REDSKY ALLIANCE

01 March 2024

Cyber Security Whitepaper

Cyber Threat Intelligence Data Sets & Services

This whitepaper describes Red Sky Alliance's proprietary Cyber Threat Intelligence services and datasets. The content contained herein is current as of 01 March 2024. Red Sky Alliance's security services, collections and systems are continuously evolving, as we continually improve and enhance of our targeted cyber threat intelligence services for our clients.

Introduction

Red Sky Alliance Corporation is a privately held USA owned cyber threat intelligence firm that delivers proprietary intelligence, analysis and in-depth strategic reporting. Our company will continue to deliver insightful, actionable intelligence in formats best suited to your strategic, operational, and tactical needs.

Founded in 2011 by information security and software professionals, we focus solely on the collection and analysis of indicators of compromised to help our clients better protect their networks. We have ten (9) dataset collections and in most cases can deliver 10+ years of cyber threat history on nearly any domain in the world. We have developed services using our data to easily provide targeted cyber threat notification and analysis services via text, email, portfolios and dashboards.

Cyber Threat Analysis Center-CTAC

https://www.redskyalliance.com/ctac

Our cyber threat intelligence services use a warning problem methodology; an approach used in the defense and intelligence communities to monitor and report on threats from both nation-states and non-state actors. Attacks can range from phishing, denial-of-service, and even cyber-physical destruction essentially anything that you may consider a cyber threat to your enterprise. Red Sky Alliance's analysts incorporate data and factors beyond the technical to include geographic, political, and economic trends and developments. Red Sky Alliance follows this approach because "cyber" is only one aspect of the myriad threats facing your enterprise.

This white paper outlines Red Sky Alliance's approach to cyber security collection and analysis using our suite of products and services.

Information Security

When describing firms in the Information Security market segment, they can be separated into a few categories: Data collection, Data Aggregation, Analysis and Delivery. Red Sky Alliance performs all four of these functions.

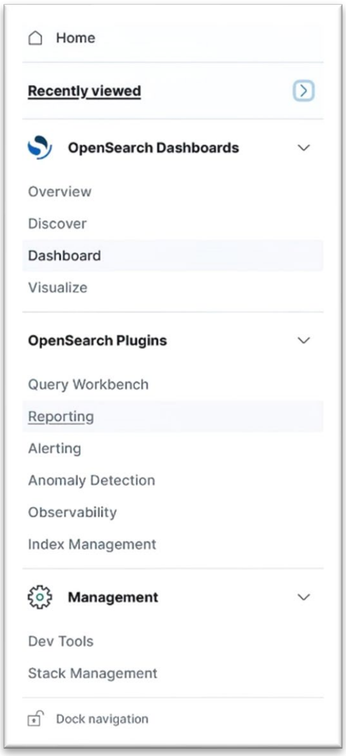


Figure 1- CTAC Dropdown

- **Collection:** Red Sky Alliance has established their own proprietary sources and collections of cyber threat sources. The collections include sources include Red Sky Alliance's dark web search engine REDPANE. Our collected data is archived, so even if the posted data has been removed, it can still be shown in our reporting.
- **Aggregation**: Red Sky Alliance adds Open-Source Intelligence (OSINT), such as Virus Total data to their own collections to take advantage of their historical data. Client data and other data sources can easily be aggregated in the CTAC service
- **Analysis**: This is the CTAC service, consolidating the first three categories in one service. Any client data, such as net flow can be added and analyzed against Red Sky Alliance's cyber threat data. Any metric can be run against the cyber threat reporting, such as share price or manufacturing down time.
- **Delivery**: Users can have their choice of deliver methods: Text, email, dashboards, portfolios and APIs.

Dashboard Access

The CTAC service brings all of these services together in one screen. CTAC is an analytic environment that allows you to consolidate your feeds, create meaningful visualizations, analyze technical intelligence, and access Twelve (12) years of finished intelligence reporting. It is a one-stop shop for cyber defenders and threat intelligence analysts to quickly identify and prioritize problems, drill down into minutia if required, and produce high-level assessments of threats to any organization. CTAC includes Red Sky Alliance's APIs for ease of use. CTAC's all-in-one suite of tools will help you level-up your analytic capabilities faster than other approaches, and for a fraction of the cost of building, staffing, and maintaining your own system.

