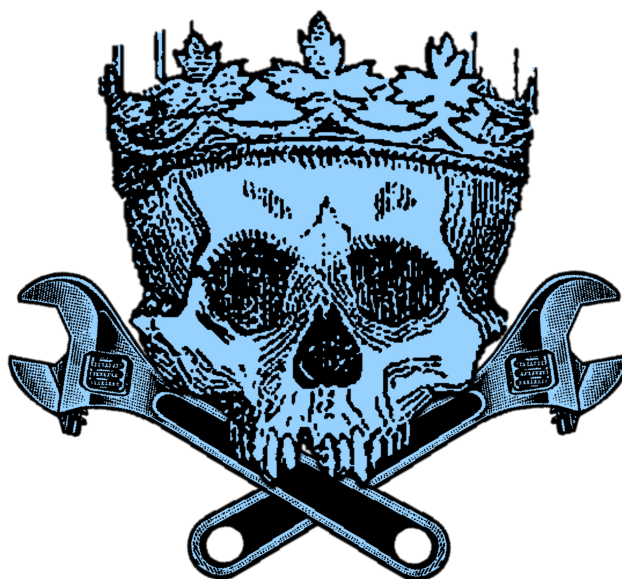


# BlueTeam-Tools

---



This github repository contains a collection of **65+ tools** and **resources** that can be useful for **blue teaming activities**.

Some of the tools may be specifically designed for blue teaming, while others are more general-purpose and can be adapted for use in a blue teaming context.

## Tool List

---

### ▼ Blue Team Tips 4 tips

- [Payload extraction with Process Hacker](#) @embee\_research
- [Prevent Script Execution via Double Click](#) Default Application GPO Change
- [Detect Cryptojacking Malware with Proxy Logs](#) Dave Mckay
- [Remove null bytes in CyberChef malware analysis](#) @Securityinbits

### ▼ Network Discovery and Mapping 6 tools

- [Nmap](#) Network scanner
- [Nuclei](#) Vulnerability scanner
- [Masscan](#) Fast network scanner
- [Angry IP Scanner](#) IP/port scanner
- [ZMap](#) Large network scanner
- [Shodan](#) Internet facing asset search engine

## ▼ Vulnerability Management 4 tools

- [OpenVAS](#) *Open-source vulnerability scanner*
- [Nessus Essentials](#) *Vulnerability scanner*
- [Nexpose](#) *Vulnerability management tool*
- [HackerOne](#) *Bug Bounty Management Platform*

## ▼ Security Monitoring 10 tools

- [Sysmon](#) *System Monitor for Windows*
- [Kibana](#) *Data visualization and exploration*
- [Logstash](#) *Data collection and processing*
- [parsedmarc](#) *Email DMARC data visualisation*
- [Phishing Catcher](#) *Phishing catcher using Certstream*
- [maltrail](#) *Malicious traffic detection system*
- [AutorunsToWinEventLog](#) *Windows AutoRuns Event Parser*
- [procfilter](#) *YARA-integrated process denial framework*
- [velociraptor](#) *Endpoint visibility and collection tool*
- [SysmonSearch](#) *Sysmon event log visualisation*

## ▼ Threat Tools and Techniques 11 tools

- [lolbas-project.github.io](#) *Living Off The Land Windows Binaries*
- [gtfobins.github.io](#) *Living Off The Land Linux Binaries*
- [filesec.io](#) *Attacker file extensions*
- [KQL Search](#) *KQL query aggregator*
- [Unprotect Project](#) *Malware evasion techniques knowledge base*
- [chainsaw](#) *Fast Windows Forensic Artefacts Searcher*
- [freq](#) *Domain generation algorithm malware detection*
- [yarGen](#) *YARA rule generator*
- [EmailAnalyzer](#) *Suspicious emails analyser*
- [VCG](#) *Code security scanning tool*
- [CyberChef](#) *GCHQ online data manipulation platform*

## ▼ Threat Intelligence 4 tools

- [Maltego](#) *Threat Intelligence Platform*
- [MISP](#) *Malware Information Sharing Platform*
- [ThreatConnect](#) *Threat data aggregation*
- [Adversary Emulation Library](#) *An open library of adversary emulation plans*

### ▼ Incident Response Planning 5 tools

- [NIST Cybersecurity Framework](#)
- [Incident Response Plan Framework](#) Framework for incident response
- [Ransomware Response Plan Framework](#) Framework for ransomware response
- [Incident Response Reference Guide](#) Incident preparation guidance paper
- [Awesome Incident Response](#) List of tools for incident response

### ▼ Malware Detection and Analysis 11 tools

- [VirusTotal](#) Malicious IOC Sharing Platform
- [IDA](#) Malware disassembler and debugger
- [Ghidra](#) Malware reverse engineering tool
- [decode-vbe](#) Encoded VBE script decoder
- [pafish](#) Virtual machine sandbox detector
- [lookyloo](#) Phishing domain mapping
- [YARA](#) Malware identification via pattern matching
- [Cuckoo Sandbox](#) Malware analysis sandbox
- [Radare2](#) Reverse engineering framework
- [dnSpy](#) .NET debugger and assembly editor
- [malware-traffic-analysis.net](#) Malware and packet capture samples

### ▼ Data Recovery 3 tools

- [Recuva](#) File recovery
- [Extundelete](#) Ext3 or ext4 partition recovery
- [TestDisk](#) Data Recovery

### ▼ Digital Forensics 3 tools

- [SANS SIFT](#) Forensic toolkit
- [The Sleuth Kit](#) Disk images analysis tools
- [Autopsy](#) Digital forensics platform

### ▼ Security Awareness Training 3 tools

- [TryHackMe](#) Cyber security challenges platform
- [HackTheBox](#) Cyber security challenges platform
- [PhishMe](#) Phishing training

### ▼ Communication and Collaboration 2 tools

- [Twitter Cyber Security Accounts](#)
- [Facebook TheatExchange](#) Malicious indicators sharing platform

# Blue Team Tips

Learn from Blue Teamers with a collection of Blue Teaming Tips. These tips cover a range of tactics, tools, and methodologies to improve your blue teaming abilities.

## BACK Payload extraction with Process Hacker

The image consists of four screenshots illustrating a malware analysis workflow:

- Top Left:** Process Hacker window showing a list of processes. A red box highlights `installutil.exe` with the annotation: "This process was spawned by malware.exe." An arrow points to the process name.
- Top Right:** Properties window for `installutil.exe`, with the `.NET assemblies` tab selected. A red box highlights the assembly list, with the annotation: "an assembly which looks different to the".
- Bottom Left:** DnSpy window showing the `test.exe` process. A red box highlights the `installutil.exe` module in the Modules list. Annotations include: "debug => attach to process", "view modules", "right click on module name", and "Open Module from memory".
- Bottom Right:** DnSpy window showing the `Program.cs` code. A red box highlights the `Test` method. An annotation states: "test -> right click -> go to entry point Reveals that the 'test' module is async and was injected into the installutil.exe process".

**Description:** 'Malware Analysis Tip - Use Process Hacker to watch for suspicious .NET assemblies in newly spawned processes. Combined with DnSpy - it's possible to locate and extract malicious payloads without needing to manually de-obfuscate.'

**Credit:** @embee\_research

**Link:** [Twitter](#)

## BACK Prevent Script Execution via Double Click



## File Extension Behavior Override

Data collected on: 5/10/2016 12:46:43 PM

[show all](#)

### Computer Configuration (Enabled)

[hide](#)

No settings defined.

### User Configuration (Enabled)

[hide](#)

#### Preferences

[hide](#)

#### Control Panel Settings

[hide](#)

#### Folder Options

[hide](#)

Open With (Extension: js, Program: %windir%\system32\notepad.exe)

[show](#)

Open With (Extension: hta, Program: %windir%\system32\notepad.exe)

[hide](#)

hta (Order: 2)

[hide](#)

#### General

[hide](#)

Action

Replace

#### Properties

File Extension

hta

Associated Program

%windir%\system32\notepad.exe

Set as default

Enabled

#### Common

[show](#)

**Description:** *On Windows, it's common to see threat actors achieve initial execution via malicious script files masquerading as Microsoft Office files. A nice way to prevent this attack chain is to alter the default application associated with these files (HTA, JS, VBA, VBS) to notepad.exe. Now when a user is successfully tricked into clicking a HTA file on disk it will open the script in notepad and execution will not occur.*

**Credit:** [bluesoul](#)

**Link:** [Blog](#)

## Detect Cryptojacking Malware with Proxy Logs

**Description:** *Cryptojacking malware is becoming more sophisticated, with mining malware leveraging DLL sideloading to hide on machine and reducing CPU load to stay below detection thresholds. One thing they all have in common is they have to make connections to mining pools, this is where we can find them. Monitor your proxy and DNS logs for connections containing common mining pool strings (e.g \*xmr.\* OR \*pool.com OR \*pool.org OR pool.\*).*

**Credit:** [Dave Mckay](#)

**Link:** [Blog](#)

## Remove null bytes in CyberChef malware analysis



Nmap (short for Network Mapper) is a free and open-source network scanner tool used to discover hosts and services on a computer network, and to probe for information about their characteristics.

It can be used to determine which ports on a network are open and what services are running on those ports. Including the ability to identify security vulnerabilities on the network.

### Install:

You can download the latest release from [here](#).

### Usage:

```
# Scan a single IP
```

```
nmap 192.168.1.1
```

```
# Scan a range
```

```
nmap 192.168.1.1-254
```

```
# Scan targets from a file
```

```
nmap -iL targets.txt
```

```
# Port scan for port 21
```

```
nmap 192.168.1.1 -p 21
```

```
# Enables OS detection, version detection, script scanning, and traceroute
```

```
nmap 192.168.1.1 -A
```

Nice usage [cheat sheet](#).

```
root@montsegur:/# nmap -O 192.168.43.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-01 14:06 -03
Nmap scan report for 192.168.43.1
Host is up (0.0077s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 4C:DD:31:DD:61:B3 (Unknown)
Device type: phone
Running: Google Android 5.X|6.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:linux:linux_kernel:3.4
OS details: Android 5.0 - 6.0.1 (Linux 3.4)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.78 seconds
root@montsegur:/# █
```

\*Image used from <https://tinyurl.com/27q22bn3>

← **Nuclei**  
BACK

A specialized tool designed to automate the process of detecting vulnerabilities in web applications, networks, and infrastructure.

Nuclei uses pre-defined templates to probe a target and identify potential vulnerabilities. It can be used to test a single host or a range of hosts, and can be configured to run a variety of tests to check for different types of vulnerabilities.

### Install:

```
git clone https://tinyurl.com/2cym9dd4 \
cd nuclei/v2/cmd/nuclei; \
go build; \
mv nuclei /usr/local/bin/; \
nuclei -version;
```

### Usage:

```
# All the templates gets executed from default template installation path.
nuclei -u https://tinyurl.com/peakb

# Custom template directory or multiple template directory
nuclei -u https://tinyurl.com/peakb -t cves/ -t exposures/

# Templates can be executed against list of URLs
nuclei -list http_urls.txt
```





```
sudo apt install masscan
```

## Install: (Git)

```
sudo apt-get install clang git gcc make libpcap-dev  
git clone https://tinyurl.com/ote7r3g  
cd masscan  
make
```

## Usage:

```
# Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/  
masscan -p22,80,445 192.168.1.0/24
```

```
# Scan a class B subnet for ports 22 through 25  
masscan 10.11.0.0/16 -p22-25
```

```
# Scan a class B subnet for the top 100 ports at 100,000 packets per second  
masscan 10.11.0.0/16 --top-ports 100 --rate 100000
```

```
# Scan a class B subnet, but avoid the ranges in exclude.txt  
masscan 10.11.0.0/16 --top-ports 100 --excludefile exclude.txt
```

```
root@kali:~# masscan 216.58.196.0/24 -p80,443  
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-02-03 04:07:46 GMT  
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth  
Initiating SYN Stealth Scan  
Scanning 256 hosts [2 ports/host]  
Discovered open port 80/tcp on 216.58.196.12  
Discovered open port 80/tcp on 216.58.196.104  
Discovered open port 443/tcp on 216.58.196.52  
Discovered open port 80/tcp on 216.58.196.209  
Discovered open port 80/tcp on 216.58.196.69  
Discovered open port 443/tcp on 216.58.196.48  
Discovered open port 443/tcp on 216.58.196.50  
Discovered open port 80/tcp on 216.58.196.210  
Discovered open port 80/tcp on 216.58.196.57  
Discovered open port 80/tcp on 216.58.196.193  
Discovered open port 443/tcp on 216.58.196.249  
Discovered open port 80/tcp on 216.58.196.46  
Discovered open port 80/tcp on 216.58.196.130  
Discovered open port 80/tcp on 216.58.196.136  
Discovered open port 443/tcp on 216.58.196.87  
Discovered open port 80/tcp on 216.58.196.6
```

\*Image used from <https://tinyurl.com/25wtpva6>

## ← BACK Angry IP Scanner

A free and open-source tool for scanning IP addresses and ports.

It's a cross-platform tool, designed to be fast and easy to use, and can scan an entire network or a range of IP addresses to find live hosts.

Angry IP Scanner can also detect the hostname and MAC address of a device, and can be used to perform basic ping sweeps and port scans.

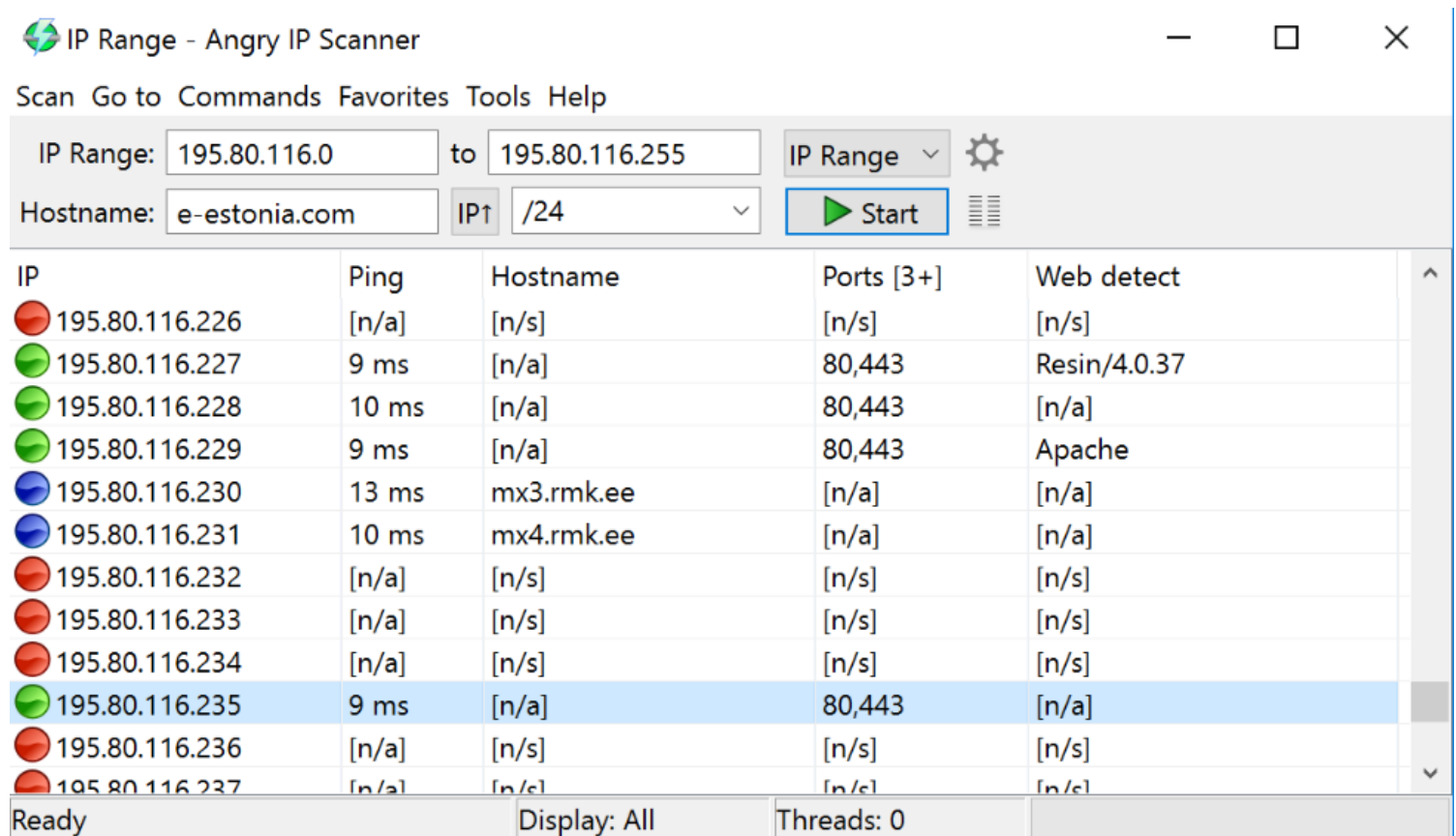
### Install:

You can download the latest release from [here](#).

### Usage:

Angry IP Scanner can be used via the GUI.

Full usage information and documentation can be found [here](#).



IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 195.80.116.0 to 195.80.116.255 IP Range [v] [gear]

Hostname: e-estonia.com IP↑ /24 [v] [Start] [list]

IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmkk.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmkk.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display: All Threads: 0

Image used from <https://tinyurl.com/yxnsennqscreenshots/>

## ← BACK ZMap

ZMap is a network scanner designed to perform comprehensive scans of the IPv4 address space or large portions of it.

On a typical desktop computer with a gigabit Ethernet connection, ZMap is capable scanning the entire public IPv4 address space in under 45 minutes.

### Install:

You can download the latest release from [here](#).

### Usage:

```
# Scan only 10.0.0.0/8 and 192.168.0.0/16 on TCP/80
zmap -p 80 10.0.0.0/8 192.168.0.0/16
```

Full usage information can be found [here](#).

```
kali@kali:~$ sudo zmap -p 80 10.0.0.0/16 -o LANresults.csv
Nov 05 12:55:35.813 [WARN] blacklist: ZMap is currently using the default blacklist located
at /etc/zmap/blacklist.conf. By default, this blacklist excludes locally scoped networks (
e.g. 10.0.0.0/8, 127.0.0.1/8, and 192.168.0.0/16). If you are trying to scan local networks
, you can change the default blacklist by editing the default ZMap configuration at /etc/zm
ap/zmap.conf.
Nov 05 12:55:35.820 [INFO] zmap: output module: csv
0:00 0%; send: 100 0 p/s (2.27 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s a
vg); hitrate: 0.00%
0:01 4%; send: 3347 3.25 Kp/s (3.20 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0
p/s avg); hitrate: 0.00%
0:02 4%; send: 3347 0 p/s (1.63 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s
avg); hitrate: 0.00%
0:03 5%; send: 3347 0 p/s (1.09 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s
avg); hitrate: 0.00%
0:04 5%; send: 3347 0 p/s (819 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s av
g); hitrate: 0.00%
0:05 5% (1m43s left); send: 3347 0 p/s (657 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0
```

\*Image used from <https://tinyurl.com/23wfx2ly>



Shodan is a search engine for internet-connected devices.

It crawls the internet for assets, allowing users to search for specific devices and view information about them.

This information can include the device's IP address, the software and version it is running, and the type of device it is.

