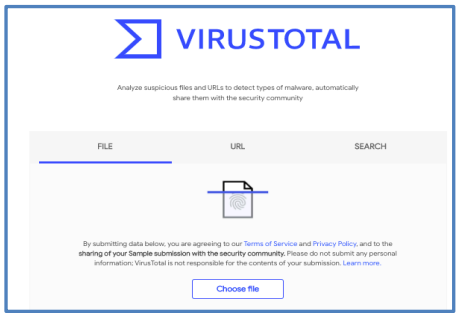
(U) Open Source Malware Analysis Tools

(U) Scope Note **2 October 2020**

(U) Cybersecurity sharing of threat information is critical to preventing cyber-attacks. The Hawaii State Fusion Center (HSFC) recently developed an ongoing series of cyber security intelligence reports that focus on specific cyber threats which could potentially impact our critical infrastructure partners.

(U) The following is a collection of open source analysis tools to assist individuals in identifying malicious activity that may affect their systems. The list includes online scan engines, malware analysis portals, email header message analyzers, and web browsers that block ads and website trackers.

(U) Virus Total



(U) VirusTotal was launched in June 2004 and acquired by Google Inc., in September 2012. VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives. Files up to 550 MB can be uploaded to the website or sent via email.[1,2]

(U) Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and VirusTotals' own capability. Users can also scan suspect URLs and search through the VirusTotal dataset. VirusTotal for dynamic analysis of malware uses the Cuckoo sandbox.[3,4]

(U) VirusTotal: https://www.virustotal.com/gui/

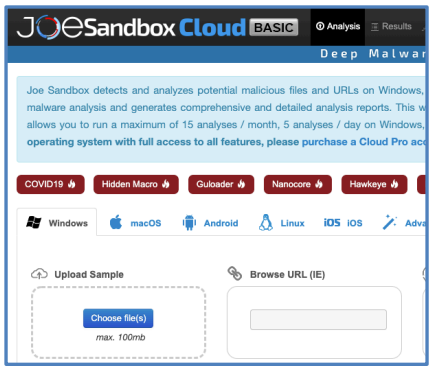
(U) Hybrid Analysis

(U) Hybrid Analysis, recently acquired by CrowdStrike, is a free malware analysis service for the cyber community. Using this service, individuals can submit files for in-depth static and dynamic analysis. Hybrid Analysis utilizes Falcon Sandbox which is a high-end malware analysis framework. It can be implemented as a large-scale system processing hundreds of thousands of files automatically (by using the simple REST API) or as a webservice for incident response, forensics and/or as an enterprise self-service portal.[5]

(U) Due to its simple interface and numerous integration capabilities with other technology providers, Falcon Sandbox seamlessly enriches a SOCs incident response workflow and security stack. Falcon Sandbox is currently in use by SOCs, CERTs, IT-security forensic labs, researchers and threat intelligence service providers throughout the world.[6]

(U) Hybrid Analysis: https://www.hybrid-analysis.com/

(U) Joe Sandbox Cloud

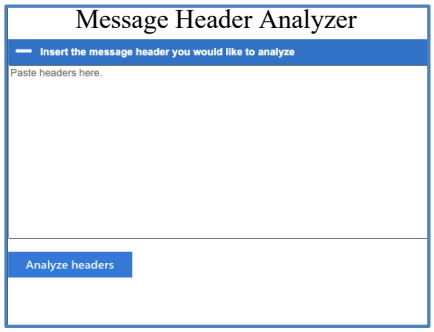


(U) The online malware detection site Joe Sandbox detects and analyzes potential malicious files and URLs on Windows, Android, Mac OS, Linux, and iOS for suspicious activities. It performs deep malware analysis and generates comprehensive and detailed analysis reports. The website gives individuals access to the Community Edition of the Joe Sandbox Cloud. It allows a maximum of 15

analyses/month, 5 analyses/day on Windows, Linux, and Android with limited analysis output. If more analyses are needed, organizations can purchase a Cloud Pro account.

(U) Joe Sandbox Cloud https://www.joesandbox.com/#windows

(U) Microsoft Message Header Analyzer



(U) Microsoft Message Header Analyzer provides analysis of email headers. SMTP message headers contain a wealth of information which allows you to determine the origin of a message and how it made its way through one or more SMTP servers to its destination.

(U) To use Message Analyzer, copy message headers from an email message and paste them in the Message Analyzer tab on the web site.

(U) Microsoft Message Header Analyzer: https://mha.azurewebsites.net/

(U) DuckDuckGo Search Engine

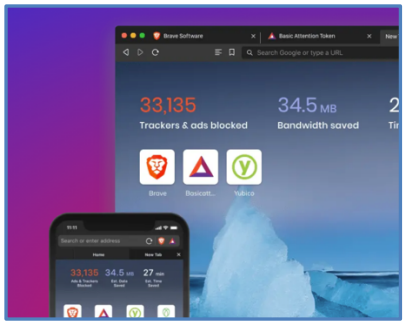
(U) DuckDuckGo is an internet search engine that emphasizes protecting searchers' privacy and avoiding the filter bubble of personalized search results. DuckDuckGo distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term.[7]

(U) DuckDuckGo Privacy Browser is fast and includes features such as tabs and bookmarks. Its enhanced privacy features include:[8]

- Tap Fire Button, Burn Data — clear all tabs and browsing data with one tap.
- Escape Online Tracking — automatically block hidden third-party trackers lurking on websites you visit, which stops the companies behind those trackers from collecting and selling your data.
- Search Privately — a private search engine is built-in so you can search the Internet without being tracked.
- Enforce Encryption — force sites to use an encrypted (HTTPS) connection where available, protecting your data.
- Decode Privacy — each site you visit gets a Privacy Grade (A-F) so you can see how protected you are at a glance, and you can even dig into the details to see who may be trying to track you.
- Limit Access — secure your browser with Touch ID or Face ID.