Software-as-a-Service (SaaS)

CTAC allows organizations to reduce both operating expenses and reduce professional salary expenses, by allowing lower skill level analysts to perform more investigations, faster. CTAC was developed using the Software-as-a-Service (SaaS) model, which allows your team to produce more results, faster. We handle all the maintenance and support of the corresponding capabilities so you can focus on keeping your firm safe. CTAC enables you to automate routine tasks: lookups, source parsing, and correlations; each requiring additional labor in most environments. CTAC is designed for users to add any data source, metric or net flow to be analyzed against its dataset . It requires no additional staffing; acts as a force-multiplier enabling your current staff to do more than they could before. Using the SaaS delivery method, this eliminates the need for additional IT infrastructure and people to manage it. The service helps junior level analysts to perform more tasks in less time and is a learning platform for more advanced tasks. CTAC will allow senior level analysts to focus on complex issues and contextualize raw data. This supports better security decision making and defense planning.

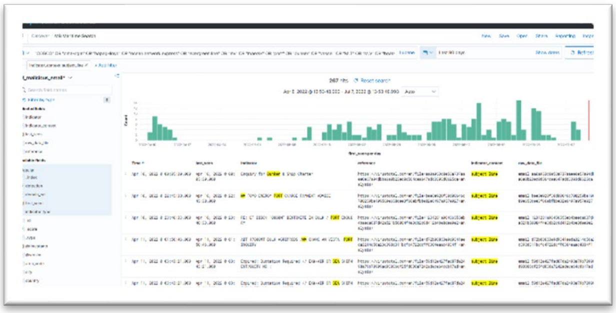


Figure 2 CTAC Maritime Data

Cyber Intelligence

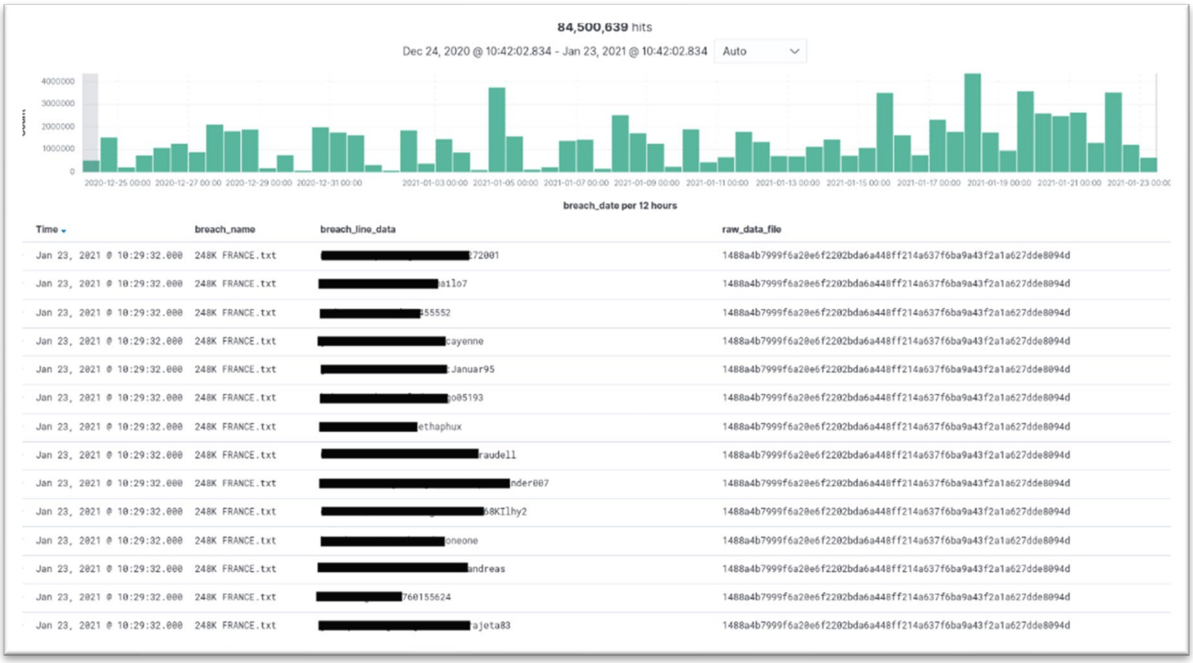
One of the core tenets of Red Sky Alliance and our CTAC initiative is to bring together people, data, and analysis services in a collaborative environment where both senior and junior level analysts can come together as "Force Multipliers" against cyber threat actors and state sponsored cyber terrorists.