### Install:

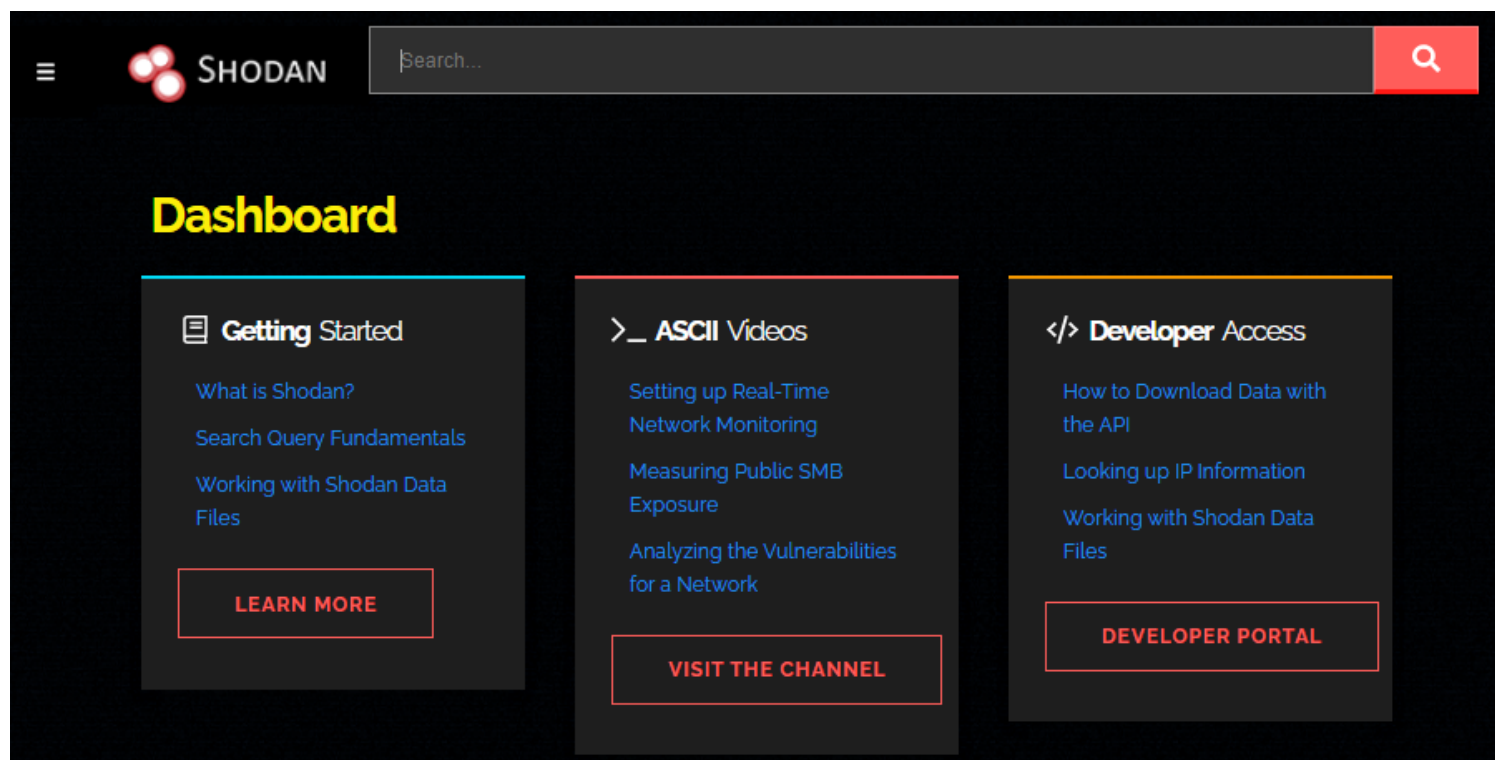
The search engine can be accessed at <https://www.shodan.io/dashboard>.

### Usage:

[Shodan query fundamentals](#)

[Shodan query examples](#)

[Nice query cheatsheet](#)



\*Image used from <https://tinyurl.com/2bxjjpdj>

## Vulnerability Management

*Tools for identifying, prioritizing, and mitigating vulnerabilities in the network and on individual devices.*

### [OpenVAS](#)

OpenVAS is an open-source vulnerability scanner that helps identify security vulnerabilities in software and networks.

It is a tool that can be used to perform network security assessments and is often used to identify vulnerabilities in systems and applications so that they can be patched or mitigated.

OpenVAS is developed by the Greenbone Networks company and is available as a free and open-source software application.

**Install: (Kali)**







vulnerabilities in systems and applications so that they can be patched or mitigated.

Nessus is developed by Tenable, Inc. and is available in both free and paid versions:

- The free version, called Nessus Essentials, is available for personal use only and is limited in its capabilities compared to the paid version.
- The paid version, called Nessus Professional, is more fully featured and is intended for use in a professional setting.

## Install:

Register for a Nessus Essentials activation code [here](#) and download.

Purchase Nessus Professional from [here](#).

## Usage:

Extensive documentation can be found [here](#).

[Nessus Plugins Search](#)

[Tenable Community](#)

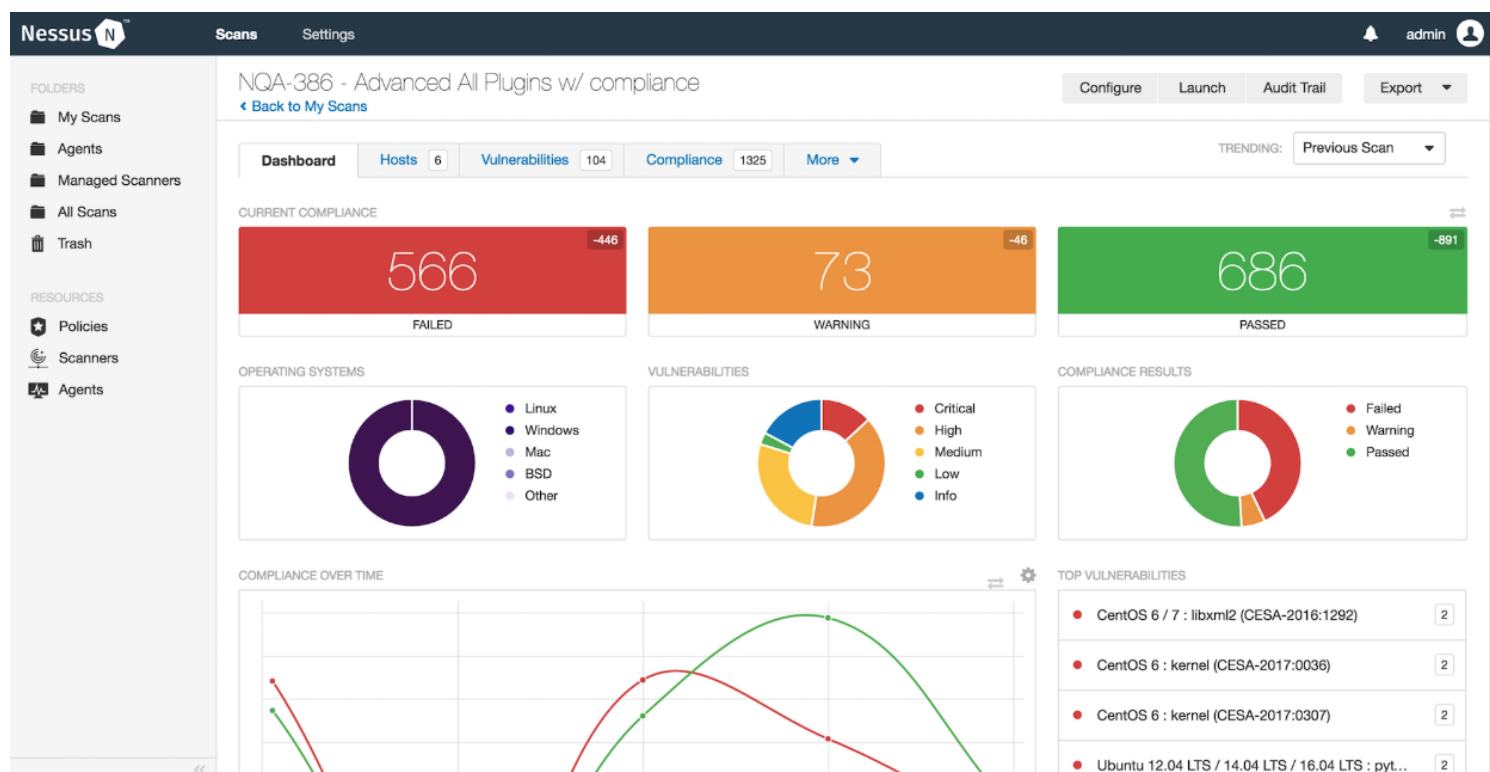


Image used from <https://www.tenable.com>

← **Nexpose**  
BACK

Nexpose is a vulnerability management tool developed by Rapid7. It is designed to help

organizations identify and assess vulnerabilities in their systems and applications in order to mitigate risk and improve security.

Nexpose can be used to scan networks, devices, and applications in order to identify vulnerabilities and provide recommendations for remediation.

It also offers features such as asset discovery, risk prioritization, and integration with other tools in the Rapid7 vulnerability management platform.

## Install:

For detailed installation instructions see [here](#).

## Usage:

For full login information see [here](#).

For usage and scan creation instructions see [here](#).

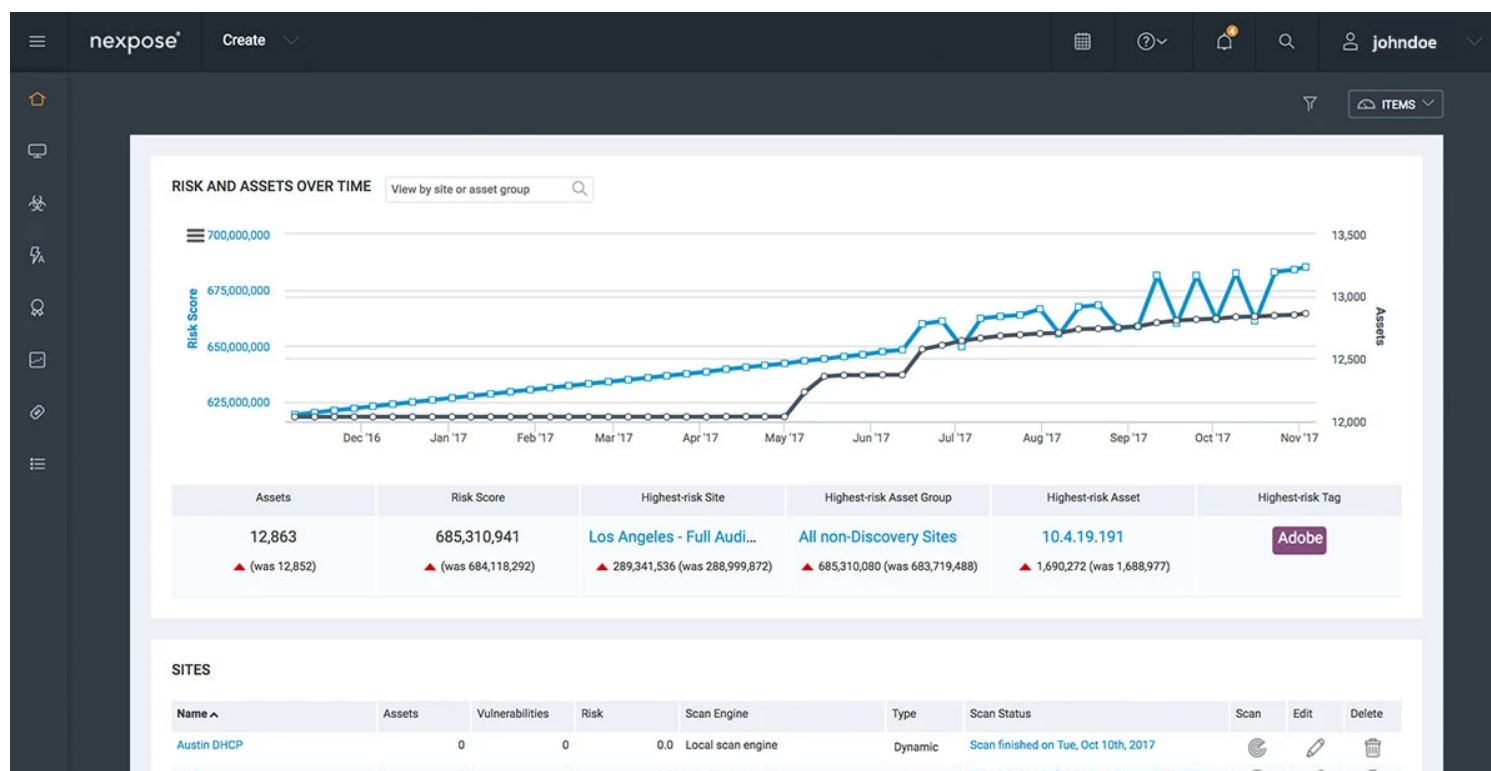


Image used from <https://tinyurl.com/zkzh785>

## ← HackerOne

HackerOne is a bug bounty management company that can be used to create and manage bug bounty programs for your business.

Bug bounty programs are a great way to outsource external vulnerability assessments, with the platform offering both private and public programs with the ability set program scopes and rules

of engagement.

HackerOne also offer initial triage and management of external bug reports from researchers, with the ability to compensate researchers directly through the platform.

HACKERONE BOUNTY

# Bug bounty programs for businesses

Tap into the skills of the global hacker community to uncover high-risk vulnerabilities faster.

Watch the Demo

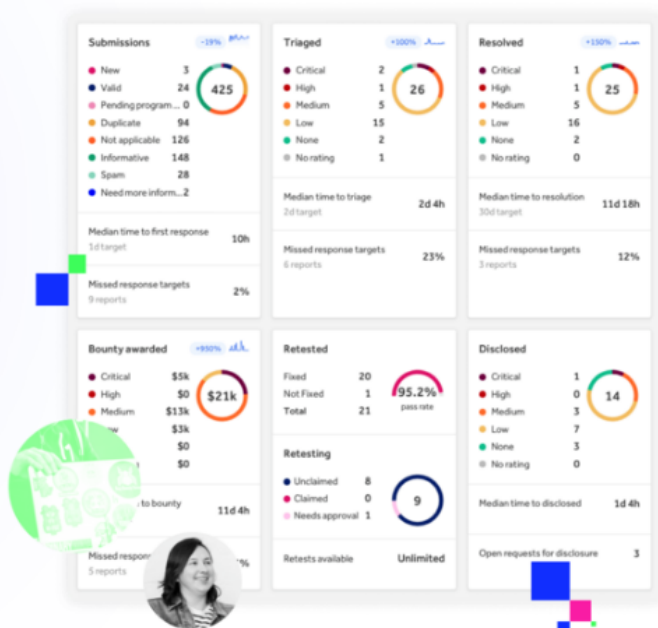


Image used from <https://tinyurl.com/ycmlxuqwproduct/bug-bounty-platform>

## Security Monitoring

Tools for collecting and analyzing security logs and other data sources to identify potential threats and anomalous activity.

← BACK **Sysmon**

Sysmon is a Windows system monitor that tracks system activity and logs it to the Windows event log.

It provides detailed information about system activity, including process creation and termination, network connections, and changes to file creation time.

Sysmon can be configured to monitor specific events or processes and can be used to alert administrators of suspicious activity on a system.

**Install:**

Download the sysmon binary from [here](#).

## Usage:

```
# Install with default settings (process images hashed with SHA1 and no network m
sysmon -accepteula -i
```

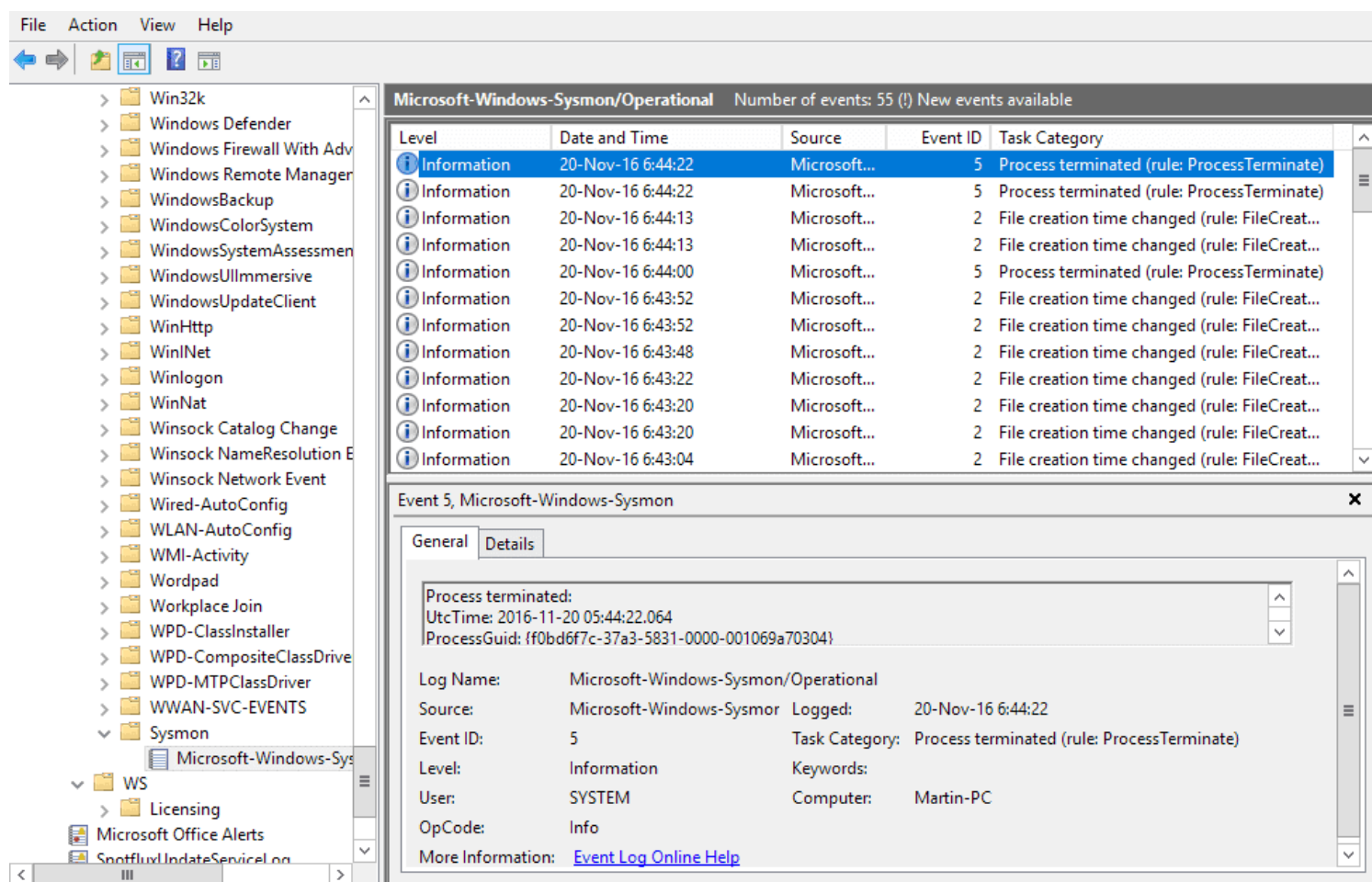
```
# Install Sysmon with a configuration file (as described below)
sysmon -accepteula -i c:\windows\config.xml
```

```
# Uninstall
sysmon -u
```

```
# Dump the current configuration
sysmon -c
```

Full event filtering information can be found [here](#).

The Microsoft documentation page can be found [here](#).



Level	Date and Time	Source	Event ID	Task Category
Information	20-Nov-16 6:44:22	Microsoft...	5	Process terminated (rule: ProcessTerminate)
Information	20-Nov-16 6:44:22	Microsoft...	5	Process terminated (rule: ProcessTerminate)
Information	20-Nov-16 6:44:13	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:44:13	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:44:00	Microsoft...	5	Process terminated (rule: ProcessTerminate)
Information	20-Nov-16 6:43:52	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:52	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:48	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:22	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:20	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:20	Microsoft...	2	File creation time changed (rule: FileCreat...
Information	20-Nov-16 6:43:04	Microsoft...	2	File creation time changed (rule: FileCreat...

Event 5, Microsoft-Windows-Sysmon

General Details

Process terminated:  
UtcTime: 2016-11-20 05:44:22.064  
ProcessGuid: {ff0bd6f7c-37a3-5831-0000-001069a70304}

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Microsoft-Windows-Sysmon Logged: 20-Nov-16 6:44:22  
Event ID: 5 Task Category: Process terminated (rule: ProcessTerminate)  
Level: Information Keywords:  
User: SYSTEM Computer: Martin-PC  
OpCode: Info  
More Information: [Event Log Online Help](#)

\*Image used from <https://tinyurl.com/29mp297x>



Kibana is an open-source data visualization and exploration tool that is often used for log

analysis in combination with Elasticsearch.

Kibana provides a user-friendly interface for searching, visualizing, and analyzing log data, which can be helpful for identifying patterns and trends that may indicate a security threat.

Kibana can be used to analyze a wide range of data sources, including system logs, network logs, and application logs. It can also be used to create custom dashboards and alerts to help security teams stay informed about potential threats and respond quickly to incidents.

### **Install:**

You can download Kibana from [here](#).

Installation instructions can be found [here](#).

