samples are accessible to others.
- **Limited Customization:** Sandbox environment might not be fully customizable to replicate specific target environments.

Good About the Tool: Malcore

- **Automation:** Significantly reduces manual effort in malware analysis.
- **Speed:** Provides rapid analysis results, crucial for time-sensitive incidents.
- **Detailed Reports:** Offers comprehensive and easy-to-understand insights.
- **Actionable IOCs:** Directly provides valuable indicators for detection and blocking.
- **Accessibility:** Lowers the barrier to entry for malware analysis.
- **Safe Environment:** Allows for safe execution of potentially dangerous files.