The CTAC OpenSearch analyst tools build on 12+ years of Red Sky Alliance Community cyber threat intelligence collection and analyst collaboration. Red Sky Alliance publishes in depth analysis on hundreds of technical, geopolitical, and criminal cyber activities per year. Many of these reports include Yara rules and indicators of compromise (IoC's) derived from these reports.

Refer to CTAC guide for the data dictionary:
https://wapack-labs-llc.gitbook.io/ctac-guide/overview/elastic-stack/data-sets

Tailored Cyber Protection

Red Sky Alliance currently maintains collections that yield thousands of newly compromised global accounts on a daily basis in different industries across the globe. These industries range from shipping/receiving and port operations, to manufacturing, to markets/finance and beyond.

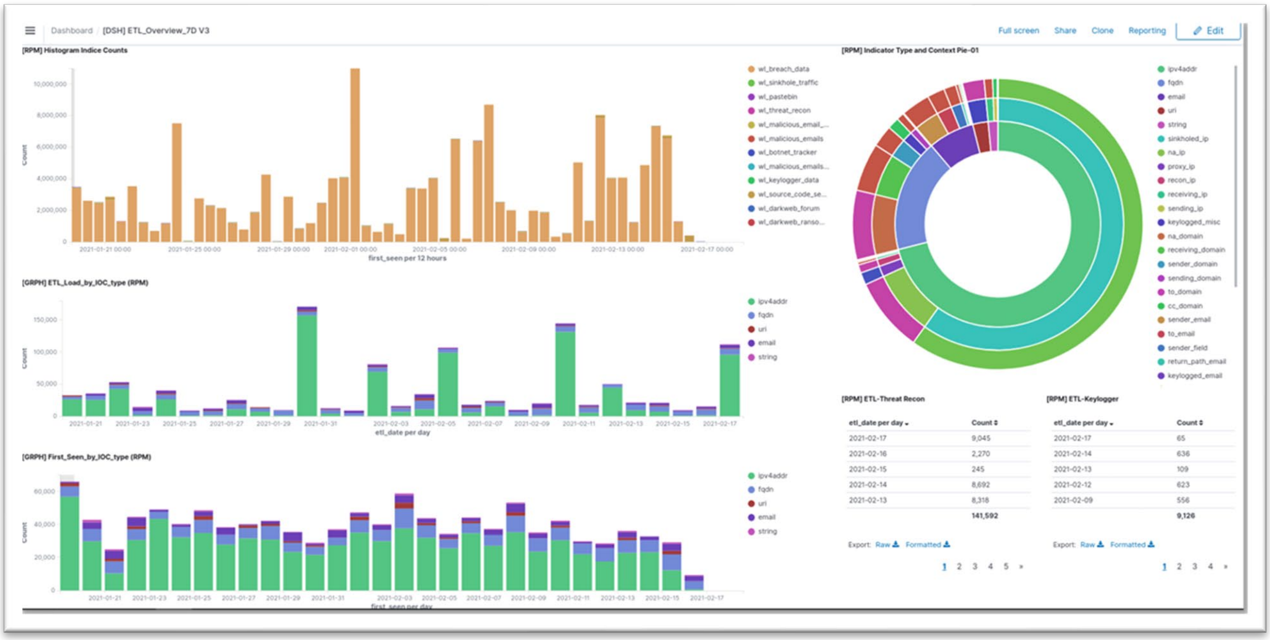


Time	breach_name	breach_line_data	raw_data_file
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]72001	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]a1lo7	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]55552	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]cayenne	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]Januar95	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]o05193	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]ethaphux	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]raudell	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]nder007	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]68KIlhy2	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]oneone	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]andreas	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]760155624	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d
Jan 23, 2021 @ 10:29:32.000	248K FRANCE.txt	[redacted]ajeta83	1488a4b7999f6a20e6f2202bda6a448ff214a637f6ba9a43f2a1a627dde8094d

Figure 3 CTAC Breach data collection

Different pieces of the CTAC platform include:

- OpenSearch
  - Discover
  - Visualize
  - Dashboard
  - Timeline
  - Dev Tools
- OpenSearch REST API
  - OpenSearch DSL (Domain Specific Language)
- AWS Open-distro for OpenSearch Plug-ins
  - Reporting
  - Security
  - Alerting