### **Usage: (Visualize and explore log data)**

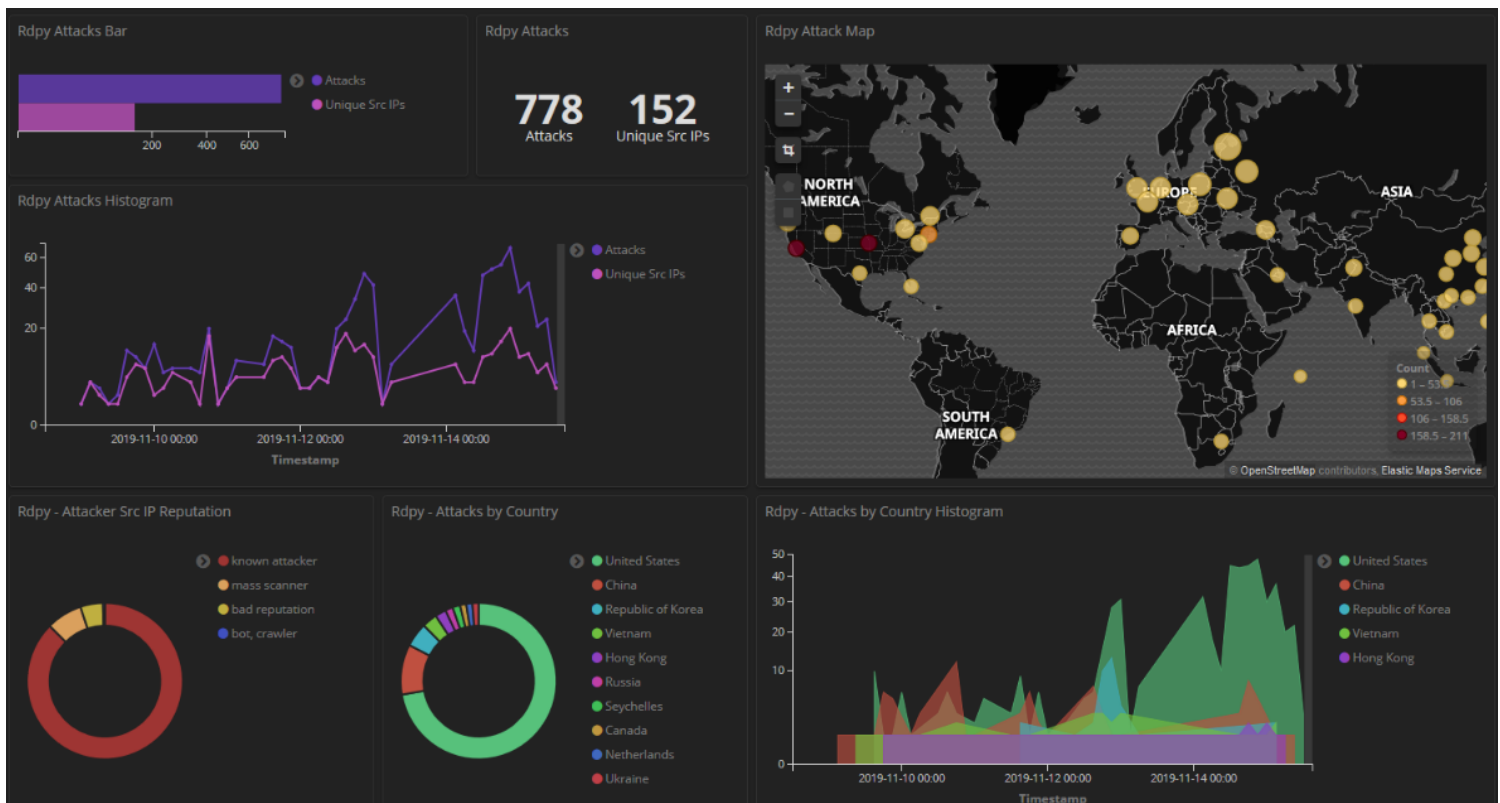
Kibana provides a range of visualization tools that can help you identify patterns and trends in your log data. You can use these tools to create custom dashboards that display relevant metrics and alerts.

### **Usage: (Threat Alerting)**

Kibana can be configured to send alerts when it detects certain patterns or anomalies in your log data. You can set up alerts to notify you of potential security threats, such as failed login attempts or network connections to known malicious IP addresses.

Nice [blog](#) about querying and visualizing data in Kibana.





\*Image used from <https://tinyurl.com/2yamdcnp>

## ← Logstash

Logstash is a open-source data collection engine with real-time pipelining capabilities. It is a server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch.

Logstash has a rich set of plugins, which allows it to connect to a variety of sources and process the data in multiple ways. It can parse and transform logs, translate data into a structured format, or send it to another tool for further processing.

With its ability to process large volumes of data quickly, Logstash is an integral part of the ELK stack (Elasticsearch, Logstash, and Kibana) and is often used to centralize, transform, and monitor log data.

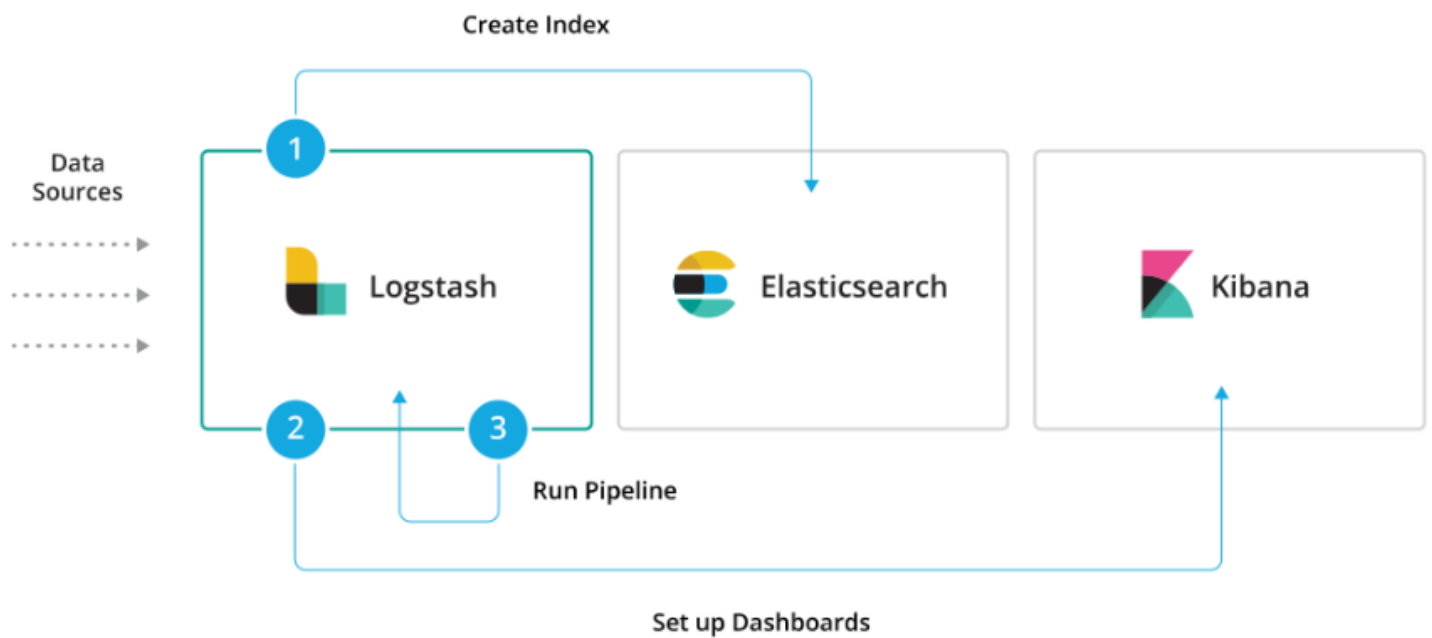
### Install:

Download logstash from [here](#).

### Usage:

Full logstash documentation [here](#).

Configuration examples [here](#).



\*Image used from <https://tinyurl.com/27ot5gwp>

← **parsedmarc**

A Python module and CLI utility for parsing DMARC reports.

When used with Elasticsearch and Kibana (or Splunk), it works as a self-hosted open source alternative to commercial DMARC report processing services such as Agari Brand Protection, Dmarcian, OnDMARC, ProofPoint Email Fraud Defense, and Valimail.

Features:

- Parses draft and 1.0 standard aggregate/rua reports
- Parses forensic/failure/ruf reports
- Can parse reports from an inbox over IMAP, Microsoft Graph, or Gmail API
- Transparently handles gzip or zip compressed reports
- Consistent data structures
- Simple JSON and/or CSV output
- Optionally email the results
- Optionally send the results to Elasticsearch and/or Splunk, for use with premade dashboards
- Optionally send reports to Apache Kafka

&gt; Search... (e.g. status:200 AND extension:PHP)

Options

Refresh

Add a filter +

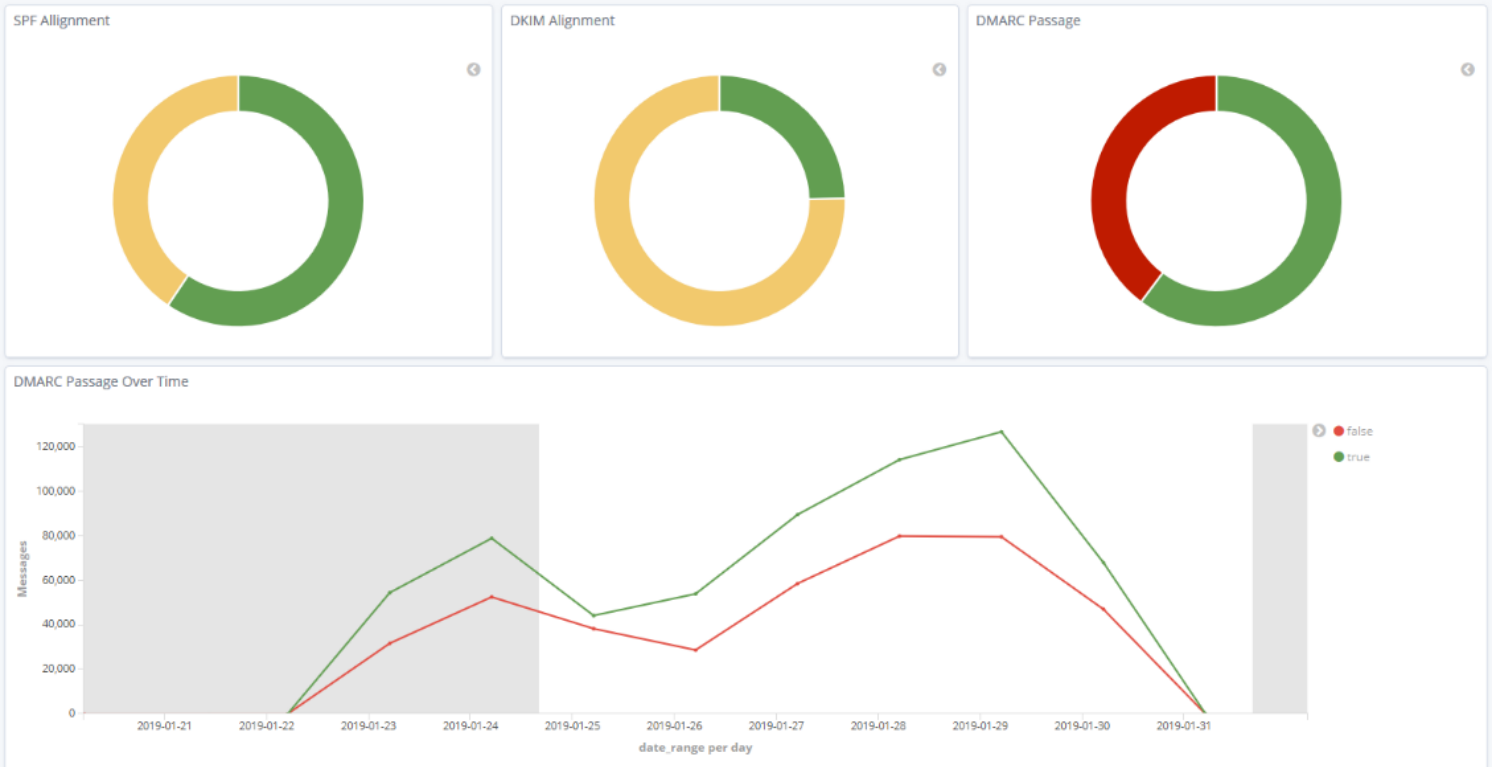


Image used from <https://tinyurl.com/y2xok72q>

## ← BACK Phishing Catcher

As a business, phishing can cause reputational and financial damage to you and your customers. Being able to proactively identify phishing infrastructure targeting your business helps to reduce the risk of these damages.

Phish catcher allows you to catch possible phishing domains in near real time by looking for suspicious TLS certificate issuances reported to the Certificate Transparency Log (CTL) via the CertStream API.

"Suspicious" issuances are those whose domain name scores beyond a certain threshold based on a configuration file.

```
user@debian:~/Work/sslphish$ ./catch_phishing.py
certificate_update: 0cert [00:00, ?cert/s][INFO:root] 2017-11-07 11:09:18,627 - Connection established to CertStrea
n! Listening for events...
Suspicious: paupalaccountupdate.com (score=107)
Suspicious: apple_appleidsecured.com (score=82)
Suspicious: recovery-my-paupal.com-locale-country-us_help-accessid.net (score=165)
Suspicious: cpanel.cudi-com.pl (score=82)
Suspicious: cudi-com.niedrogi.net (score=82)
Suspicious: cudi-com.pl (score=80)
Suspicious: mail.cudi-com.pl (score=81)
Suspicious: webdisk.cudi-com.pl (score=84)
Suspicious: webmail.cudi-com.pl (score=83)
Suspicious: www.cudi-com.niedrogi.net (score=83)
Suspicious: www.cudi-com.pl (score=81)
Suspicious: paupal-login.com,accountreviews-highrisk.com (score=112)
certificate_update: 10406cert [00:22, 370.58cert/s]
```

Image used from <https://tinyurl.com/ybx7rdlo>



Maltrail is a malicious traffic detection system, utilizing publicly available lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists. A trail can be anything from domain name, URL, IP address or HTTP User-Agent header value.

A demo page for this tool can be found [here](#).

### Install:

```
sudo apt-get install git python3 python3-dev python3-pip python-is-python3 libpca
sudo pip3 install pcap-ng
git clone --depth 1 https://tinyurl.com/jlujhah.git
cd maltrail
```

### Usage:

```
sudo python3 sensor.py
```

2016-01-20 (a day ago)

6,945 Threats | 903,708 Events | medium Severity | 4,498 Sources | 6,402 Tracks

25 threats per page

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
419c7e3	bitvenica	33288	low	2016-01-20 00:00:04	2016-01-20 23:59:59		175.6.228.149				TCP	IP	175.6.228.149	bad reputation	alienvault.com	
b4433c0	bitvenica	4	low	2016-01-20 18:04:40	2016-01-20 23:59:59		51.255.65.22			80 (http)	TCP	IP	51.255.65.22	spammer	botscout.com	
6a5952a	bitvenica	1111	low	2016-01-20 00:00:02	2016-01-20 23:59:58		71.6.158.166				TCP	IP	71.6.158.166	bad reputation	alienvault.com	
783399c	bitvenica	3939	low	2016-01-20 00:00:03	2016-01-20 23:59:58		71.6.135.131				TCP	IP	71.6.135.131	mass scanner	(static)	
ef30918	bitvenica	2808	low	2016-01-20 00:00:32	2016-01-20 23:59:58		222.186.21.34			22 (ssh)	TCP	IP	222.186.21.34	known attacker	autosshun.org	
ef1b727	bitvenica	127	medium	2016-01-20 03:16:13	2016-01-20 23:59:58				54.231.50.44		TCP	IP	54.231.50.44 (s3.amazonaws.com)	malware distribution	mal0fe.com	
422130d	bitvenica	403	low	2016-01-20 23:40:34	2016-01-20 23:59:58		125.64.93.78			22 (ssh)	TCP	IP	125.64.93.78	known attacker	ba0ips.com	
80b11c3	bitvenica	30298	low	2016-01-20 00:00:00	2016-01-20 23:59:57		185.130.5.224			53413 (netis)	UDP	IP	185.130.5.224	known attacker	ba0ips.com	
813f359	bitvenica	21	low	2016-01-20 01:46:09	2016-01-20 23:59:57		91.200.12.106			80 (http)	TCP	IP	91.200.12.106	known attacker	blocklist.de	
8130829	bitvenica	137	medium	2016-01-20 03:24:55	2016-01-20 23:59:57				53 (dns)		UDP	DNB	Q.info	constant threshold no such domain (suspicious)	(heuristic)	
6a020a4	bitvenica	7082	low	2016-01-20 00:00:32	2016-01-20 23:59:55		198.20.99.130				TCP	IP	198.20.99.130	mass scanner	(static)	
90f7ca13	bitvenica	2837	low	2016-01-20 00:00:50	2016-01-20 23:59:55		94.102.48.195	43905			TCP	IP	94.102.48.195	bad reputation	alienvault.com	
6999e141	bitvenica	627	low	2016-01-20 08:37:38	2016-01-20 23:59:54		141.212.122.194				TCP	IP	141.212.122.194	mass scanner	(static)	
7180610	bitvenica	564	low	2016-01-20 08:39:29	2016-01-20 23:59:54		141.212.122.193				TCP	IP	141.212.122.193	mass scanner	(static)	
9751ac10	bitvenica	55	medium	2016-01-20 01:07:21	2016-01-20 23:59:53				8.8.8.8	53 (dns)	UDP	DNB	Q.sx	domain (suspicious)	(static)	
9130400	bitvenica	801	low	2016-01-20 08:45:14	2016-01-20 23:59:53		141.212.122.207				TCP	IP	141.212.122.207	mass scanner	(static)	
7080340	bitvenica	413	low	2016-01-20 09:05:22	2016-01-20 23:59:53		141.212.122.206				TCP	IP	141.212.122.206	mass scanner	(static)	
4c10172	bitvenica	4828	low	2016-01-20 00:00:10	2016-01-20 23:59:50		149.202.238.216			8080 (http-alt)	TCP	IP	149.202.238.216	bad reputation	alienvault.com	
6070302	bitvenica	101	low	2016-01-20 00:03:52	2016-01-20 23:59:50		141.212.121.40			443 (https)	TCP	IP	141.212.121.40	mass scanner	(static)	
6052642	bitvenica	3999	low	2016-01-20 00:00:05	2016-01-20 23:59:49		71.6.165.200				TCP	IP	71.6.165.200	mass scanner	(static)	
07420af	bitvenica	967	low	2016-01-20 00:00:45	2016-01-20 23:59:49		82.221.105.7				TCP	IP	82.221.105.7	mass scanner	(static)	
90b0321	bitvenica	5	medium	2016-01-20 07:04:43	2016-01-20 23:59:48				8.8.8.8	53 (dns)	UDP	DNB	amsrela0jy.ru	excessive no such domain (suspicious)	(heuristic)	
50b03b0	bitvenica	1	low	2016-01-20 23:59:48	2016-01-20 23:59:48		67.21.35.231	43025			UDP	IP	67.21.35.231	http spammer	zblam.com	
4300000	bitvenica	1875	low	2016-01-20 00:00:04	2016-01-20 23:59:47		188.138.17.205				TCP	IP	188.138.17.205	bad reputation	alienvault.com	
20c0000	bitvenica	43	medium	2016-01-20 00:21:23	2016-01-20 23:59:47				8.8.8.8	53 (dns)	UDP	DNB	Q.eease.com	excessive no such domain (suspicious)	(heuristic)	

Showing 1 to 25 of 6,945 threats

Image used from <https://tinyurl.com/jlujhah>

## ← BACK AutorunsToWinEventLog

Autoruns is a tool developed by Sysinternals that allows you to view all of the locations in Windows where applications can insert themselves to launch at boot or when certain applications are opened. Malware often takes advantages of these locations to ensure that it runs whenever your computer boots up.

Autoruns conveniently includes a non-interactive command line utility. This code generates a CSV of Autoruns entries, converts them to JSON, and finally inserts them into a custom Windows Event Log. By doing this, we can take advantage of our existing WEF infrastructure to get these entries into our SIEM and start looking for signs of malicious persistence on endpoints and servers.

### Install:

Download [AutorunsToWinEventLog](#).