(U) DuckDuckGo: https://duckduckgo.com/

(U) Brave Privacy Browser



(U) Brave is a free and open-source web browser developed by Brave Software, Inc. and is based on the Chromium web browser, it blocks ads and most website trackers. As of 2019, Brave has been released for Windows, macOS, Linux, Android, and iOS. The current version features five search engines by default, including their business partner DuckDuckGo.[9]

(U) Brave privacy browser:[10]

- Blocks most ads and the trackers that come with them
- Deletes cookies other than the ones from the sites you actually visit
- Makes your browser harder to recognize and follow without cookies
- Upgrades you to secure connections whenever sites support them
- Blocks malicious code and malicious sites — like ones which try to use your computer to mine cryptocurrencies.

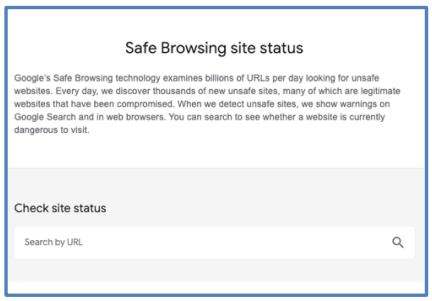
(U) Brave Privacy Browser: https://brave.com/

(U) Feodo Tracker

(U) Feodo Tracker tracks certain malware families that are related or that evolved from Feodo, an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet. Dridex and Emotet (aka Heodo) are still active and are being tracked by Feodo Tracker. The purpose of the project is to identify botnet command & control servers (C&C) associated with a Feodo malware variant and provide a blocklist so that the cyber community can protect themselves from the threat.[11]

(U) Feodotracker: https://feodotracker.abuse.ch/

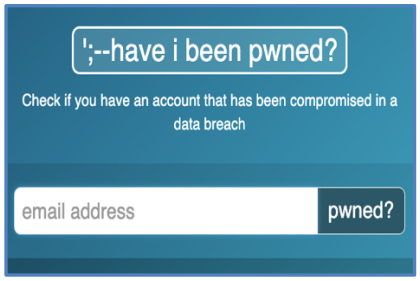
(U) Google Safe Browsing



(U) Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, Google discovers thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When Google detects unsafe sites, they show warnings on Google Search and in web browsers. You can access the Google Safe Browsing site to determine whether a website is dangerous to visit.[12]

(U) Google Safe Browsing: https://transparencyreport.google.com/safe-browsing/search?url=

(U) Have I Been Pwned



(U) Have I Been Pwned, is an online platform that allows Internet users to check whether their personal data has been compromised by data breaches. The service collects and analyzes hundreds of database dumps and pastes containing information about billions of leaked accounts. It allows users to search for their own information by entering their username, or email address.[13]

(U) Users can also sign up to be notified if their email address appears in future dumps. As of June 2019, Have I Been Pwned averages around one hundred and sixty thousand daily visitors, the site has nearly three million active email subscribers and contains records of almost eight billion accounts.[14]

(U) Have I Been Pwned: https://haveibeenpwned.com/

(U) Add to our List

(U) If you are aware of other open source tools that should be included to this list, please send the link and a brief description of the website to the Hawaii State Fusion Center at HSFC@hawaii.gov.

(U) This product supports DHS Standing Information Needs (SINs): HSEC-1, HSEC-1.3, HSEC-1.8 and Hawaii State Fusion Center SIN, HSFC-2. This information was researched by HSFC, Cort M. Chambers, PhD, cort.m.chambers@hawaii.gov.

(U) Report Suspicious Cyber Activity
(U) If you have information concerning this type of cyber activity please report it to the FBI at: (808) 566-4300, and the Hawaii State Fusion Center at: HSFC@hawaii.gov

[1] (U) Wikipedia; *Virus Total*; https://en.wikipedia.org/wiki/VirusTotal; accessed 30 September 2020: online information source
[2] (U) Virus Total; https://www.virustotal.com/gui/; accessed 30 September 2020: online cyber security company
[3] (U) Wikipedia; *Virus Total*; https://en.wikipedia.org/wiki/VirusTotal; accessed 30 September 2020: online information source

[4] (U) Virus Total; https://www.virustotal.com/gui/; accessed 30 September 2020: online cyber security company
[5] (U) Hybrid Analysis; https://www.hybrid-analysis.com/; accessed 30 September 2020: online cyber security company
[6] (U) Hybrid Analysis; https://www.hybrid-analysis.com/; accessed 30 September 2020: online cyber security company
[7] (U) Wikipedia; *DuckDuckGo*; https://en.wikipedia.org/wiki/DuckDuckGo; accessed 30 September 2020: online information source
[8] (U) DuckDuckGo website; https://duckduckgo.com/; accessed 30 September 2020: online search engine
[9] (U) Brave Browser; https://brave.com/; accessed 30 September 2020: Privacy browser
[10] (U) Brave Browser; https://brave.com/; accessed 30 September 2020: Privacy browser
[11] (U) Feodo Tracker; https://feodotracker.abuse.ch/about/; accessed 30 September 2020: Privacy browser
[12] (U) Google Safe Browsing: https://transparencyreport.google.com/safe-browsing/search?url=; Safe browsing website
[13] (U) Wikipedia; https://en.wikipedia.org/wiki/Have_I_Been_Pwned%3F; accessed 30 September 2020; online information source
[14] (U) Wikipedia; https://en.wikipedia.org/wiki/Have_I_Been_Pwned%3F; accessed 30 September 2020; online information source