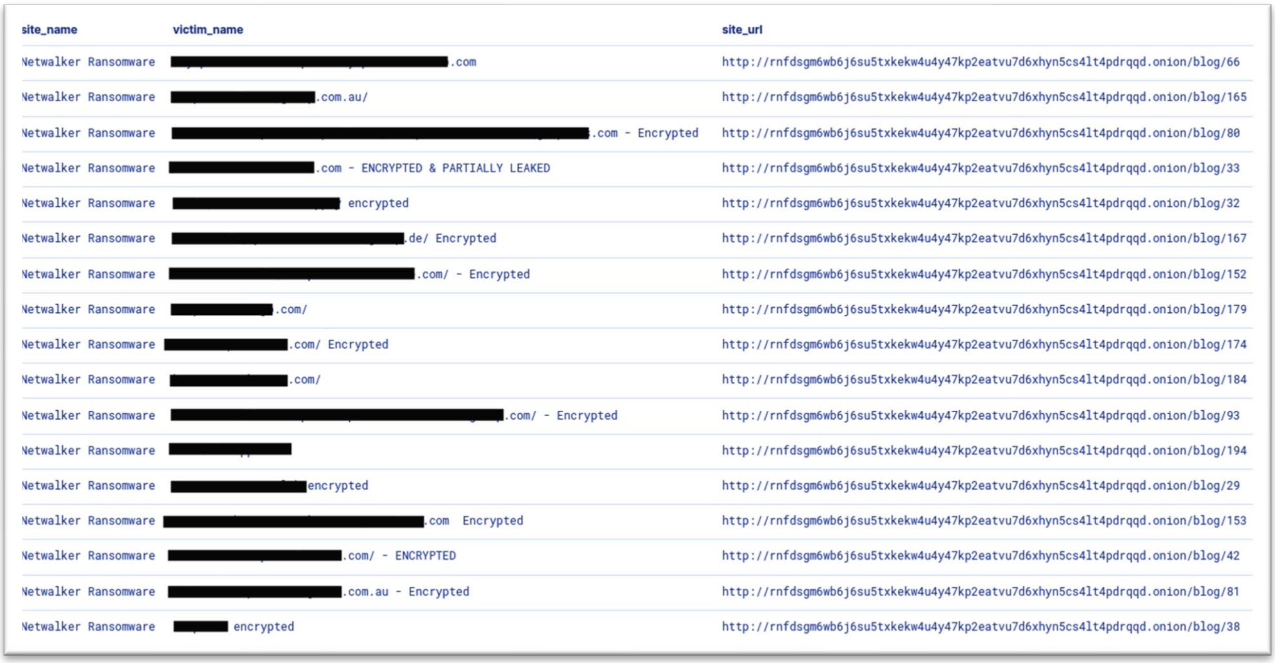
[RPM] ETL-Threat Recon

etl_date per day	Count
2021-02-17	9,045
2021-02-16	2,270
2021-02-15	245
2021-02-14	8,692
2021-02-13	8,318
	141,592

[RPM] ETL-Keylogger

etl_date per day	Count
2021-02-17	65
2021-02-14	636
2021-02-13	109
2021-02-12	623
2021-02-09	556
	9,126