### Usage:

From an Admin Powershell console run `.\Install.ps1`

This script does the following:

- Creates the directory structure at `c:\Program Files\AutorunsToWinEventLog`
- Copies over `AutorunsToWinEventLog.ps1` to that directory
- Downloads `Autorunsc64.exe` from <https://tinyurl.com/je3be4s>
- Sets up a scheduled task to run the script daily @ 11am



_time	host	Category	Entry_Location	Entry	Launch_String
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BTHUSB	\SystemRoot\System32\drivers\BTHUSB.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BTHPORT	\SystemRoot\System32\drivers\BTHport.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BTHMODEM	\SystemRoot\System32\drivers\bthmodem.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BthMini	\SystemRoot\System32\drivers\BTHMINI.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BthLEEnum	\SystemRoot\System32\drivers\Microsoft.Bluetooth.Legacy.LEEnum.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BthHfEnum	\SystemRoot\System32\drivers\bthhfenum.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	bthEnum	\SystemRoot\System32\drivers\bthEnum.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BthA2dp	\SystemRoot\System32\drivers\BthA2dp.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	bowser	system32\DRIVERS\bowser.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	bindf11	\SystemRoot\system32\drivers\bindf11.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	Beep	Beep
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	bcmf2	\SystemRoot\System32\drivers\bcmf2.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BasicRender	\SystemRoot\System32\DriverStore\FileRepository\basicrender_inf_and64_9ff437f462543a42\BasicRender.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	BasicDisplay	\SystemRoot\System32\DriverStore\FileRepository\basicdisplay_inf_and64_25ab9518f018cfda\BasicDisplay.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	ban	system32\drivers\ban.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	b06bdrv	system32\drivers\b06bdrv.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	atap1	system32\drivers\atap1.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	AsynchMac	\SystemRoot\System32\drivers\asynmac.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	arcsaa	System32\drivers\arcsaa.sys
2021-01-04 22:03:39	win10.windowsin.local	Drivers	HKLM\System\CurrentControlSet\Services	AppVFs	\SystemRoot\system32\drivers\AppVFs.sys

\*Image used from <https://tinyurl.com/2c69cynb>

## ← procfilter

ProcFilter is a process filtering system for Windows with built-in [YARA](#) integration. YARA rules can be instrumented with custom meta tags that tailor its response to rule matches. It runs as a Windows service and is integrated with [Microsoft's ETW API](#), making results viewable in the Windows Event Log. Installation, activation, and removal can be done dynamically and does not require a reboot.

ProcFilter's intended use is for malware analysts to be able to create YARA signatures that protect their Windows environments against a specific threat. It does not include a large signature set. Think lightweight, precise, and targeted rather than broad or all-encompassing. ProcFilter is also intended for use in controlled analysis environments where custom plugins can perform artifact-specific actions.

### Install:

#### [ProcFilter x86/x64 Release/Debug Installers](#)

*Note: Unpatched Windows 7 systems require hotfix 3033929 to load the driver component. More information can be found [here](#).*

Nice configuration template file [here](#).

## Usage:

```
procfilter -start
```

Usage screenshots can be found [here](#).

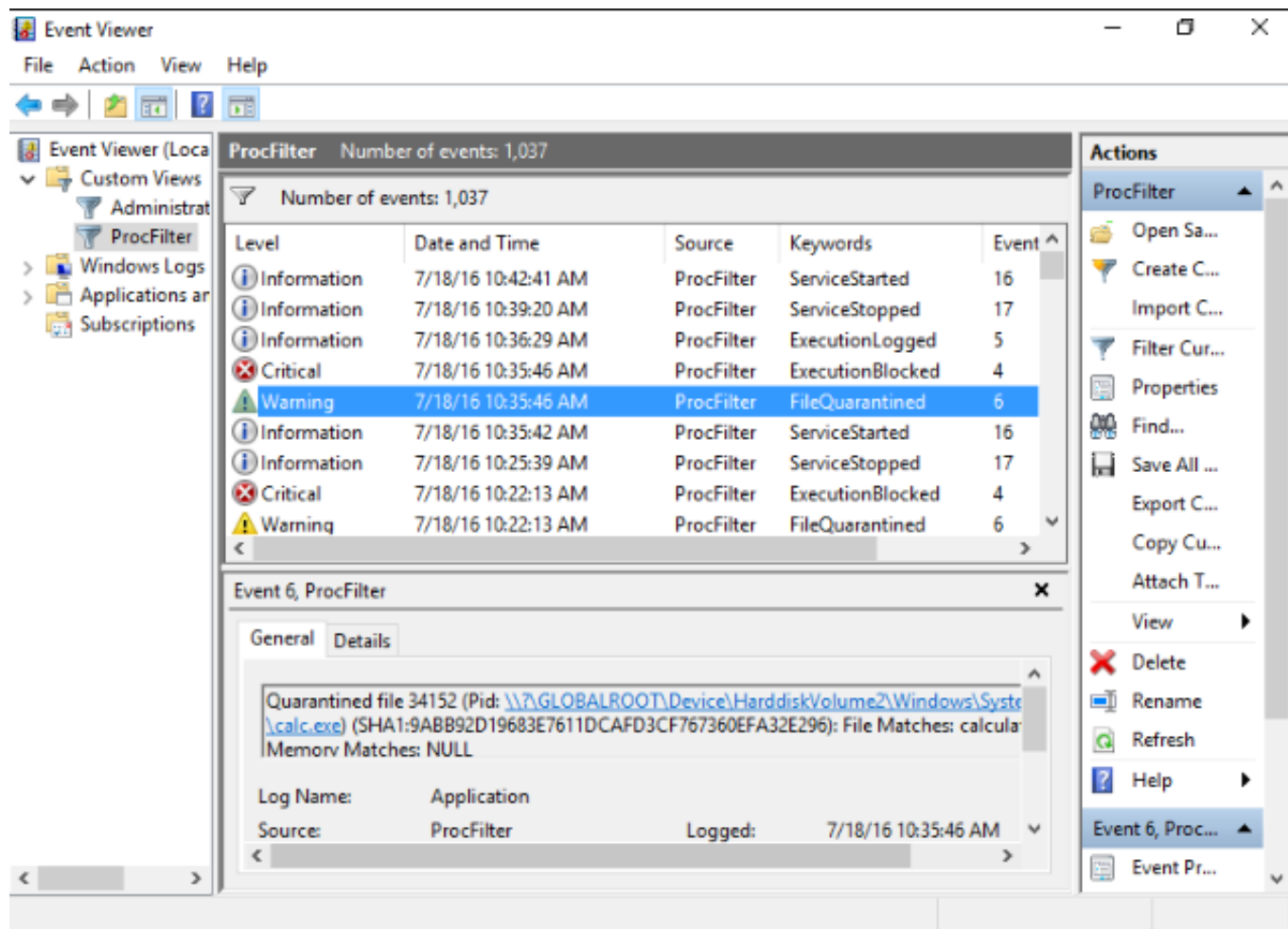


Image used from <https://tinyurl.com/jj7rwq4w>

## ← BACK **velociraptor**

Velociraptor is a unique, advanced open-source endpoint monitoring, digital forensic and cyber response platform.

It was developed by Digital Forensic and Incident Response (DFIR) professionals who needed a powerful and efficient way to hunt for specific artifacts and monitor activities across fleets of endpoints. Velociraptor provides you with the ability to more effectively respond to a wide range of digital forensic and cyber incident response investigations and data breaches:

Features:

- Reconstruct attacker activities through digital forensic analysis
- Hunt for evidence of sophisticated adversaries
- Investigate malware outbreaks and other suspicious network activities
- Monitor continuously for suspicious user activities, such as files copied to USB devices
- Discover whether disclosure of confidential information occurred outside the network
- Gather endpoint data over time for use in threat hunting and future investigations

## Install:

Download the binary from the [release page](#).

## Usage:

`velociraptor gui`

Full usage information can be found [here](#).

```
[INFO] 2020-09-08T05:36:06-07:00
[INFO] 2020-09-08T05:36:06-07:00
[INFO] 2020-09-08T05:36:06-07:00
[INFO] 2020-09-08T05:36:06-07:00
[INFO] 2020-09-08T05:36:06-07:00 Digging deeper! https://www.velocidex.com
[INFO] 2020-09-08T05:36:06-07:00 This is Velociraptor 0.4.9 built on 2020-09-02T14:19:59+10:00 (6a559265)
[INFO] 2020-09-08T05:36:06-07:00 No embedded config - you can pack one with the `config repack` command
[INFO] 2020-09-08T05:36:06-07:00 Env var VELOCIRAPTOR_CONFIG is not set
[INFO] 2020-09-08T05:36:06-07:00 Loading config from file C:\Users\test\AppData\Local\Temp\server.config.yaml
[INFO] 2020-09-08T05:36:06-07:00 No valid config found - will generate a new one at C:\Users\test\AppData\Local\Temp\server.config.yaml
[INFO] 2020-09-08T05:36:06-07:00 Starting Frontend. {"build_time":"2020-09-02T14:19:59+10:00","commit":"6a559265","version":"0.4.9"}
[INFO] 2020-09-08T05:36:06-07:00 Starting Journal service.
[INFO] 2020-09-08T05:36:06-07:00 Starting the notification service.
[INFO] 2020-09-08T05:36:06-07:00 Starting Inventory Service
[INFO] 2020-09-08T05:36:06-07:00 Loaded 185 built in artifacts in 97.1217ms
[INFO] 2020-09-08T05:36:06-07:00 Starting Label service.
[INFO] 2020-09-08T05:36:06-07:00 Starting Hunt Dispatcher Service.
[INFO] 2020-09-08T05:36:06-07:00 Selected frontend configuration localhost:8000
[INFO] 2020-09-08T05:36:06-07:00 Starting Client Monitoring Service
[INFO] 2020-09-08T05:36:06-07:00 Creating default Client Monitoring Service
[INFO] 2020-09-08T05:36:06-07:00 Initial user admin not present, creating
[INFO] 2020-09-08T05:36:06-07:00 Server upgrade detected -> 0.4.9... running upgrades.
```

Image used from <https://docs.velociraptor.app>

 **SysmonSearch**

SysmonSearch makes event log analysis more effective and less time consuming, by aggregating event logs generated by Microsoft's Sysmon.

SysmonSearch uses Elasticsearch and Kibana (and Kibana plugin).

- **Elasticsearch**  
Elasticsearch collects/stores Sysmon's event log.

- **Kibana**

Kibana provides user interface for your Sysmon's event log analysis. The following functions are implemented as Kibana plugin.

- Visualizes Function

This function visualizes Sysmon's event logs to illustrate correlation of processes and networks.

- Statistical Function

This function collects the statistics of each device or Sysmon's event ID.

- Monitor Function

This function monitor incoming logs based on the preconfigured rules, and triggers alert.

- **StixloC server**

You can add search/monitor condition by uploading STIX/IOC file. From StixloC server Web UI, you can upload STIXv1, STIXv2 and OpenIOC format files.

### **Install: (Linux)**

```
git clone https://tinyurl.com/25z78a7j.git
```

[Modify Elasticsearch configuration](#)

[Modify Kibana configuration](#)

Full installation instructions can be found [here](#).

### **Usage:**

*Once Elasticsearch and Kibana configurations have been modified, restart the services and navigate to your Kibana interface. The SysmonSearch ribbon should be visible.*

[Visualize the Sysmon log to investigate suspicious behavior](#)

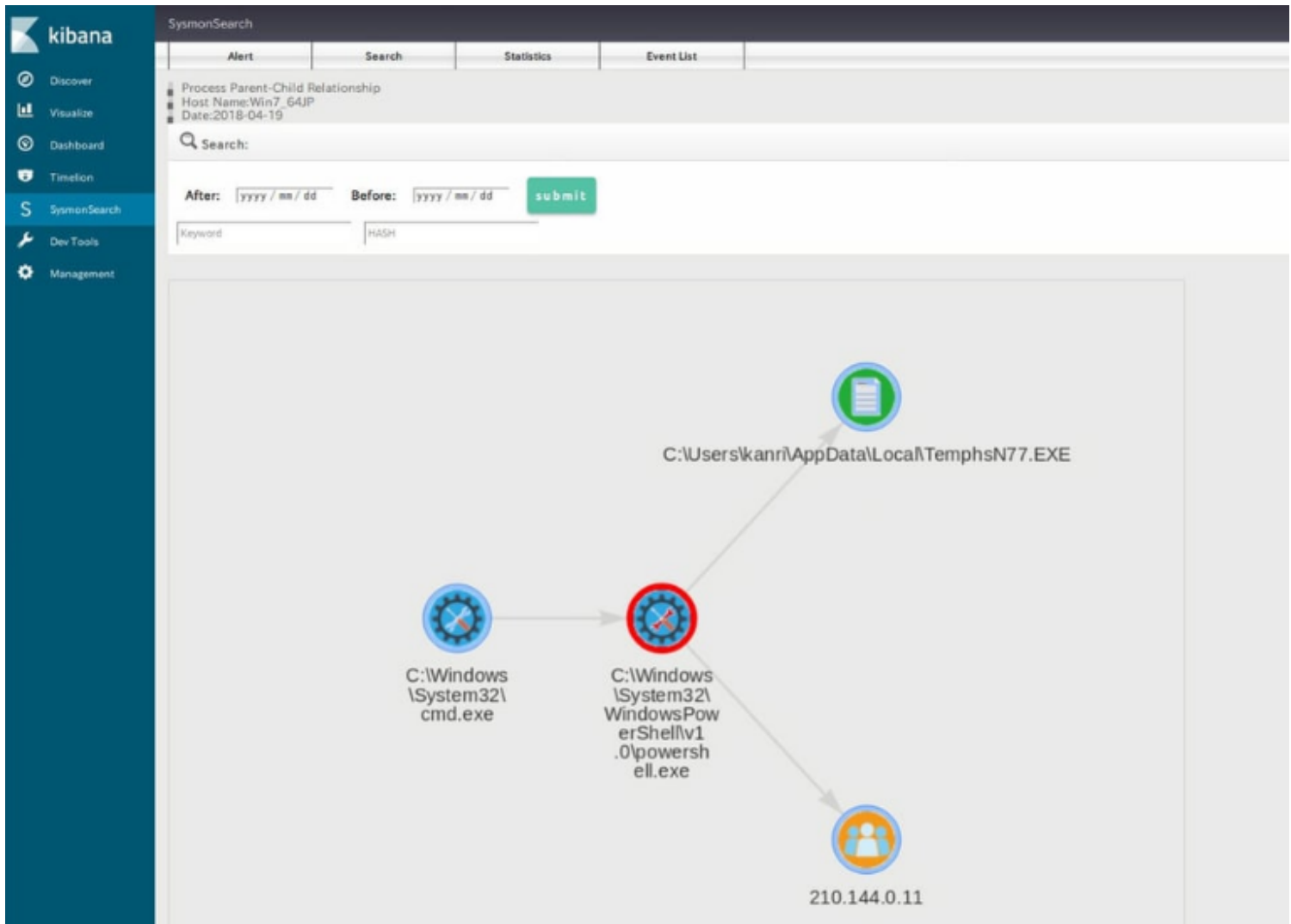


Image used from <https://tinyurl.com/22gyzhf5>

## Threat Tools and Techniques

*Tools for identifying and implementing detections against TTPs used by threat actors.*

[← lolbas-project.github.io](https://github.com/lolbas-project)

Living off the land binaries (LOLBins) are legitimate Windows executables that can be used by threat actors to carry out malicious activities without raising suspicion.

Using LOLBins allows attackers to blend in with normal system activity and evade detection, making them a popular choice for malicious actors.

The LOLBAS project is a MITRE mapped list of LOLBINS with commands, usage and detection information for defenders.

Visit <https://tinyurl.com/y6ct9yf9>.

## Usage:

Use the information for detection opportunities to harden your infrastructure against LOLBIN usage.

Here are some project links to get started:

- [Bitsadmin.exe](#)
- [Certutil.exe](#)
- [Cscript.exe](#)

## LOLBAS

☆ Star 5,019



### Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).

Search among 173 binaries by name (e.g. 'MSBuild'), function (e.g. 'execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
<a href="#">AppInstaller.exe</a>	<a href="#">Download</a>	Binaries	<a href="#">T1105: Ingress Tool Transfer</a>
<a href="#">Aspnet_Compiler.exe</a>	<a href="#">AWL bypass</a>	Binaries	<a href="#">T1127: Trusted Developer Utilities Proxy Execution</a>
<a href="#">At.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1053.002: At</a>
<a href="#">Atbroker.exe</a>	<a href="#">Execute</a>	Binaries	<a href="#">T1218: System Binary Proxy Execution</a>
<a href="#">Bash.exe</a>	<a href="#">Execute</a> <a href="#">AWL bypass</a>	Binaries	<a href="#">T1202: Indirect Command Execution</a>

Image used from <https://tinyurl.com/y6ct9yf9>

[← BACK](#) [gtfobins.github.io](https://gtfobins.github.io)

GTFOBins (short for "Get The F\* Out Binaries") is a collection of Unix binaries that can be used to escalate privileges, bypass restrictions, or execute arbitrary commands on a system.

They can be used by threat actors to gain unauthorized access to systems and carry out malicious activities.

The GTFOBins project is a list of Unix binaries with command and usage information for attackers. This information can be used to implement unix detections.



Visit <https://tinyurl.com/y5shmqsr>.

## Usage:

Here are some project links to get started:

- [base64](#)
- [curl](#)
- [nano](#)

## GTFOBins ☆ Star 7,751

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate [functions](#) of Unix binaries that can be abused to ~~get the f\*\*\*~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).



Shell Command Reverse shell Non-interactive reverse shell Bind shell Non-interactive bind shell File upload File download  
File write File read Library load SUID Sudo Capabilities Limited SUID

Search among 358 binaries: <binary> +<function> ...

Binary	Functions
<a href="#">7z</a>	File read Sudo
<a href="#">ab</a>	File upload File download SUID Sudo
<a href="#">agetty</a>	SUID
<a href="#">alpine</a>	File read SUID Sudo
<a href="#">ansible-playbook</a>	Shell Sudo
<a href="#">aoss</a>	Shell Sudo

Image used from <https://tinyurl.com/y5shmqsr>

 [filesec.io](#)

Filesec is a list of file extensions that can be used by attackers for phishing, execution, macros etc.

This is a nice resource to understand the malicious use cases of common file extensions and ways that you can defend against them.

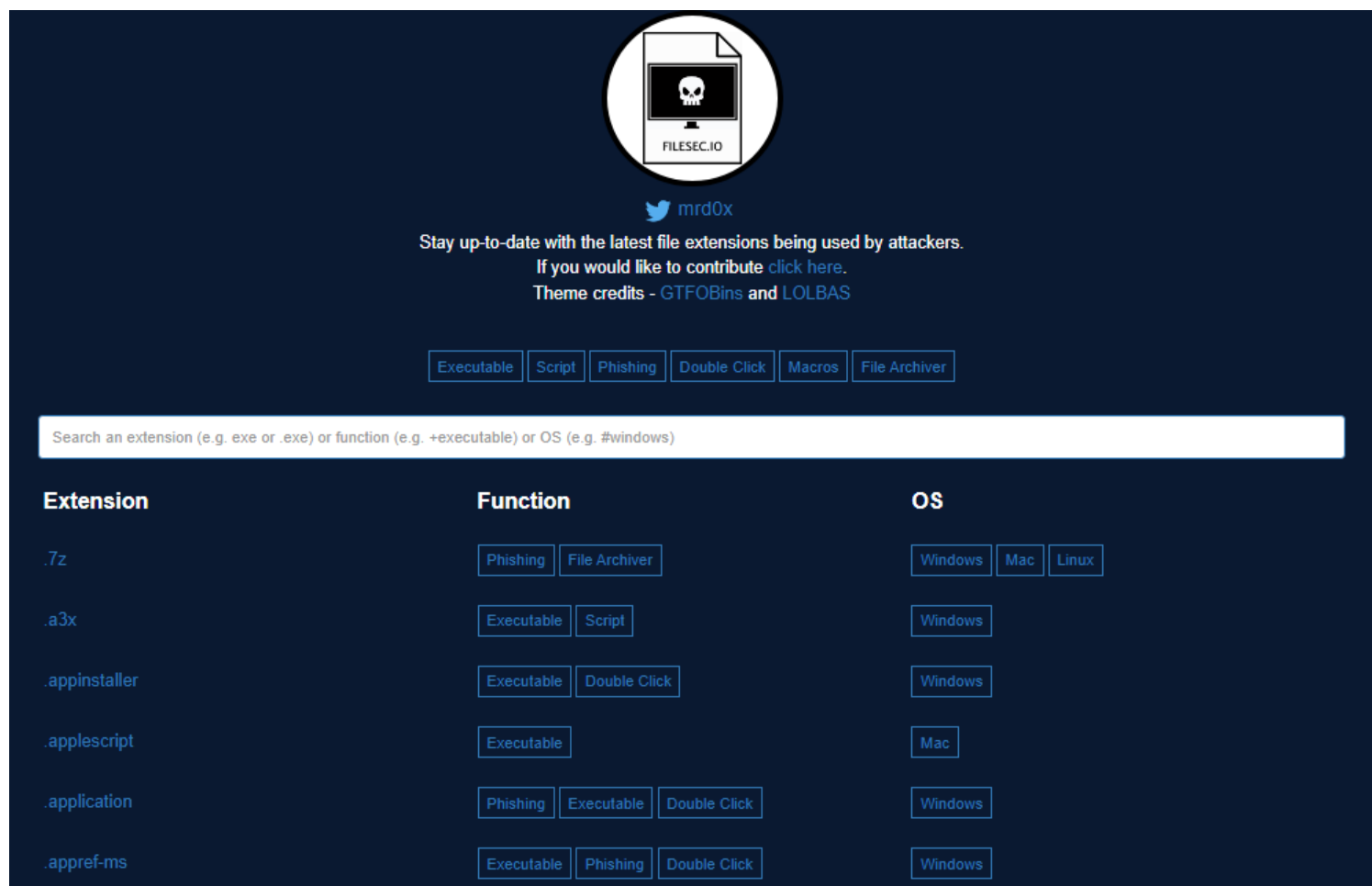
Each file extension page contains a description, related operating system and recommendations.

Visit <https://tinyurl.com/248sbkdm>.

## Usage:

Here are some project links to get started:

- [.Docm](#)
- [.Iso](#)
- [.Ppam](#)



The screenshot shows the FILESEC.IO website interface. At the top, there is a circular logo with a skull icon and the text 'FILESEC.IO'. Below the logo is a Twitter handle '@mrd0x'. The main heading reads: 'Stay up-to-date with the latest file extensions being used by attackers. If you would like to contribute click here. Theme credits - GTF0Bins and LOLBAS'. Below this is a navigation bar with buttons for 'Executable', 'Script', 'Phishing', 'Double Click', 'Macros', and 'File Archiver'. A search bar contains the text: 'Search an extension (e.g. exe or .exe) or function (e.g. +executable) or OS (e.g. #windows)'. Below the search bar is a table with three columns: 'Extension', 'Function', and 'OS'.

Extension	Function	OS
.7z	Phishing, File Archiver	Windows, Mac, Linux
.a3x	Executable, Script	Windows
.appinstaller	Executable, Double Click	Windows
.applescript	Executable	Mac
.application	Phishing, Executable, Double Click	Windows
.appref-ms	Executable, Phishing, Double Click	Windows

Image used from <https://tinyurl.com/248sbkdm>

## ← KQL Search

KQL stands for "Kusto Query Language", and it is a query language used to search and filter data in Azure Monitor logs. It is similar to SQL, but is more optimized for log analytics and time-series data.

KQL query language is particularly useful for blue teamers because it allows you to quickly and easily search through large volumes of log data to identify security events and anomalies that may indicate a threat.

KQL Search is a web app created by [@ugurkocde](#) that aggregates KQL queries that are shared on GitHub.

You can visit the site at <https://tinyurl.com/29tu4s33>.

More information about Kusto Query Language (KQL) can be found [here](#).



The screenshot shows the KQL Search web application interface. At the top, the title "KQL Search" is displayed in a large, bold, white font. Below the title, a subtitle reads "This is an aggregator for KQL queries that are shared on GitHub." The main content area features a search bar with the placeholder text "Search a keyword (e.g. User, Device) ..." and a dropdown menu currently set to "All". Below the search bar, it indicates "Last Refresh: January 5, 2023" and "Total Number of KQL Queries found: 850". A list of KQL queries is shown, each with a GitHub icon to its right. The queries listed are: "AWS-PublicIPAddedtoInstance.kql", "Anamoly-HigherThanExpectedSysLog.kql", "Duo-LogParserwithIdentityInfo.kql", "SysLog-DetectAnomaliesInEvents.kql", "Active Directory: AADPasswordProtection-AllEvents", and "Active Directory: SecurityEvent-AccountPreAuthChanges".

Image used from <https://tinyurl.com/29tu4s33>

## Unprotect Project

Malware authors spend a great deal of time and effort to develop complex code to perform malicious actions against a target system. It is crucial for malware to remain undetected and avoid sandbox analysis, antiviruses or malware analysts.

With this kind of technics, malware are able to pass under the radar and stay undetected on a system. The goal of this free database is to centralize the information about malware evasion techniques.

The project aims to provide Malware Analysts and Defenders with actionable insights and detection capabilities to shorten their response times.

The project can be found at <https://unprotect.it/>.

The project has an API - Docs [here](#).



Anti-Debugging



Anti-Disassembly



Anti-Forensic



Anti-Monitoring



Antivirus Evasion



Data Obfuscation



Defense Evasion [Mitre]



Machine Learning Evasion



Network Evasion



Others



Packers



Process Manipulating



Sandbox Evasion

\*Image used from <https://tinyurl.com/2d4sr3t2>

← **chainsaw**

Chainsaw provides a powerful 'first-response' capability to quickly identify threats within Windows forensic artefacts such as Event Logs and MFTs. Chainsaw offers a generic and fast method of searching through event logs for keywords, and by identifying threats using built-in support for Sigma detection rules, and via custom Chainsaw detection rules.

Features:

- Hunt for threats using Sigma detection rules and custom Chainsaw detection rules
- Search and extract forensic artefacts by string matching, and regex patterns
- Lightning fast, written in rust, wrapping the EVTX parser library by @OBenamram

- Clean and lightweight execution and output formats without unnecessary bloat
- Document tagging (detection logic matching) provided by the TAU Engine Library
- Output results in a variety of formats, such as ASCII table format, CSV format, and JSON format
- Can be run on MacOS, Linux and Windows

## Install:

```
git clone https://tinyurl.com/2ao4fsst
cargo build --release
git clone https://tinyurl.com/234plxto
git clone https://tinyurl.com/2ax487lo
```

## Usage:

```
./chainsaw hunt EVTX-ATTACK-SAMPLES/ -s sigma/ --mapping mappings/sigma-event-log
```

**CHAINSAW**  
By F-Secure Countercept (Author: @FranticTyping)

```
[+] Found 266 EVTX files
[+] Loaded 734 detection rules (74 were not loaded)
[+] Printing results to screen
[+] Hunting: [-----] 100%
```

[+] Detection: Suspicious Process Creation

system_time	id	detection_rules	computer_name	Event.EventData.Image	command_line
2019-02-16 10:02:21	1	Exfiltration and Tunneling Tools Execution	"PC01.example.corp"	C:\Users\IEUser\Desktop\plink.exe	plink.exe 10.0.2.18 -P 80 -C -R 127.0.0.3:4444:127.0.0.2:3389 -l test -pw test
2019-03-17 20:18:09	1	Netsh Port or Application Allowed Netsh RDP Port Opening	"PC04.example.corp"	C:\Windows\System32\netsh.exe	netsh advfirewall firewall add rule name="Remote Desktop" dir=in protocol=tcp localport=3389 profile=any action=allow
2019-04-30 07:46:15	1	Meterpreter or Cobalt Strike Getsystem Service Start	"IEWIN7"	C:\Windows\System32\cmd.exe	cmd.exe /c echo nsdch > \\.\pipe\nsdch
2019-04-30 20:19:52	1	Mimikatz Command Line FromBase64String Command Line Curl Start Combination	"IEWIN7"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]:Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir}\system64\WindowsPowerShell\1.0\powershell.exe";\$s=New-Object System.Diagnostics.ProcessStartInfo;\$s.FileName=\$b;\$s.Arguments="-noni -nop -w hidden -c &{[ScriptBlock]::create((New-Object IO.StreamReader(New-Object IO.Compression.GzipStream(New-Object IO.MemoryStream([Convert]::FromBase64String('H4sIAIuuyFwCA7VW+2/aSB0+0ZiH6P1gYEzCMA60a5JWu035y7GUVWdyP6kiEw0psexgQck7s8pg... (use --full to show all content)

[+] Detection: Security audit log was cleared

system_time	id	computer	subject_user
2019-11-15 08:19:02	1102	"alice.insecurebank.local"	"bob"

[+] Detection: Suspicious Command Line

system_time	id	detection_rules	computer_name	Event.EventData.CommandLine	process_name
2019-02-13 18:03:28	4688	Exfiltration and Tunneling Tools Execution	"PC01.example.corp"	<empty>	C:\Users\user01\Desktop\plink.exe

\*Image used from <https://tinyurl.com/2csejd7d>

Adversaries attempt to bypass signature based/pattern matching/blacklist techniques by introducing random: filenames, service names, workstation names, domains, hostnames, SSL cert subjects and issuer subjects, etc.

Freq is a python API designed by Mark Baggett to handle mass entropy testing. It was designed to be used in conjunction with a SIEM solutions but can work with anything that can submit a web request.

The tool uses frequency tables that map how likely one character will follow another

### Install:

```
git clone https://tinyurl.com/2djeryez
cd freq
```

### Usage:

```
# Running freq_server.py on port 10004 and using a frequency table of /opt/freq/d
/usr/bin/python /opt/freq/freq_server.py 10004 /opt/freq/dns.freq
```



yarGen is a generator for YARA rules

The main principle is the creation of yara rules from strings found in malware files while removing all strings that also appear in goodware files. Therefore yarGen includes a big goodware strings and opcode database as ZIP archives that have to be extracted before the first use.

The rule generation process also tries to identify similarities between the files that get analyzed and then combines the strings to so called super rules. The super rule generation does not remove the simple rule for the files that have been combined in a single super rule. This means that there is some redundancy when super rules are created. You can suppress a simple rule for a file that was already covered by super rule by using `--nosimple`.

### Install:

Download the latest [release](#).

```
pip install -r requirements.txt
python yarGen.py --update
```



## Usage:

```
# Create a new strings and opcodes database from an Office 2013 program directory
yarGen.py -c --opcodes -i office -g /opt/packs/office2013

# Update the once created databases with the "-u" parameter
yarGen.py -u --opcodes -i office -g /opt/packs/office365
```

Usage examples can be found [here](#).

```
#####
          /---\
         /---\
        /---\
       /---\
      /---\
     /---\
    /---\
   /---\
  /---\
 /---\
/---\

Yara Rule Generator
by Florian Roth
July 2015
Version 0.14.0

#####
[+] Reading goodness strings from database 'good-strings.db' ...
    (This could take some time and uses up to 2 GB of RAM)
[+] Initializing Bayes Filter ...
[-] Training filter with good strings from ./lib/good.txt
[+] Processing malware files ...
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/backdoor.exe
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/dropper.exe
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/install.m.apk
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/ndisk.sys
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/putty.exe
[-] Processing: /Volumes/Work/MAL/HackingTeam/bin/rcs.exe
[+] Generating statistical data ...
[+] Generating Super Rules ... (a lot of foo magic)
[E] ERROR while generating general condition - check the global rule and remove it if it's faulty
[+] Generating simple rules ...
[-] Applying intelligent filters to string findings ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/rcs.exe ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/putty.exe ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/dropper.exe ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/install.m.apk ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/backdoor.exe ...
[-] Filtering string set for /Volumes/Work/MAL/HackingTeam/bin/ndisk.sys ...
[+] Generating super rules ...
[=] Generated 6 SIMPLE rules.
[=] Generated 0 SUPER rules.
[=] All rules written to yargen_rules.yar
```

Image used from <https://tinyurl.com/q2zk84j>

## EmailAnalyzer

With EmailAnalyzer you can able to analyze your suspicious emails. You can extract headers, links and hashes from the .eml file

## Install:

```
git clone https://tinyurl.com/2deo6mk7
cd EmailAnalyzer
```

## Usage:

```
# View headers in eml file
python3 email-analyzer.py -f <eml file> --headers

# Get hashes
python3 email-analyzer.py -f <eml file> --digests

# Get links
python3 email-analyzer.py -f <eml file> --links

# Get attachments
python3 email-analyzer.py -f <eml file> --attachments
```

```
C:\> python3 email-analyzer.py -f <eml file> --links
```

```
Links
```

```
[1]->https://example.com
[2]->https://testlinks.com/campaing/123124
```

```
Investigation
```

---

```
[1]
[VirusTotal]:
https://www.virustotal.com/gui/search/example.com
[UrlScan]:
https://urlscan.io/search/#example.com
```

---

```
[2]
[VirusTotal]:
https://www.virustotal.com/gui/search/testlinks.com/campaing/123124
[UrlScan]:
https://urlscan.io/search/#testlinks.com/campaing/123124
```



VCG is an automated code security review tool that handles C/C++, Java, C#, VB and PL/SQL. It has a few features that should hopefully make it useful to anyone conducting code security reviews, particularly where time is at a premium:

- In addition to performing some more complex checks it also has a config file for each language that basically allows you to add any bad functions (or other text) that you want to search for
- It attempts to find a range of around 20 phrases within comments that can indicate broken code ("ToDo", "FixMe", "Kludge", etc.)
- It provides a nice pie chart (for the entire codebase and for individual files) showing relative proportions of code, whitespace, comments, 'ToDo' style comments and bad code

### Install:

You can install the pre-compiled binary [here](#).

Open the project .sln, choose "Release", and build.

### Usage:

#### STARTUP OPTIONS:

(Set desired starting point **for** GUI. **If** using console mode these options will  
-t, --target <Filename|DirectoryName>: Set target file **or** directory. Use thi  
-l, --language <CPP|PLSQL|JAVA|CS|VB|PHP|COBOL>: Set target language (Defa  
-e, --extensions <ext1|ext2|ext3>: Set file extensions **to** be analysed (See R  
-i, --import <Filename>: Import XML/CSV results **to** GUI.

#### OUTPUT OPTIONS:

(Automagically export results **to** a file **in** the specified format. Use XML **or** C  
-x, --export <Filename>: Automatically export results **to** XML file.  
-f, --csv-export <Filename>: Automatically export results **to** CSV file.  
-r, --results <Filename>: Automatically export results **to** flat text file.

#### CONSOLE OPTIONS:

-c, --console: Run application **in** console only (hide GUI).  
-v, --verbose: Set console output **to** verbose mode.  
-h, --help: Show help.



CyberChef is a free, web-based tool that allows users to manipulate and transform data using a wide range of techniques.

With CyberChef, you can perform a wide range of operations on data, such as converting between different data formats (e.g., hexadecimal, base64, ASCII), encoding and decoding data, searching and replacing text etc.

The tool also includes a recipe system, which allows you to save and share data manipulation workflows with others.

The tool can be used from [here](#).

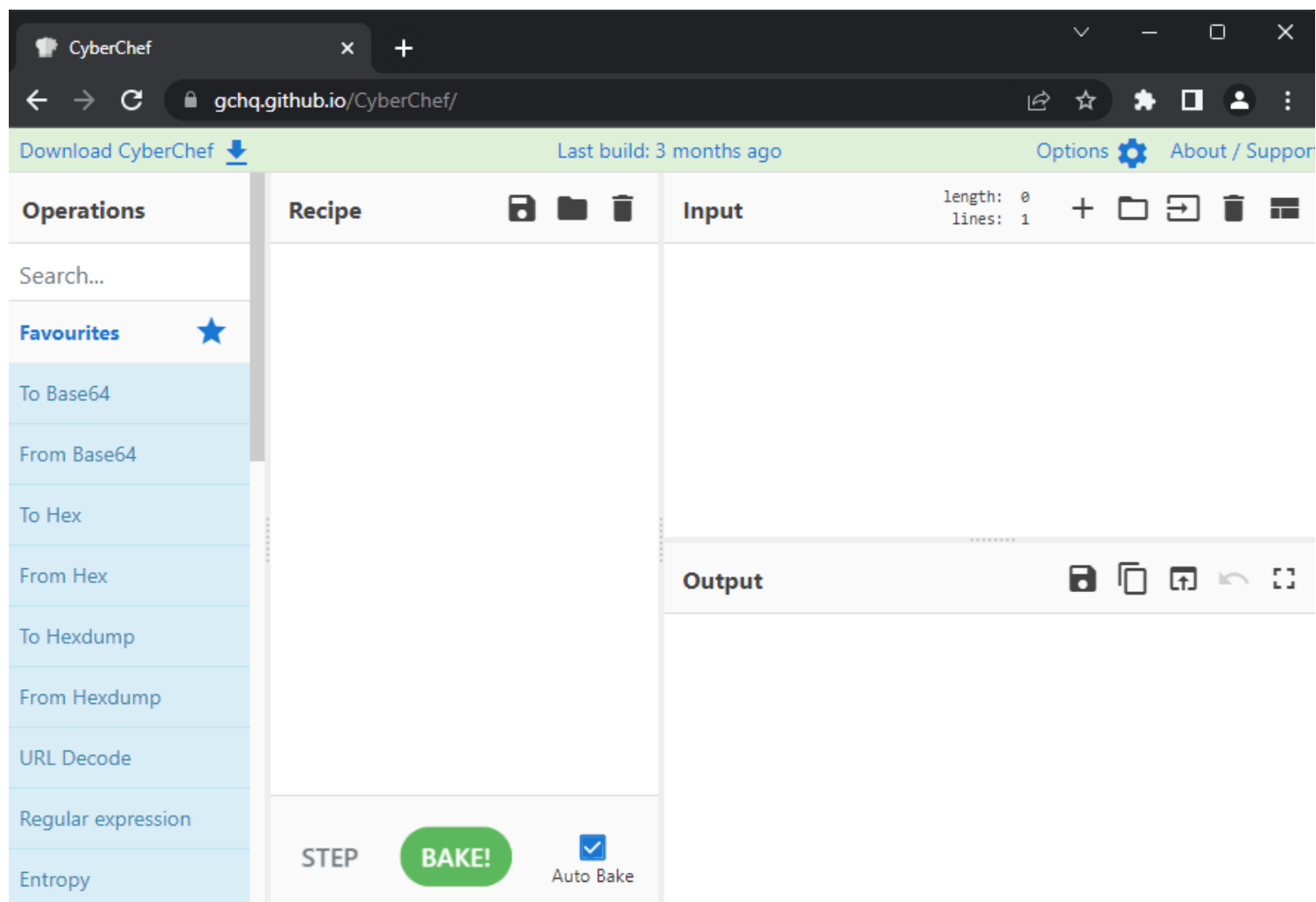


Image used from <https://tinyurl.com/y2aa4tyy>

## Threat Intelligence

*Tools for gathering and analyzing intelligence about current and emerging threats, and for generating alerts about potential threats.*

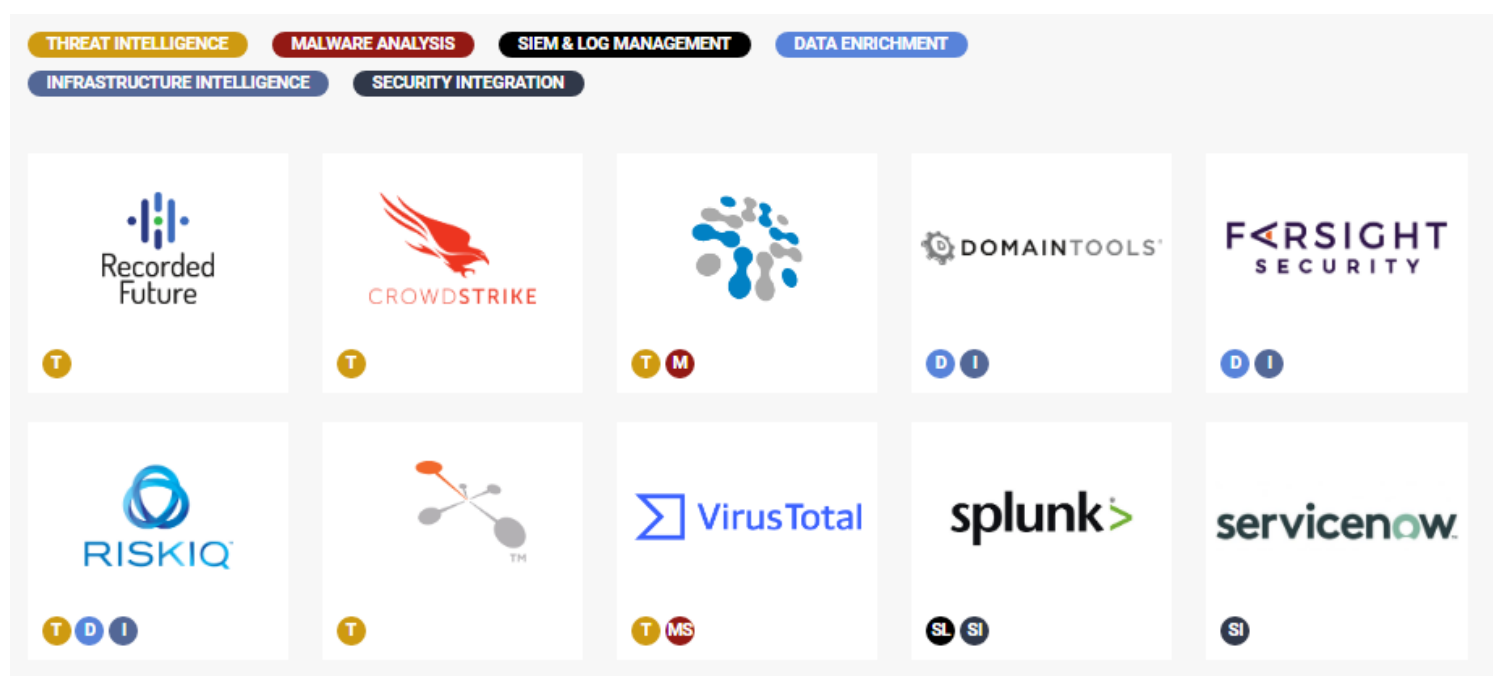
Maltego is a commercial threat intelligence and forensics tool developed by Paterva. It is used by security professionals to gather and analyze information about domains, IP addresses, networks, and individuals in order to identify relationships and connections that might not be immediately apparent.