Figure 4 Sample Dashboard Generated in CTAC

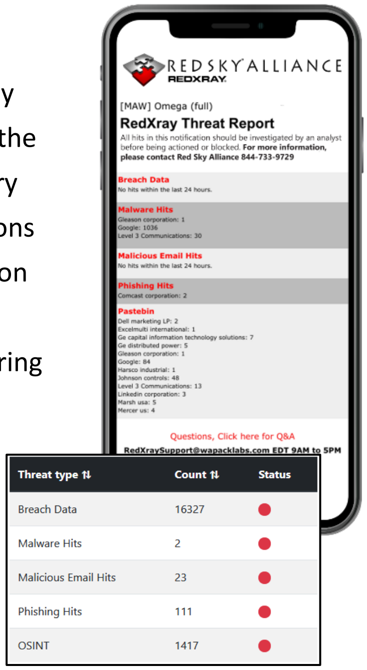


site_name	victim_name	site_url
Netwalker Ransomware	[redacted].com	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/66
Netwalker Ransomware	[redacted].com.au/	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/165
Netwalker Ransomware	[redacted].com - Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/80
Netwalker Ransomware	[redacted].com - ENCRYPTED & PARTIALLY LEAKED	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/33
Netwalker Ransomware	[redacted] encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/32
Netwalker Ransomware	[redacted].de/ Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/167
Netwalker Ransomware	[redacted].com/ - Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/152
Netwalker Ransomware	[redacted].com/	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/179
Netwalker Ransomware	[redacted].com/ Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/174
Netwalker Ransomware	[redacted].com/	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/184
Netwalker Ransomware	[redacted].com/ - Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/93
Netwalker Ransomware	[redacted]	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/194
Netwalker Ransomware	[redacted]encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/29
Netwalker Ransomware	[redacted].com Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/153
Netwalker Ransomware	[redacted].com/ - ENCRYPTED	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/42
Netwalker Ransomware	[redacted].com.au - Encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/81
Netwalker Ransomware	[redacted] encrypted	http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog/38

Figure 5 CTAC Red Pane dark web search engine, ransomware data leaks.

REDXRAY (https://www.redskyalliance.com/redxray)

REDXRAY® is an automatic cyber threat notification service provided by Red Sky Alliance using the same datasets as the CTAC service. One of the features is that portfolios of suppliers, clients, competitors and industry groups can be enrolled and monitored by users. The enroll organizations can be viewed on one dashboard and only updates and new information will trigger an alert. This means that one (1) analyst can follow a large number of organizations daily. The service delivers a daily report covering the following threat types: Botnet Tracker, Breach Data, Keylogger Records, Malicious Emails, OSINT Records, Sinkhole Traffic, Phishing, and more. REDXRAY® is designed for personnel from the C-Suite to cyber analysts. Multiple people can receive the daily alerts, so analysts can share them with clients or senior management as they are issued.



[MAW] Omega (full)

RedXray Threat Report

All hits in this notification should be investigated by an analyst before being actioned or blocked. **For more information, please contact Red Sky Alliance 844-733-9729**

Breach Data
No hits within the last 24 hours.

Malware Hits
Gleason corporation: 1
Google: 1036
Level 3 Communications: 30

Malicious Email Hits
No hits within the last 24 hours.

Phishing Hits
Comcast corporation: 2

Pastebin
Dell marketing LP: 2
Excelmulti international: 1
Ge capital information technology solutions: 7
Ge distributed power: 5
Gleason corporation: 1
Google: 84
Harsco industrial: 1
Johnson controls: 48
Level 3 Communications: 13
Linkedin corporation: 3
Marsh usa: 5
Mercer us: 4

Questions, Click here for Q&A

RedXraySupport@wapacklabs.com EDT 9AM to 5PM

Threat type ⇅	Count ⇅	Status
Breach Data	16327	●
Malware Hits	2	●
Malicious Email Hits	23	●
Phishing Hits	111	●
OSINT	1417	●

Figure 6 Sample daily report from a client using REDXRAY

The report includes counts for each category and is visually attractive as fields with issues are noted with a red light, fields with no issues are represented with a green light. Notifications can be delivered via text, email, dashboard or API. Red Sky Alliance has extensive intelligence/information/documentation behind each threat recorded. Using the time-filter feature companies can view all archived threats over time, or view activity for the past day, week, month, or 90 days. In addition to the alerts, the artifacts and history of each entry is only a click away. Cyber threat daily files can be entered into an organization's SIEM and be blacklisted/blocked against future attacks.

A cyber threat score is presented to the user each time the enrolled entity is monitored. This is a key time saving for analysts who can observe if he targeted domain is receiving more or fewer cyber threats each day or review period.

Specific use REDXRAY services are available for Supply Chain, cyber insurance and vCISO support services and can be found at https://www.redskyalliance.com . Groups of organizations can be followed using REDXRAY portfolio and notifications for only entities experiencing new data, threats or changes can be delivered to consultants and/or senior management daily.

Datasets are available for subscription purchase & delivered by API Integration partners can purchase datasets to enhance the scope and context of their current product services. These datasets have been named REDCURRENT API https://www.redskyalliance.com/redcurrent .

Indicator Types

These are considered the highest confidence indicators and are used to derive new information. Approximately 20% are APT, 60% are criminals, and the remainder, misc. All indicators are directly observed. Most are attributed to specific groups or activities.