Maltego uses a visual interface to represent data as entities, which can be linked together to form a network of relationships. It includes a range of transforms, which are scripts that can be used to gather data from various sources, such as social media, DNS records, and WHOIS data.

Maltego is often used in conjunction with other security tools, such as SIEMs and vulnerability scanners, as part of a comprehensive threat intelligence and incident response strategy.

You can schedule a demo [here](#).

[Maltego handbook Handbook for Cyber Threat Intelligence](#)



\*Image used from <https://tinyurl.com/2yfc4zm2>

← **MISP**  
BACK

MISP (short for Malware Information Sharing Platform) is an open-source platform for sharing, storing, and correlating Indicators of Compromise (IOCs) of targeted attacks, threats, and malicious activity.

MISP includes a range of features, such as real-time sharing of IOCs, support for multiple formats, and the ability to import and export data to and from other tools.

It also provides a RESTful API and various data models to facilitate the integration of MISP with other security systems. In addition to its use as a threat intelligence platform, MISP is also used

for incident response, forensic analysis, and malware research.

## Install:

```
# Kali
```

```
wget -O /tmp/misp-kali.sh https://tinyurl.com/y63cqbq5 && bash /tmp/misp-kali.sh
```

```
# Ubuntu 20.04.2.0-server
```

```
wget -O /tmp/INSTALL.sh https://tinyurl.com/y63cqbq5  
bash /tmp/INSTALL.sh
```

Full installation instructions can be found [here](#).

## Usage:

MISP documentation can be found [here](#).

[MISP user guide](#)

[MISP Training Cheat sheet](#)

## Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 next »

Published	Org	Owner org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	covid-19		10616	current-event:pandemic="covid-19"  pandemic:covid-19="cyber"  osint:source.type="manual collection"  ttp:white  osint:certainty="93%"  COVID-19  circ:incident-classification="covid-19"  workflow:state="complete"	12		admin@admin.test	2020-03-31	maldoc, covid19	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Siemens AG		10597		1		admin@admin.test	2020-03-12	This is a central test event	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>			10614	processed_by_intelmq	8	3	admin@admin.test	2020-05-04	IntelMQ test	Organisation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	BitDefender		10611	Bitdefender:validated  MalwareFamily-Ursnif  TIM:validated  ttp:green	32	3	admin@admin.test	2019-12-19	Ongoing malware campaign (9-13/12)	Telcos SG	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Vairav Technology		10622	Download	112		admin@admin.test	2020-03-31	VX Vault - Malware Dropper feed	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Vairav Technology		10621		569	9	admin@admin.test	2020-01-03	Azorult Tracker Feed feed	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Vairav Technology		10618	Download	527	1	admin@admin.test	2019-08-29	URL feed	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	BitDefender		10593	TIM:validated  ttp:green  Bitdefender:validated  MalwareFamily:Ursnif	32	3	admin@admin.test	2019-12-11	Ongoing malware propagation campaign	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Siemens AG		10600		2		admin@admin.test	2020-04-22	Another test to push / zmq v2	All	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Siemens AG		10599		1		admin@admin.test	2020-04-21	Another test to push / zmq	All	

\*Image used from <https://tinyurl.com/2cfmjfw>



ThreatConnect is a threat intelligence platform that helps organizations aggregate, analyze, and



act on threat data. It is designed to provide a single, unified view of an organization's threat landscape and enable users to collaborate and share information about threats.

The platform includes a range of features for collecting, analyzing, and disseminating threat intelligence, such as a customizable dashboard, integration with third-party data sources, and the ability to create custom reports and alerts.

It is intended to help organizations improve their security posture by providing them with the information they need to identify, prioritize, and respond to potential threats.

You can request a demo from [here](#).

## ThreatConnect for Threat Intel Analysts - PDF

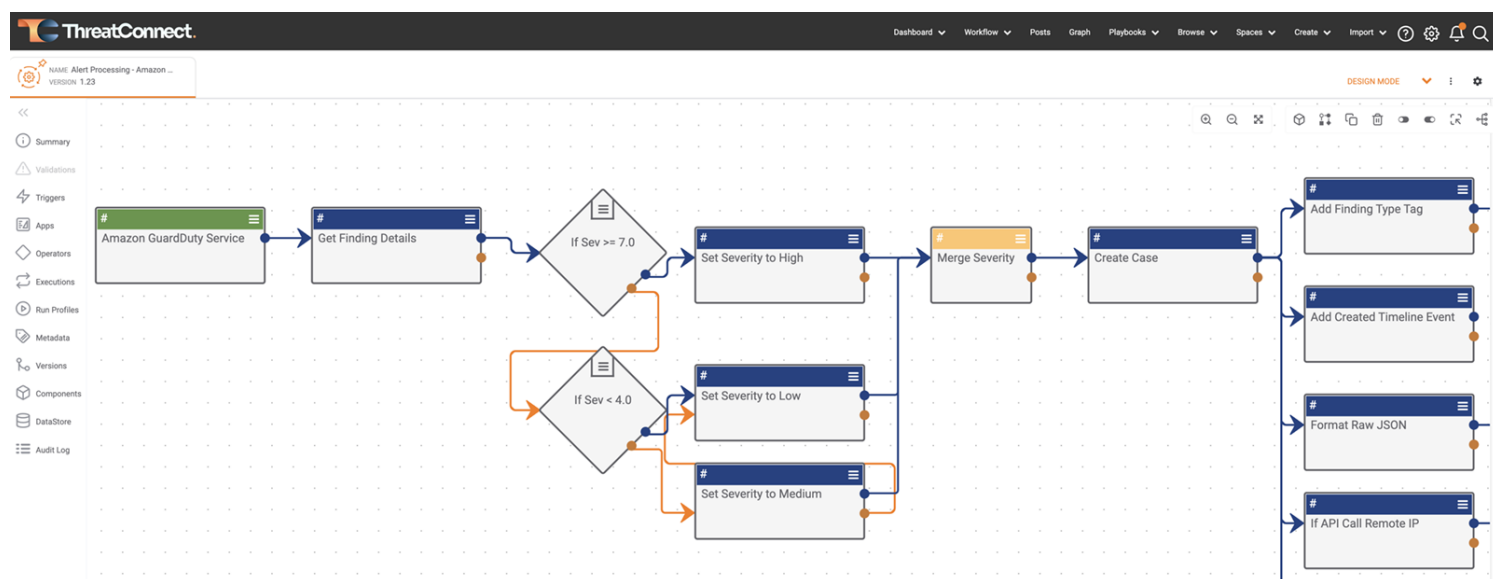


Image used from <https://tinyurl.com/2c73pzw9>

## ← Adversary Emulation Library

This is a library of adversary emulation plans to enable you to evaluate your defensive capabilities against real-world threats.

Emulation plans are an essential component for organizations looking to prioritize defenses against behavior from specific threats.

The TTPs outlined in this resource can be used to design specific threat emulation activities to test your organisations defenses against specific threat actors.

Visit the resource [here](#).

### Example (sandworm)

- [Sandworm Emulated Software Source Code](#)

- [Sandworm Detection Scenario Walkthrough](#)
- [Sandworm Intelligence Summary](#)

☰ README.md

Available adversary emulation plans are listed below:

Full Emulation Plans	Intelligence Summary
FIN6	FIN6 is thought to be a financially motivated cyber-crime group. The group has aggressively targeted and compromised high-volume POS systems in the hospitality and retail sectors since at least 2015...
APT29	APT29 is thought to be an organized and well-resourced cyber threat actor whose collection objectives appear to align with the interests of the Russian Federation...
menuPass	menuPass is thought to be threat group motivated by collection objectives, with targeting that is consistent with Chinese strategic objectives...
Carbanak Group	Carbanak is a threat group who has been found to manipulate financial assets, such as by transferring funds from bank accounts or by taking over ATM infrastructures...
FIN7	FIN7 is a financially-motivated threat group that has been associated with malicious operations dating back to late 2015. The group is characterized by their persistent targeting and large-scale theft of payment card data from victim systems...
	Sandworm Team is a destructive threat group attributed to Russia's General Staff of the Armed Forces, Main Intelligence Directorate (GRU) that has been reportedly active since 2009...

Image used from <https://tinyurl.com/2d442487>

## Incident Response Planning

*Tools for creating and maintaining an incident response plan, including templates and best practices for responding to different types of incidents.*



The NIST Cybersecurity Framework (CSF) is a framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage cybersecurity risks. It provides a set of guidelines, best practices, and standards for implementing and maintaining a robust cybersecurity program.

The framework is organized around five core functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a structure for understanding and addressing the various components of cybersecurity risk.

The CSF is designed to be flexible and adaptable, and it can be customized to fit the specific needs and goals of an organization. It is intended to be used as a tool for improving an organization's cybersecurity posture and for helping organizations better understand and manage their cybersecurity risks.

### Useful Links:

[NIST Quickstart Guide](#)

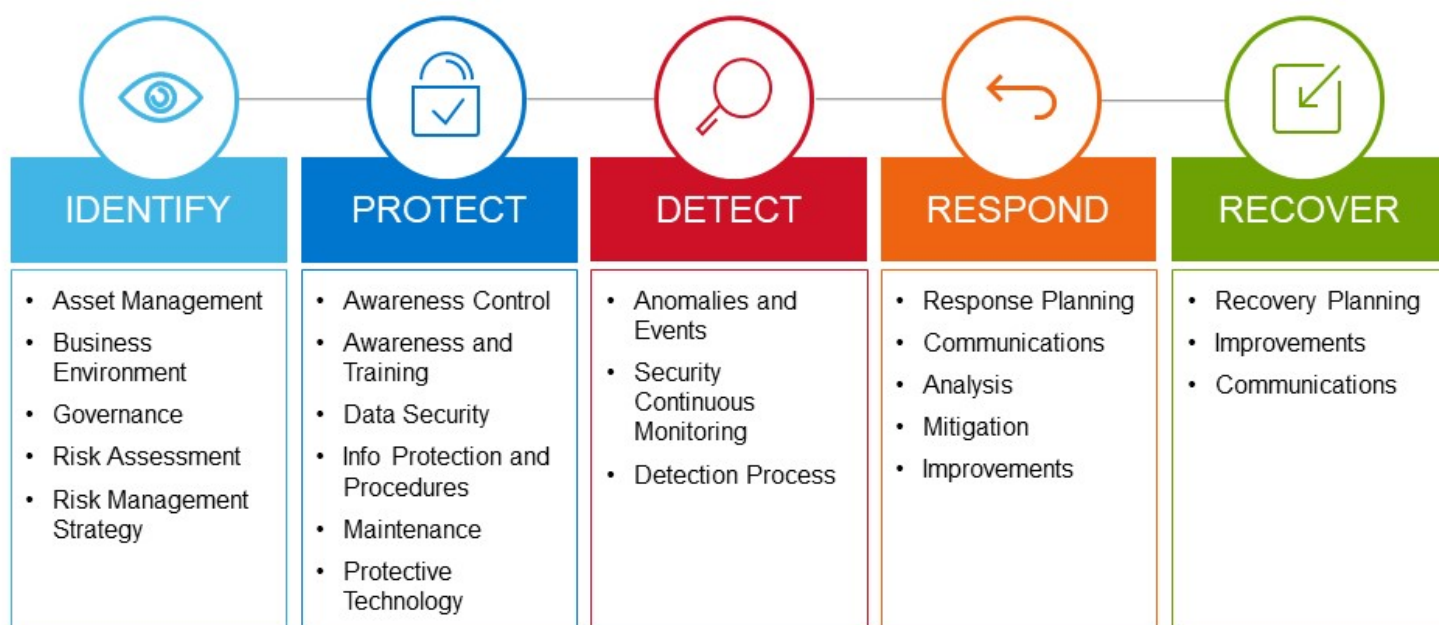
[Framework for Improving Critical Infrastructure Cybersecurity](#)

[Data Breach Response: A Guide for Business](#)

[NIST Events and Presentations](#)

[Twitter - @NISTcyber](#)

## NIST Cybersecurity Framework Overview



\*Image used from <https://tinyurl.com/27wqx2gn>

### Incident Response Plan

An incident response plan is a set of procedures that a company puts in place to manage and mitigate the impact of a security incident, such as a data breach or a cyber attack.

The theory behind an incident response plan is that it helps a company to be prepared for and respond effectively to a security incident, which can minimize the damage and reduce the

chances of it happening again in the future.

There are several reasons why businesses need an incident response plan:

1. **To minimize the impact of a security incident:** An incident response plan helps a company to identify and address the source of a security incident as quickly as possible, which can help to minimize the damage and reduce the chances of it spreading.
2. **To meet regulatory requirements:** Many industries have regulations that require companies to have an incident response plan in place. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires merchants and other organizations that accept credit cards to have an incident response plan.
3. **To protect reputation:** A security incident can damage a company's reputation, which can lead to a loss of customers and revenue. An incident response plan can help a company to manage the situation and minimize the damage to its reputation.
4. **To reduce the cost of a security incident:** The cost of a security incident can be significant, including the cost of remediation, legal fees, and lost business. An incident response plan can help a company to minimize these costs by providing a roadmap for responding to the incident.

## Useful Links:

[National Cyber Security Centre - Incident Response overview](#)

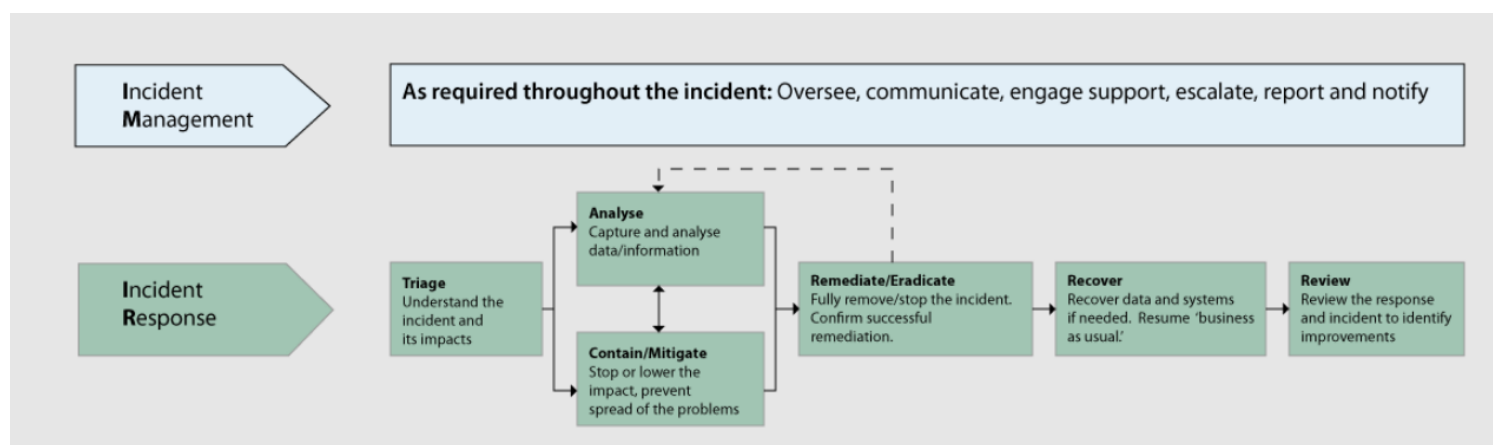
[SANS - Security Policy Templates](#)

[SANS - Incident Handler's Handbook](#)

[FRSecure - Incident Response Plan Template](#)

[Cybersecurity and Infrastructure Security Agency - CYBER INCIDENT RESPONSE](#)

[FBI - Incident Response Policy](#)



## Ransomware Response Plan

Ransomware is a type of malicious software that encrypts a victim's files. The attackers then demand a ransom from the victim to restore access to the files; hence the name ransomware.

The theory behind a ransomware response plan is that it helps a company to be prepared for and respond effectively to a ransomware attack, which can minimize the impact of the attack and reduce the chances of it happening again in the future.

There are several reasons why businesses need a ransomware response plan:

1. **To minimize the impact of a ransomware attack:** A ransomware response plan helps a company to identify and address a ransomware attack as quickly as possible, which can help to minimize the damage and reduce the chances of the ransomware spreading to other systems.
2. **To protect against data loss:** Ransomware attacks can result in the loss of important data, which can be costly and disruptive for a business. A ransomware response plan can help a company to recover from an attack and avoid data loss.
3. **To protect reputation:** A ransomware attack can damage a company's reputation, which can lead to a loss of customers and revenue. A ransomware response plan can help a company to manage the situation and minimize the damage to its reputation.
4. **To reduce the cost of a ransomware attack:** The cost of a ransomware attack can be significant, including the cost of remediation, legal fees, and lost business. A ransomware response plan can help a company to minimize these costs by providing a roadmap for responding to the attack.

### Useful Links:

[National Cyber Security Centre - Mitigating malware and ransomware attacks](#)

[NIST - Ransomware Protection and Response](#)

[Cybersecurity and Infrastructure Security Agency - Ransomware Guide](#)

[Microsoft Security - Ransomware response](#)

[Blog - Creating a Ransomware Response Plan](#)

## Steps you can take *now* to help you **RECOVER** from a *future* ransomware attack:

1

### **MAKE AN INCIDENT RECOVERY PLAN**

Develop and implement an incident recovery plan with defined roles and strategies for decision making.



2

### **BACKUP & RESTORE**

Carefully plan, implement, and test a data backup and restoration strategy – and secure and isolate backups of important data.

3

### **KEEP YOUR CONTACTS**

Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.



Image used from <https://tinyurl.com/2y2xqrzw>

## **Incident Response Reference Guide**

This is a “first aid” style of guidance for cybersecurity to help you prepare for a crisis and limit the potential damage in a crisis.

This includes tips and guidance for technical, operational, legal, and communications aspects of a major cybersecurity incident.

### **Key Takeaways**

- **Preparation pays off** – Preparing for a major incident can reduce damage to the organization, as well as reduce incident cost and management difficulty.
- **Operationalize your incident management processes** – Managing major cybersecurity incidents must be part of standard business risk management processes.
- **Coordination is critical** – Effective cybersecurity incident management requires collaboration and coordination of technical, operations, communications, legal, and governance functions.
- **Stay calm and do no harm in an incident** – Overreacting can be as damaging as underreacting.

You can read the paper [here](#).



# INCIDENT RESPONSE REFERENCE GUIDE

First aid tips and preparation guidance to  
limit damage and protect your mission

Image used from <https://tinyurl.com/y5zc3npf>

## **Awesome Incident Response**

A curated list of tools and resources for security incident response, aimed to help security analysts and **DFIR** teams.

This is a great resource full of links for different aspects of incident response, including:

- Adversary Emulation
- All-In-One Tools
- Books
- Communities
- Disk Image Creation Tools

Visit the resource [here](#).

# Awesome Incident Response

A curated list of tools and resources for security incident response, aimed to help security analysts and DFIR teams.

Digital Forensics and Incident Response (DFIR) teams are groups of people in an organization responsible for managing the response to a security incident, including gathering evidence of the incident, remediating its effects, and implementing controls to prevent the incident from recurring in the future.

## Contents

- [Adversary Emulation](#)
- [All-In-One Tools](#)
- [Books](#)
- [Communities](#)
- [Disk Image Creation Tools](#)
- [Evidence Collection](#)
- [Incident Management](#)

Image used from <https://tinyurl.com/hnaj7lc>

# Malware Detection and Analysis

*Tools for detecting and analyzing malware, including antivirus software and forensic analysis tools.*

## [VirusTotal](#)

VirusTotal is a website and cloud-based tool that analyzes and scans files, URLs, and software for viruses, worms, and other types of malware.

When a file, URL, or software is submitted to VirusTotal, the tool uses various antivirus engines and other tools to scan and analyze it for malware. It then provides a report with the results of the analysis, which can help security professionals and blue teams identify and respond to potential threats.

VirusTotal can also be used to check the reputation of a file or URL, and to monitor for malicious activity on a network.

Visit <https://tinyurl.com/y2dpvfye>

## Usage:

```
# Recently created documents with macros embedded, detected at least by 5 AVs  
(type:doc OR type: docx) tag:macros p:5+ generated:30d+
```

```
# Excel files bundled with powershell scripts and uploaded to VT for the last 10  
days  
(type:xls OR type:xlsx) tag:powershell fs:10d+
```

```
# Follina-like exploit payloads  
entity:file magic:"HTML document text" tag:powershell have:itw_url
```

```
# URLs related to specified parent domain/subdomain with a specific header in  
the response  
entity:url header_value:"Apache/2.4.41 (Ubuntu)" parent_domain:domain.org
```

```
# Suspicious URLs with a specific HTML title  
entity:url ( title:"XY Company" or title:"X.Y. Company" or title:"XYCompany" ) p:
```

Full documentation can be found [here](#).

## VT INTELLIGENCE CHEAT SHEET



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Choose file

Image used from <https://tinyurl.com/y2dpvfye>



\*Image used from <https://tinyurl.com/2yrvna4a>



Ghidra is a free, open-source software reverse engineering tool developed by the National Security Agency (NSA). It is used to analyze compiled and executable code, including malware.

Ghidra allows users to disassemble code, decompile it into a higher-level programming language, and view and edit the resulting source code. This can be useful for identifying vulnerabilities, analyzing malware, and understanding how a program works.

Ghidra also includes a range of features and tools that support SRE tasks, such as debugging, code graphing, and data visualization. Ghidra is written in Java and is available for Windows, MacOS, and Linux.

### **Install:**

1. Download the latest release from [here](#).
2. Extract the zip

Full installation and error fix information can be found [here](#).

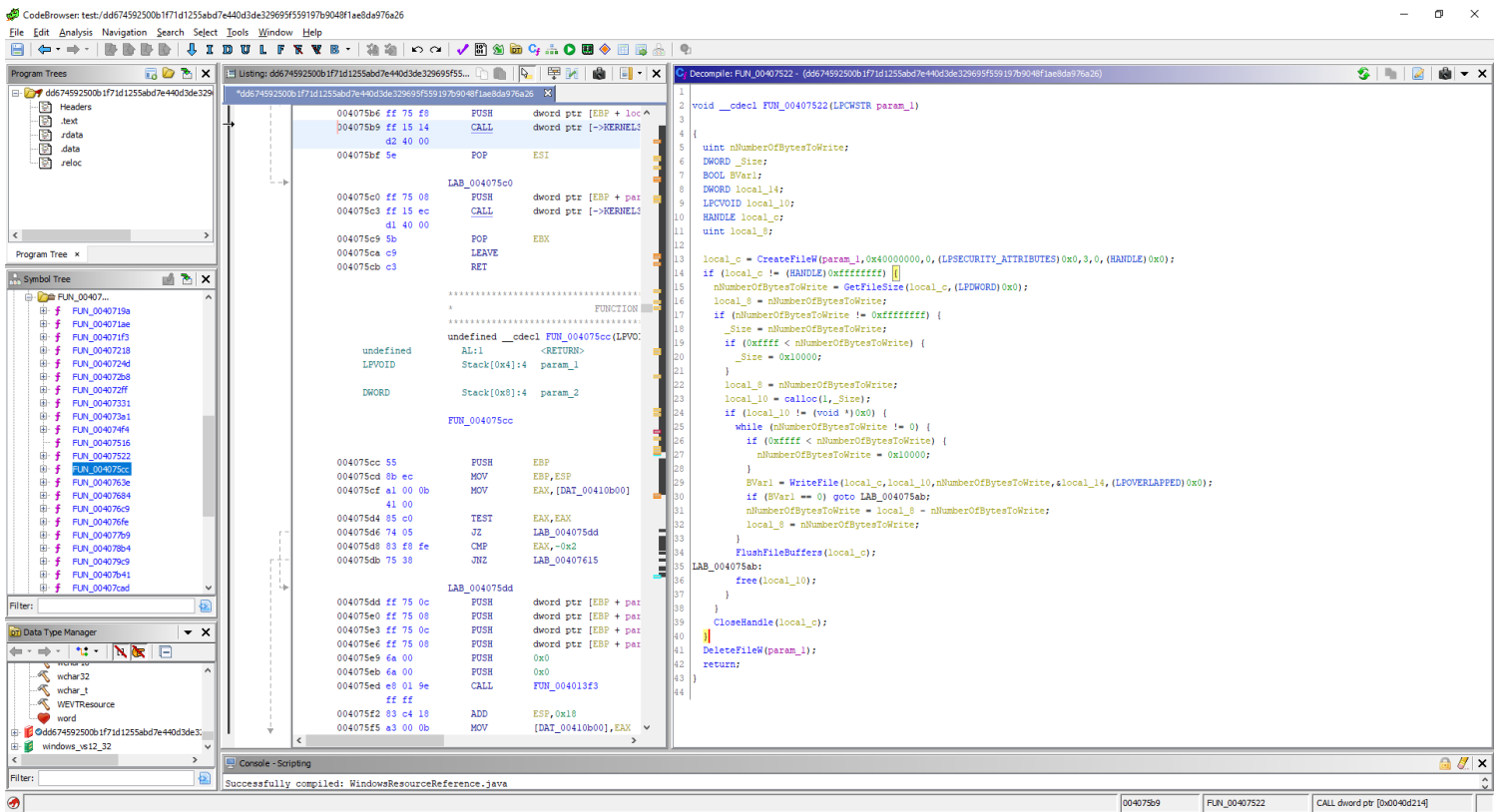
### **Usage:**

1. Navigate to the unzipped folder

```
# Windows  
ghidraRun.bat
```

```
# Linux  
./ghidraRun
```

If Ghidra failed to launch, see the [Troubleshooting](#) link.



\*Image used from <https://tinyurl.com/2ar6965b>

## ← decode-vbe

Script Encoding was introduced by Microsoft (long ago) to prevent people from being able to read, understand and alter VBScript files.

Encoded scripts are unreadable but still able to execute, making it a popular mechanism with threat actors looking to hide their malicious code, IOCs, hardcoded C2 domains etc whilst still being able to achieve execution.

The decode-vbe script can be used to convert encoded VBE files back to plaintext for analysis.

Nice blog about VBE files [here](#).

### Install:

```
git clone https://tinyurl.com/2bnb9y9a
cd DidierStevensSuite
```

### Usage:

```
# Decode literal string
decode-vbe.py "##@~^DgAAAA==\ko$K6,JC[V^GJqAQAAA==^#~@"
```



```
# Decode hexadecimal (prefix #h#)
```

```
decode-vbe.py #h#23407E5E4467414141413D3D5C6B6F244B362C4A437F565E474A714151414141
```

```
# Decode base64 (prefix #b#)
```

```
decode-vbe.py #b#I0B+XkRnQUFBQT09XGtvJEs2LEpDf1ZeR0pxQVFBQUE9PV4jfkA=
```



Pafish is a testing tool that uses different techniques to detect virtual machines and malware analysis environments in the same way that malware families do.

The project is free and open source; the code of all the anti-analysis techniques is publicly available. Pafish executables for Windows (x86 32-bit and 64-bit) can be downloaded from the [releases page](#).

### Install: (Build)

Pafish is written in C and can be built with Mingw-w64 and make.

The wiki page "[How to build](#)" contains detailed instructions.

### Usage:

```
pafish.exe
```

```
* Pafish (Paranoid Fish) *
[-] Windows version: 6.2 build 9200
[-] Running in WoW64: False
[-] CPU: AuthenticAMD
    CPU brand: AMD Ryzen 7 2700X Eight-Core Processor

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using BeingDebugged via PEB access ... OK

[-] CPU information based detections
[*] Checking the difference between CPU timestamp counters (rdtsc) ... OK
[*] Checking the difference between CPU timestamp counters (rdtsc) forcing VM exit ... OK
[*] Checking hypervisor bit in cpuid feature bits ... OK
[*] Checking cpuid hypervisor vendor for known VM vendors ... OK

[-] Generic reverse turing tests
[*] Checking mouse presence ... OK
[*] Checking mouse movement ... OK
[*] Checking mouse speed ... OK
[*] Checking mouse click activity ... traced!
[*] Checking mouse double click activity ... traced!
[*] Checking dialog confirmation ... traced!
[*] Checking plausible dialog confirmation ... traced!
```

Image used from <https://tinyurl.com/7mv22ty>

Lookyloo is a web interface that captures a webpage and then displays a tree of the domains, that call each other.

Use Lookyloo to map the journey a website page takes - from entering the initial URL address to the various redirects to third-party affiliations.

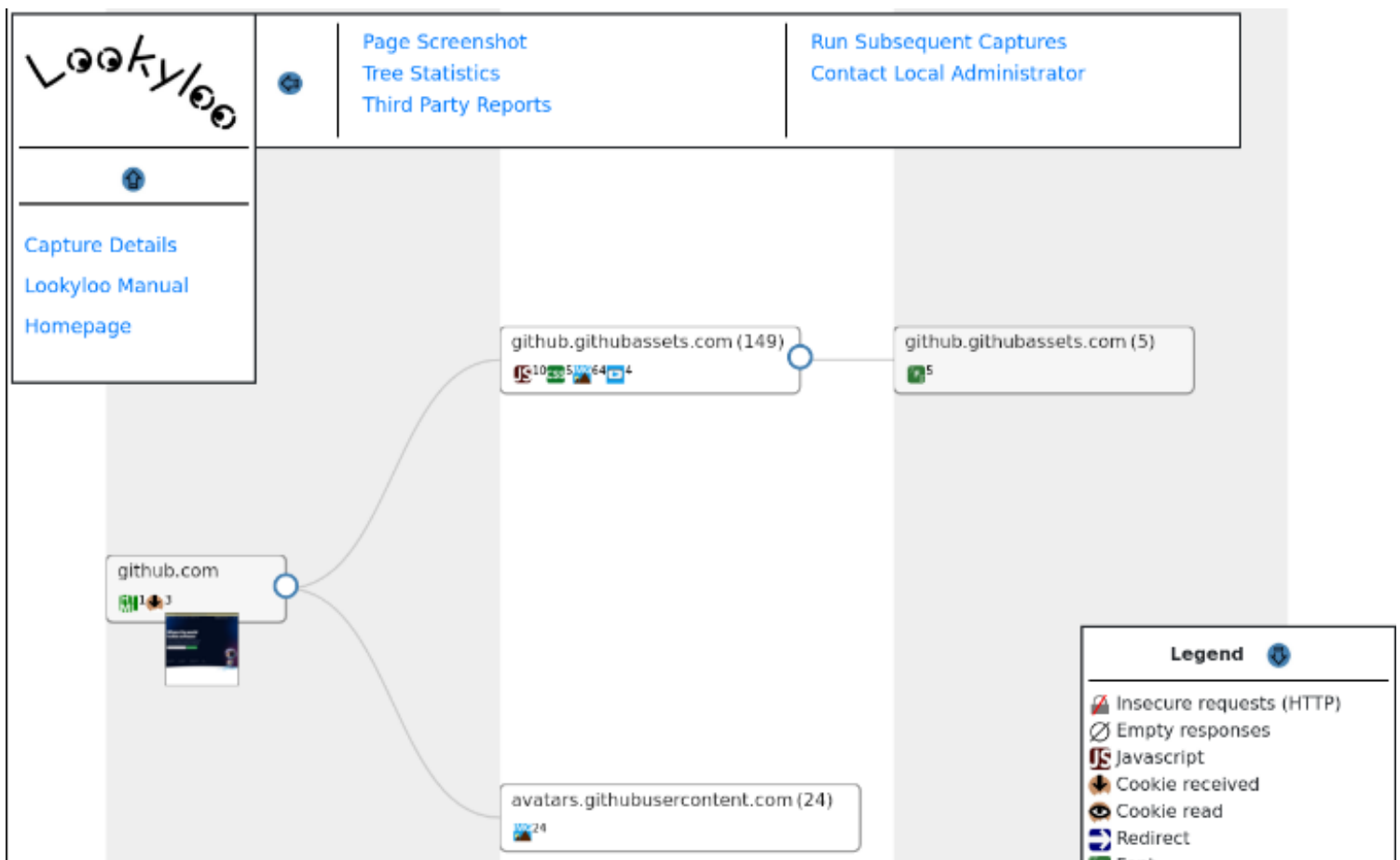
### Install:

```
git clone https://tinyurl.com/24zze3sl.git
cd lookyloo
poetry install
echo LOOKYLOO_HOME="`pwd`" > .env
```

Full installation instructions can be found [here](#).

### Usage:

Once installed and running, lookyloo can be operated via the web interface hosted locally.



\*Image used from <https://tinyurl.com/26xtghsa>

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic.

### Install:

```
tar -zxf yara-4.2.0.tar.gz
cd yara-4.2.0
./bootstrap.sh
sudo apt-get install automake libtool make gcc pkg-config
git clone https://tinyurl.com/yysfssd7
cd yara
./bootstrap.sh
./configure
make
sudo make install
```

Full installation instructions can be found [here](#).

### Usage:

```
# Apply rule in /foo/bar/rules to all files in the current directory
yara /foo/bar/rules .

# Scan all files in the /foo directory and its subdirectories:
yara /foo/bar/rules -r /foo
```

Nice YARA cheatsheet [here](#).

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

\*Image used from <https://tinyurl.com/29fujrt9>

## Cuckoo Sandbox

Cuckoo is an open source automated malware analysis system.

It's used to automatically run and analyze files and collect comprehensive analysis results that outline what the malware does while running inside an isolated operating system.

It can retrieve the following type of results:

- Traces of calls performed by all processes spawned by the malware.
- Files being created, deleted and downloaded by the malware during its execution.
- Memory dumps of the malware processes.
- Network traffic trace in PCAP format.
- Screenshots taken during the execution of the malware.
- Full memory dumps of the machines.

### Install:

For installation follow the docs [here](#).

### Usage:

For usage follow the docs [here](#).

## radare2

Radare2 provides a set of libraries, tools and plugins to ease reverse engineering tasks.

r2 is a featureful low-level command-line tool with support for scripting. r2 can edit files on local hard drives, view kernel memory, and debug programs locally or via a remote gdb server. r2's wide architecture support allows you to analyze, emulate, debug, modify, and disassemble any binary.

## Install:

```
git clone https://tinyurl.com/y3tvmeoq
radare2/sys/install.sh
```

## Usage:

```
$ r2 /bin/ls # open the binary in read-only mode
> aaa # same as r2 -A, analyse the binary
> afl # list all functions (try aflt, aflm)
> px 32 # print 32 byte hexdump current block
> s sym.main # seek to the given offset (by flag name, number, ..)
> f~foo # filter flags with ~grep (same as |grep)
> iS;is # list sections and symbols (same as rabin2 -Ss)
> pdf; agf # print function and show control-flow-graph in ascii-art
> oo+;w hello # reopen in rw mode and write a string in the current offset
> ?*~... # interactive filter all command help messages
> q # quit
```

Great usage book [here](#).

The screenshot displays the Radare2 GUI with several panels open:

- Registers (r):** Lists registers like rax, rbx, rcx, etc., with their current values.
- Disassembly (pd):** Shows assembly code for a function, including instructions like `jne 0x7172`, `lea rdi, [rcx + rcx*2]`, and `call fcn.000158c0`.
- Functions (afl):** Lists detected functions such as `entry0`, `syn_obstack_memory_used`, and `syn_obstack_free`.
- Entropy (fir):** Shows a bar chart representing entropy values across different sections of the binary.
- Hexdump (xc \$r\*16):** Displays a hex dump of memory at offset 0x00007bd1, showing hex values and their ASCII representations.

Image used from <https://tinyurl.com/y3tvmeoq>



dnSpy is a debugger and .NET assembly editor. You can use it to edit and debug assemblies.

Main features:

- Debug .NET and Unity assemblies
- Edit .NET and Unity assemblies

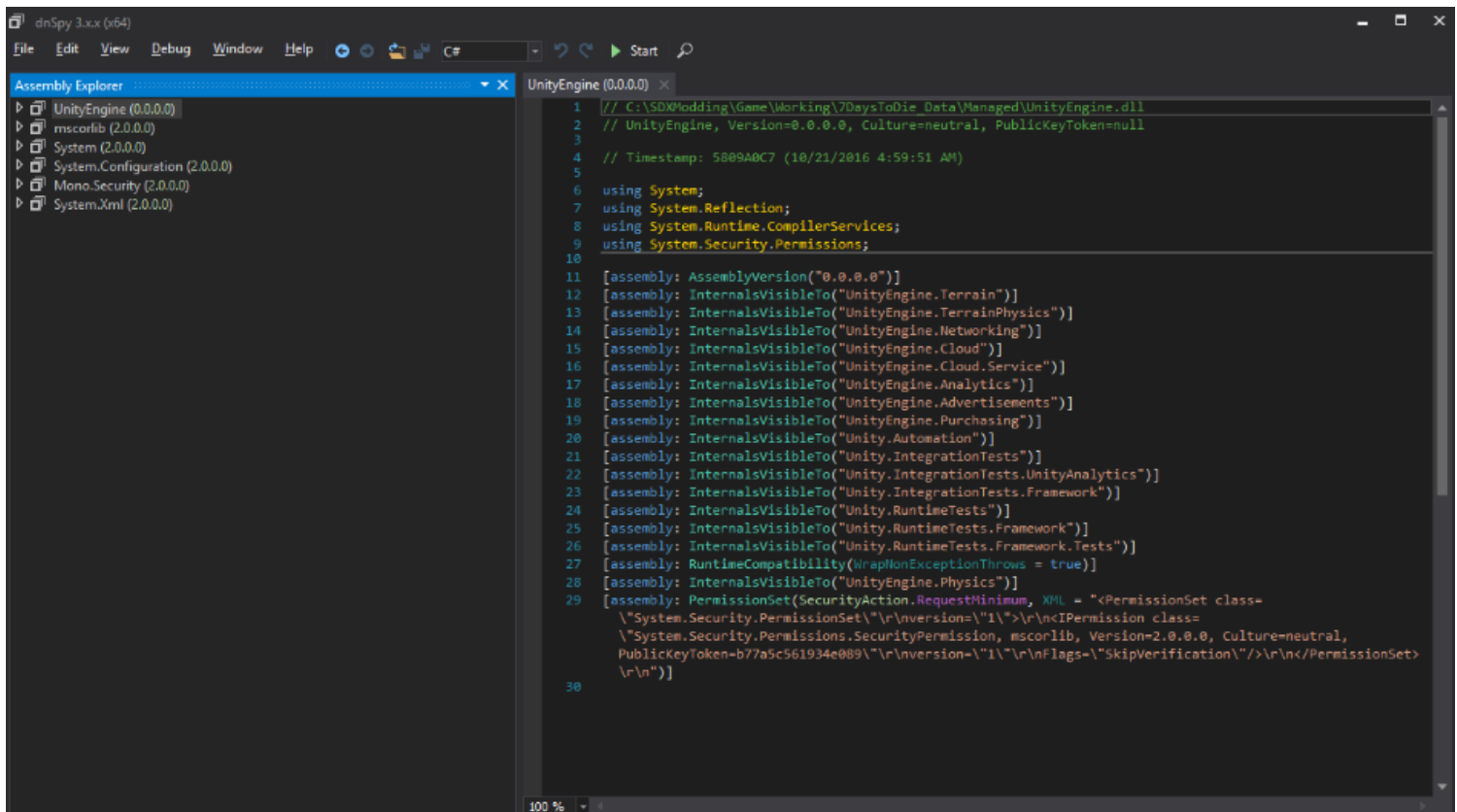
Install: (Build)

```
git clone --recursive https://tinyurl.com/y7k9r2zy.git
cd dnSpy
./build.ps1 -NoMsbuild
```

Usage:

dnSpy.exe

Nice tutorial page [here](#).



\*Image used from <https://tinyurl.com/26nk9ksx>



This is a site with over 2,200 blog entries about malicious network traffic. Almost every post on the site has pcap files or malware samples (or both).

The site also contains a number of traffic analysis exercises, including technical blog posts outlining techniques being used by threat actors.

### Usage:

Visit <https://tinyurl.com/28fywkuw>.



[RSS feed](#)

[About this blog](#)

[@malware\\_traffic on Mastodon](#)

[@malware\\_traffic on Twitter](#)

### A source for packet capture (pcap) files and malware samples...

Since the summer of 2013, this site has published over 2,200 blog entries about malicious network traffic. Almost every post on this site has pcap files or malware samples (or both).

#### Traffic Analysis Exercises

- [Click here](#) -- for training exercises to analyze pcap files of network traffic. [Click here](#) -- for some tutorials that will help for these exercises.

#### My Technical Blog Posts

- My technical blog posts by year - [\[2013\]](#) - [\[2014\]](#) - [\[2015\]](#) - [\[2016\]](#) - [\[2017\]](#) - [\[2018\]](#) - [\[2019\]](#) - [\[2020\]](#) - [\[2021\]](#) - [\[2022\]](#) - [\[2023\]](#)

#### My Pastebin Posts

- From December 2018 through December 2020 I occasionally posted information to Pastebin, so [click here](#) for posts from my Pastebin account.

#### My Github Posts

- After giving up Pastebin for posting IOCs, I started usin Github, so [click here](#) for posts from my Github account.

#### My Non-Technical Blog Posts

- [Click here](#) -- for non-technical blog posts I've written about on topics related to information security (infosec).

#### Guest Blog Posts

- [Click here](#) -- for write-ups from other people that I've edited and posted here on the blog.

Image used from <https://tinyurl.com/28fywkuw>

## Data Recovery

*Tools for recovering data from damaged or corrupted systems and devices.*

Recuva is a data recovery tool that can be used to recover deleted files from your computer.