Refer to CTAC guide for the data dictionary:
https://wapack-labs-llc.gitbook.io/ctac-guide/overview/elastic-stack/data-sets

1.) Monitor Botnets

Botnets are often used to steal data, commit distributed denial of service (DDoS) attacks, send malicious emails, or simply as a proxy for malicious internet traffic. If your IP address found in the botnet tracker, it means that it was seen in communication with a malicious endpoint. This does not automatically indicate a malware infection as there are a number of reasons why two IP addresses might communicate, but typically indicates

suspicious/malicious activity. Additionally, publicly accessible web proxies (designated as a proxy_ip in our collection) are often used by attackers to anonymously probe a target network prior to an attack, or perform credential stuffing attacks.

Botnet Tacker can be used for any/all industry segment investigations including critical infrastructure, Defense Industrial Base Sector and all commercial segments.

Data can be sourced by:

botnet data:
- historical data (2018-Jan 2020):
  - Victim IP
    - city
    - country
    - region
    - postal code
    - Geo coordinates
  - Malware attribution
  - C2 IP or domain
- recent data (Jan. 2020-now):
  - arbitrary CIDR block

Botnet Use Cases

1.) Identify IPs that are communicating with botnets

2.) Identify IPs that are hosting open web proxies

3.) Add suspicious IPs to your network defense block lists to reduce the risk of credential stuffing attacks and network probes

2.) Data Breach Research

Breach data hits are from public database leaks. Depending on the nature of the leaked database, exposed information may vary from just email addresses to username and password combinations and other personally identifiable information. Data set contains the raw breach data so you can easily see what type of data has been exposed. If the breach data contains passwords, then Red Sky Alliance recommends enforcing a password reset and investigating whether there has been unauthorized access to that account. Some companies believe that the disclosure of "old" or historical passwords is low risk. This is false however, as many attackers use old passwords to brute force/predict current passwords. Old passwords can also be used in fraud/phishing attacks as a way to build trust. Breach data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

Data can be sourced by:

breach data:

Account username
domain, if included in the account username

Breach Use Cases

1.) Search for leaked account credentials for your organization.

2.) Identify partners that have leaked account credentials.

3.) Penetration testing.

3.) Compromised Keyloggers

A keylogger hit means your domain or IP address appeared in a keylogger output file. This could mean one of the following things: 1) Keylogger malware is running on your network. 2) A username and password belonging to an employee was captured by a keylogger. 3) An email address was observed in clipboard data on an infected computer. For example, a user infected with keylogger malware, cut &amp; paste an email address belonging to your organization. The raw source data can be investigated to determine the best course of action. Keylogger can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

Red Sky Alliance currently monitors hundreds of keylogger and other malicious command and control servers providing unique insight to different threat actors. Our intelligence includes millions of credentials leaked across the web along with files leaked by threat actors including sensitive information stolen from victims.

Data can be sourced by:

keylogger data:

- victim source ip
  - city
  - country
  - region
  - postal code
  - geo coordinates
  - whois data
- account username
- URL of service for keylogged credentials
- keylogger malware

Breach Use Cases

1.) Identify credentials that have been exposed via a keylogger infection

2.) Identify computers that have been infected with a keylogger

4.) Malicious Emails Attachments

If your domain or IP address shows up in this collection, it means it was observed in the header of an email that has been identified as malicious (1 or more AV detection). The raw email should be inspected to see whether it was sent to or from your organization or if it was spoofed using your organization's data. It should be noted that some AV vendors classify emails as malicious when they are actually benign. All malicious email hits only indicate targeting but can sometimes indicate a malware infection. Malicious Email data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

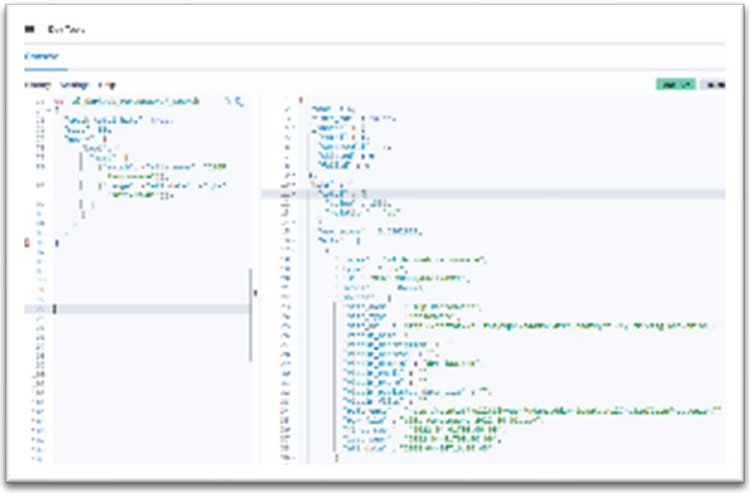


Figure 7 Drill down into data

Data can be sourced by:

Malicious email data:

email subject line
sender field (full name + email address)
sender email address
sender domain
city
country
region
postal code
geo coordinates
sending domain
city
country
region
postal code
geo coordinates
cc domain (derived from carbon copied email addresses)
city
country
region
postal code
geo coordinates

- return path email address
- sending IP
  - city
  - country
  - region
  - postal code
  - geo coordinates
- recipient email address
- receiving domain
  - city
  - country
  - region
  - postal code
  - geo coordinates
- receiving ip
  - city
  - country
  - region
  - postal code
  - geo coordinates
- to domain
  - city
  - country
  - region
  - postal code
  - geo coordinates

Malicious Emails Use Cases

1.) Identify organizations that are being targeted for malware delivered via an infected email attachment. 2. Identify organizations that are being impersonated via the Sender field or in an email subject line to lure potential victims to open malware infected email attachments.

2.) Identify and block connections from IPs that are used to originate malware infected email.

3.) Educate users on observed email subject lines that are being used to deliver emails with malware infected attachments.

4.) Perform trending analysis of malware infected emails.

5.) Add email addresses that are sending out malware infected emails to your network defense block lists.

5.) Proprietary Sinkhole Collection

This data set provides Sinkhole indicators. Sinkholing is a technique for manipulating data flow in a network, redirecting traffic from its intended destination to the server of your choosing. It can be used maliciously to steer legitimate traffic away from its intended recipient. Security professionals more commonly use sinkholing as a tool to research and react to attacks. A sinkhole "hit" (indicator) means an IP was observed in weblogs from our proprietary sinkhole server. Similar to our botnet tracker data, Sinkhole indicators shows that communication to a malicious domain was observed. The nature of that communication needs to be examined from our raw sinkhole record. If the sinkhole indicator is a result of a malware infection, then the information should be referred to incident responders.

Sinkhole data can be used for any/all industry segment and government investigations including critical infrastructure, all commercial segments and sixteen (16) Critical Infrastructure/Key Resource (CI/KR), to include any country's Defense Industrial Base Sector and all cleared commercial segments.

Data can be sourced by:

sinkhole data:

- source IP (IP connecting to our sinkhole; indicator field)
  - asn
  - whois data
  - city
  - country
  - region
  - postal code
  - geo coordinates
  - malware attribution

Sinkhole Data Use Cases

1.) Identify IP addresses that are attempting to communicate with domains that are known to have been associated with malware command and control infrastructure.

2.) Add suspicious IPs to your network defense block lists.

3.) Perform trending analysis of malware activity.

6.) Identifying Phishing Emails

The Identified Phishing Domain data set contains intelligence regarding phishing activity associated with a company. This service includes primary, open-source indicators from dozens of sources. Each indicator from this collection should be individually analyzed as each source has a different context. Phishing attacks account for more than 80% of reported security incidents. Reputational damage aside, $17,700 is lost every minute due to a phishing attack.

This data can be used for any/all government or cleared industry segment assessment or investigation including all sector critical infrastructure, Defense Industrial Base Sector and all commercial segments.

Data can be sourced by:

phishing data:

- suspicious or malicious IP addresses:
  - city
  - country
  - region
  - postal code
  - geo coordinates

Phishing Data Use Cases

1.) Add malicious phishing IP and domains to your organization's firewall, web proxy, IDS, or IPS block list.

7.) Source Code Secrets

The data product at hand is a compilation of exposed sensitive secrets retrieved from popular source code hubs like GitHub, Gitlab, and Bitbucket. The dataset captures authentication keys, usernames, passwords, API keys, and other secure credentials unintentionally revealed due to improperly configured open-source repositories. Geopolitically, this information is invaluable, as it provides insights into potential vulnerabilities that, if exploited, can jeopardize the security apparatus of nations.

The negligent exposure of such sensitive information suggests potential oversights in the development and security practices of government contractors and companies. Such breaches can open avenues for cyber espionage, interference in electoral processes, manipulation of infrastructure, and the theft of national secrets. From a socio-political perspective, it highlights the need for stringent cyber hygiene practices to protect the integrity of digital systems and databases. In essence, this data product is paramount for understanding national vulnerabilities in the cyber domain.