It is often used to recover deleted files that may contain valuable information, such as deleted logs or documents that could be used to investigate a security incident.

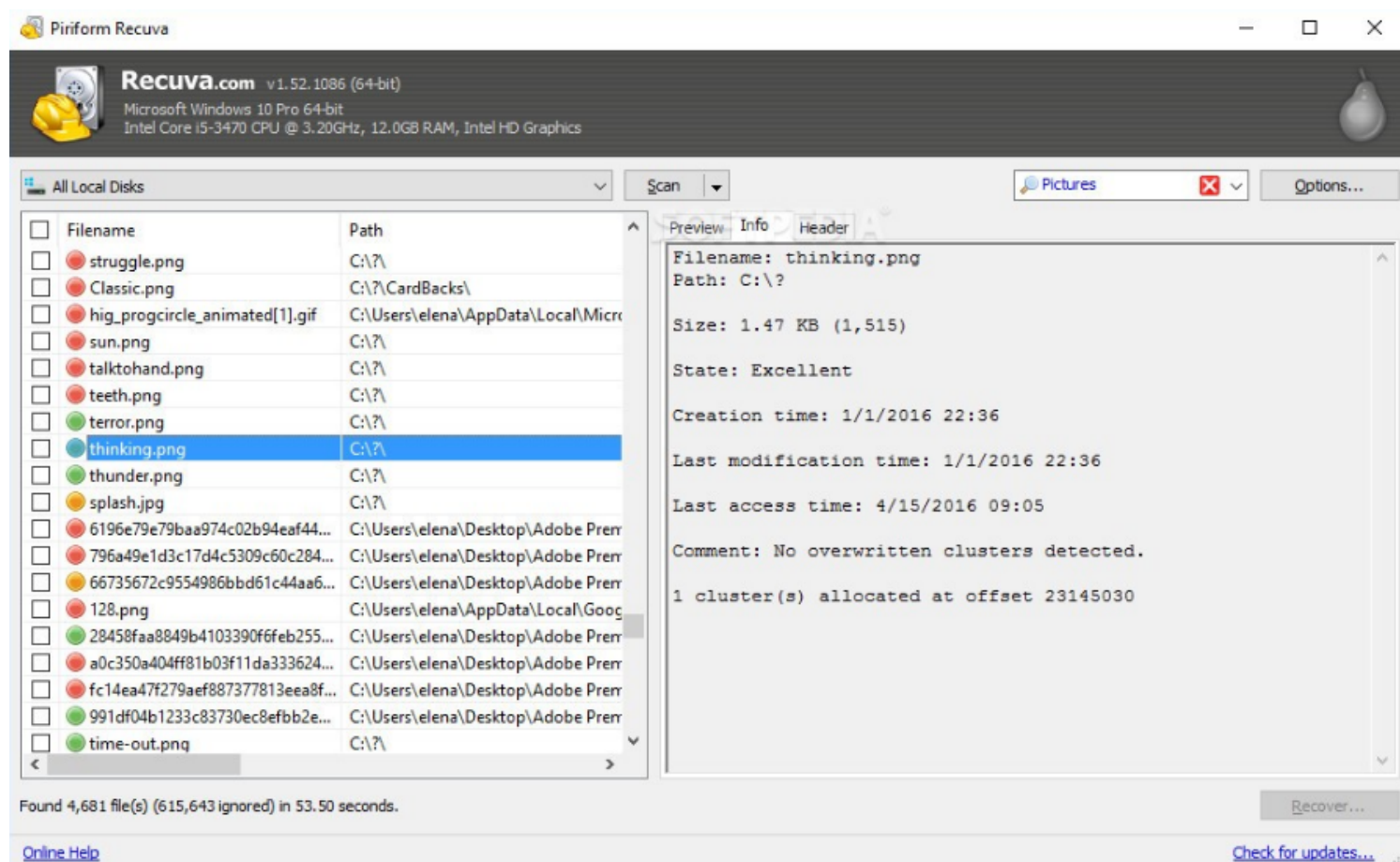
Recuva can recover files from hard drives, USB drives, and memory cards, and it is available for Windows and Mac operating systems.

## Install:

You can download the tool from [here](#).

## Usage:

Nice step by step [guide](#).



\*Image used from <https://tinyurl.com/28dwkgop>

## ← Extundelete

Extundelete is a utility that can be used to recover deleted files from an ext3 or ext4 file system.

It works by searching the file system for blocks of data that used to belong to a file, and then attempting to recreate the file using those blocks of data. It is often used to recover important files that have been accidentally or maliciously deleted.

## Install:

You can download the tool from [here](#).

## Usage:

```
# Prints information about the filesystem from the superblock.  
--superblock  
  
# Attempts to restore the file which was deleted at the given filename, called as  
--restore-file path/to/deleted/file  
  
# Restores all files possible to undelete to their names before deletion, when po  
--restore-all
```

Full usage information can be found [here](#).

```
root@bt:~# umount /media/a19846b1-aa4f-4926-8c23-28162de81383/  
root@bt:~# extundelete --restore-file 'a.txt' /dev/sdc1  
WARNING: Extended attributes are not restored.  
Loading filesystem metadata ... 64 groups loaded.  
Loading journal descriptors ... 90 descriptors loaded.  
Writing output to directory RECOVERED_FILES/  
Restored inode 12 to file RECOVERED_FILES/a.txt  
root@bt:~# md5deep RECOVERED_FILES/a.txt  
a92a6aed4fa75cebc5a30bd879963c31 /root/RECOVERED_FILES/a.txt
```

\*Image used from <https://tinyurl.com/285dmg82>

## ← TestDisk

TestDisk is a free and open-source data recovery software tool that is designed to help recover lost partitions and make non-booting disks bootable again. It is useful for both computer forensics and data recovery.

It can be used to recover data that has been lost due to a variety of reasons, such as accidental deletion, formatting, or corruption of the partition table.

TestDisk can also be used to repair damaged boot sectors, recover deleted partitions, and recover lost files. It supports a wide range of file systems, including FAT, NTFS, and ext2/3/4, and can be used to recover data from disks that are damaged or formatted with a different file system than the one they were originally created with.

## Install:

You can download the tool from [here](#).

## Usage:

Full usage examples [here](#).

```
TestDisk 7.0-WIP, Data Recovery Utility, April 2014  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org
```

```
TestDisk is free data recovery software designed to help recover lost  
partitions and/or make non-booting disks bootable again when these symptoms  
are caused by faulty software, certain types of viruses or human error.  
It can also be used to repair some filesystem errors.
```

```
Information gathered during TestDisk use can be recorded for later  
review. If you choose to create the text file, testdisk.log, it  
will contain TestDisk options, technical information and various  
outputs; including any folder/file names TestDisk was used to find and  
list onscreen.
```

```
Use arrow keys to select, then press Enter key:
```

```
>[ Create ] Create a new log file  
[ Append ] Append information to log file  
[ No Log ] Don't record anything
```

\*Image used from <https://tinyurl.com/2bhxjwm5>

## Digital Forensics

*Tools for conducting forensic investigations of digital devices and systems, including tools for collecting and analyzing evidence.*



SANS SIFT (SANS Investigative Forensic Toolkit) is a powerful toolkit for forensic analysis and incident response.

It is a collection of open source and commercial tools that can be used to perform forensic analysis on a wide range of systems, including Windows, Linux, and Mac OS X. The SANS SIFT kit is designed to be run on a forensic workstation, which is a specialized computer that is used to perform forensic analysis on digital evidence.

The SANS SIFT kit is particularly useful for blue teamers, as it provides a wide range of tools and resources that can be used to investigate incidents, respond to threats, and perform forensic analysis on compromised systems.

## Install:

1. Visit <https://tinyurl.com/2mr9sunr>.
2. Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine.
3. Once you have booted the virtual machine, use the credentials below to gain access.

Login = sansforensics

Password = forensics

**Note:** Use to elevate privileges to root while mounting disk images.

Additional install options [here](#).

## Usage:

```
# Registry Parsing - Regripper
rip.pl -r <HIVEFILE> -f <HIVETYPE>

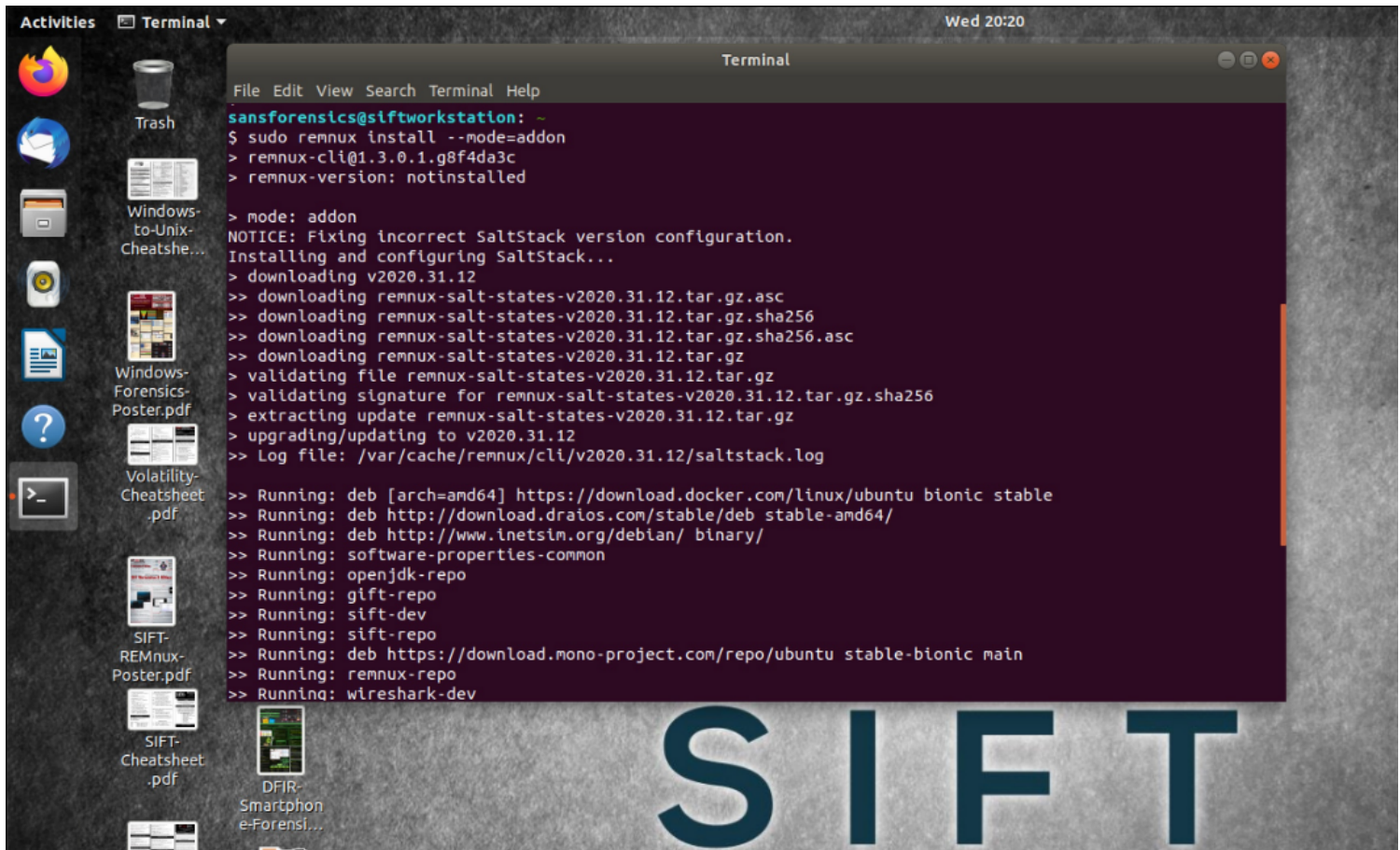
# Recover deleted registry keys
deleted.pl <HIVEFILE>

# Mount E01 Images
ewfmount image.E01 mountpoint
mount -o

# Stream Extraction
bulk_extractor <options> -o output_dir
```

Full usage guide [here](#).





\*Image used from <https://tinyurl.com/23jv2sqt>

## ← The Sleuth Kit

The Sleuth Kit is a collection of command line tools that can be used to analyze disk images and recover files from them.

It is primarily used by forensic investigators to examine digital evidence after a computer has been seized or an image of a disk has been made. It can be useful because it can help understand what happened during a security incident and identify any malicious activity.

The tools in The Sleuth Kit can be used to extract deleted files, analyze disk partition structures, and examine the file system for evidence of tampering or unusual activity.

### Install:

Download tool from [here](#).

### Usage:

Link to [documentation](#).



# The Sleuth Kit

## DIGITAL FORENSIC TOOL



\*Image used from <https://tinyurl.com/29szuv3j>

### **Autopsy**

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools.

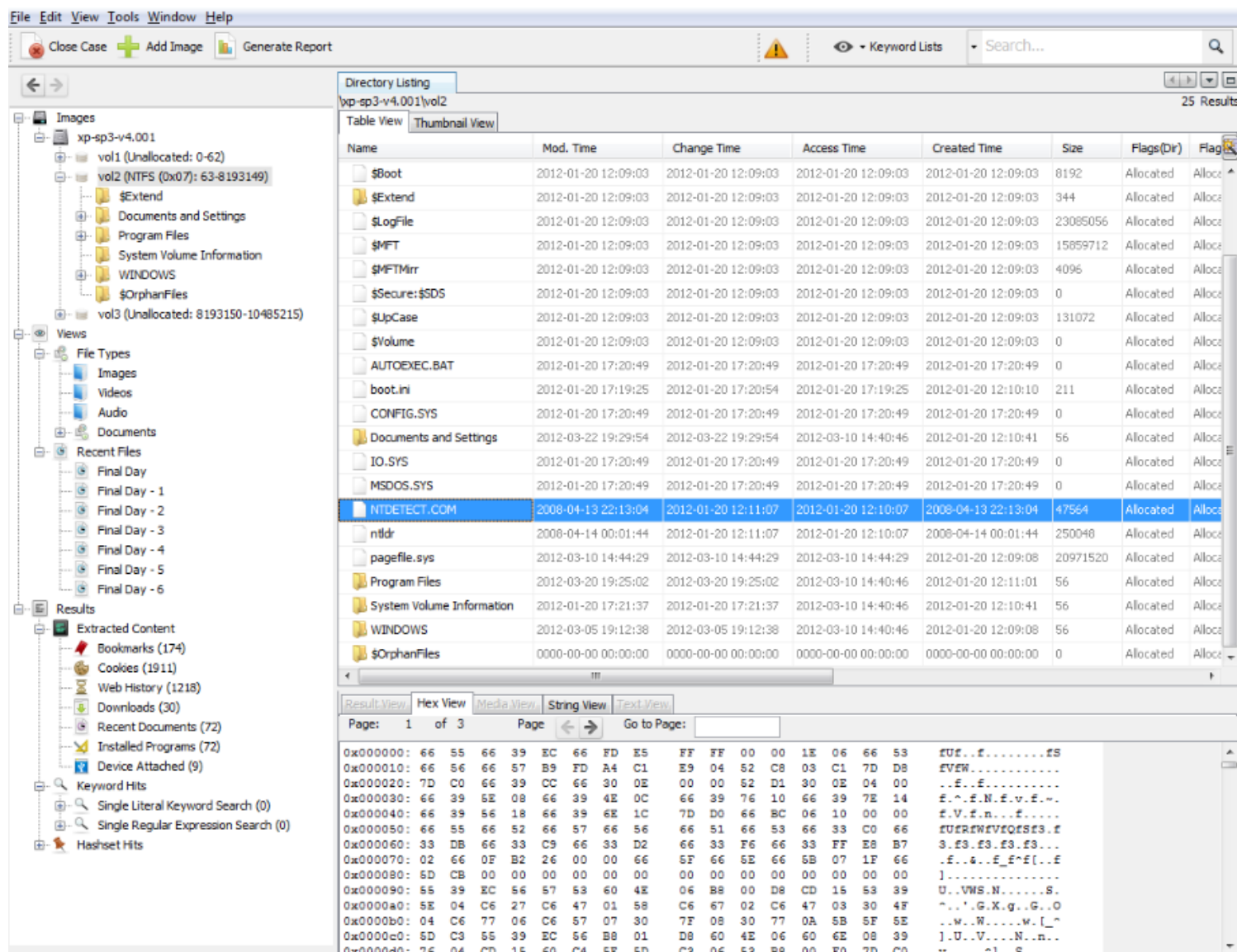
It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can use it to analyze disk images and recover files, as well as to identify system and user activity.

Autopsy is used by "blue teams" (the cybersecurity professionals who defend organizations against attacks) to conduct forensic analysis and incident response. It can help blue teams understand the nature and scope of an attack, and identify any malicious activity that may have occurred on a computer or network.

### **Install:**

Download the tool from [here](#).

### **Usage:**



\*Image used from <https://tinyurl.com/23mz9obj>

## Security Awareness Training

Tools for training employees and other users on how to recognize and prevent potential security threats.

[BACK](#) TryHackMe

TryHackMe is a platform that offers a variety of virtual machines, known as "rooms," which are designed to teach cybersecurity concepts and skills through hands-on learning.

These rooms are interactive and gamified, allowing users to learn about topics such as web

vulnerabilities, network security, and cryptography by solving challenges and completing tasks.

The platform is often used for security awareness training, as it provides a safe and controlled environment for users to practice their skills and learn about different types of cyber threats and how to defend against them.

Visit [<https://tinyurl.com/25v4spm>) and create an account.

[TryHackMe - Getting Started Guide](#)

**Useful links:**

[Pre-Security Learning Path](#)

[introduction to Cyber Security Learning Path](#)

Visit the [hacktivities](#) tab for a full list of available rooms and modules.



\*Image used from <https://tinyurl.com/2ybqwf3z>

[← HackTheBox](#)

HackTheBox is a platform for practicing and improving your hacking skills.

It consists of a set of challenges that simulate real-world scenarios and require you to use your knowledge of various hacking techniques to solve them. These challenges are designed to test your knowledge of topics such as network security, cryptography, web security, and more.

HackTheBox is often used by security professionals as a way to practice and improve their skills,

and it can also be a useful resource for security awareness training. By working through the challenges and learning how to solve them, individuals can gain a better understanding of how to identify and mitigate common security threats.

Visit [<https://tinyurl.com/29zot4mw>) and create an account.

### Useful links:

[Blog - Introduction to Hack The Box](#)

[Blog - Learn to Hack with Hack The Box: The Beginner's Bible](#)

[Blog - Introduction to Starting Point](#)



# HACKTHEBOX

Image used from <https://tinyurl.com/ycrlsadmlogin>

[← BACK](#) **PhishMe**

PhishMe is a company that provides security awareness training to help organizations educate their employees about how to identify and prevent phishing attacks.

PhishMe's training programs aim to teach employees how to recognize and report phishing attempts, as well as how to protect their personal and professional accounts from these types of attacks.

The company's training programs can be customized to fit the needs of different organizations and can be delivered through a variety of mediums, including online courses, in-person training,

and simulations.

Request a demo from [here](#).

Useful links:

[Cofense Blog](#)

[Cofense Knowledge Center](#)

## END-TO-END EMAIL SECURITY BUILT TO STOP THREATS.

Defend your organization with our complete suite of email security solutions.



Image used from <https://tinyurl.com/2a5f1959>

# Communication and Collaboration

Tools for coordinating and communicating with team members during an incident, including chat, email, and project management software.

[← BACK](#) **Twitter**

Twitter is a great platform for sharing information about cyber security.

It's a platform that is widely used by security professionals, researchers, and experts, giving you access to an endless amount of new information.

Some great accounts to follow:

- [@vxunderground](#)
- [@Alh4zr3d](#)
- [@3xp0rtblog](#)
- [@C5pider](#)
- [@\\_JohnHammond](#)
- [@mrd0x](#)

- [@TheHackersNews](#)
- [@pancak3stack](#)
- [@GossiTheDog](#)
- [@briankrebs](#)
- [@SwiftOnSecurity](#)
- [@schneierblog](#)
- [@mikko](#)
- [@campuscodi](#)

## **Facebook ThreatExchange**

Facebook ThreatExchange is a platform for security professionals to share and analyze information about cyber threats.

It was designed to help organizations better defend against threats by allowing them to share threat intelligence with each other in a private and secure way.

It is intended to be used by "blue teams", who are responsible for the security of an organization and work to prevent, detect, and respond to cyber threats.

### **Usage:**

To request access to ThreatExchange, you have to submit an application via <https://developers.facebook.com/products/threat-exchange/>.

### **Useful links:**

[Welcome to ThreatExchange!](#)

[ThreatExchange UI Overview](#)

[ThreatExchange API Reference](#)

[GitHub - ThreatExchange](#)