Data can be sourced by:

Source code secret data:

repository site: github.com, gitlab.com, bitbucket.org
repository account name
repository name

Source Code Use Cases

1.) Discover if an organization has sensitive information posted in publicly readable source code repositories.

2.) Search for sensitive information that can be used by attackers to breach networks, embed malicious code into software repositories, or cause software outages.

8.) Dark Web

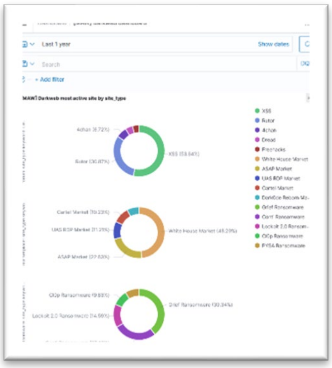


Figure 8 Graphical Filters

This data set actively monitors dozens of underground and dark websites where criminal activity takes place and is discussed. This data includes information gathered from Tor .onion sites and a few select surface web cybercrime sites. Using dark web data, analysts can learn about what subject threat actors are talking about, and where the discussion is taking place. Threat actors often advertise access to victim networks or leak sensitive information stolen during attacks. The data contain indicators from dark web forums, marketplaces, and ransomware leak sites. Threat actors often discuss or brag about their attacks. They also share tactics, techniques, and procedures. Analysts can search through dark web forums to see what threat actors are saying about them, their company, or their industry. Attackers are not just stealing data, they are selling it. Some are even selling the access they obtained illegally on purchase websites. Companies can monitor what threat actors are selling and monitor for attackers claiming to have access to, or stolen data from, their company. Ransomware actors have evolved from simply holding a network hostage. Ransomware groups are now working together to earn higher profits. Dark web ransomware data allows analysts to see who has been breached, who is selling access to which networks, and which data ransomware groups are publishing simply as punishment for non-payment. Companies can also monitor when their supply chain is compromised which may lead to future cyberattacks. Dark Web data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

Data can be sourced by:

dark web forum
- tor site name
- post author
- free text search of post content

dark web ransomware
- ransomware site name
- victim domain
- victim name
- free text search of post content

- dark web marketplace
  - marketplace name
  - item vendor name
  - item category
  - free text search of item description

Dark Web Use Cases

1. Discover if particular organizations have been subjected to or targeted for a ransomware attack.
2. Search for your data or other organizations' data is for sale on the dark web. What type of data and at what price?
3. Search for access to your organization or any other organization to see if access is for sale.
4. Track vendor activity across multiple dark marketplaces.
5. Discover user credentials leaked In the Indicator Types section, these are considered the highest confidence indicators and are used to derive new information. Approximately 20% are APT, 60% are criminals, and the remainder, misc.
6. All indicators are directly observed. Most are attributed to specific groups or activities. All are rated our highest confidence rating - 90%.

9.) Paste Storage Sites (OSINT)

This includes various sources such as paste websites, forums, and other sites where malicious activity may take place. Is one of your employee email addresses listed in an Anonymous targeting operation? Is someone running vulnerability scans against your networks and posting the results publicly? Find out by searching through the REDXRAY OSINT collection.

Data can be sourced by:

Pastebin Source by:

Indicator
Indicator Type
City, Country
Postal Code
Region
Geo Coordinates

Paste Storage Sites Use Cases

1. Discover if an organization has sensitive information posted in publicly on temporary online locations.
2. Search for sensitive information that can be used by attackers to breach networks or cause software outages.
3. Has the privacy of your stored code been changed so it is open to all users?
4. Locate and remove old code that has been forgotten and still available or dangerous if used by cyber threat actors.

Collaboration with the Security Research Community

Red Sky Alliance has long enjoyed a close relationship with the security research community. Our long term relationships with corporate and government agencies has helped Red Sky Alliance to continue to provide quality and innovative solutions. Red Sky Alliance hosts a “no charge” cyber threat intelligence reporting community at https://redskyalliance.org. Cyber threat indicators and industry segment articles are posted to help information security professionals of all skill levels. In addition, Red Sky Alliance hosts weekly cyber threat briefings on current cyber issues. These 10 minute presentations are named REDSHORTS. Previous presentations are available for viewing on this same portal.

Conclusion

Our cyber threat intelligence services and data are behind many years of Collection/Analysis, Scientific Development and GEO-Political input. Red Sky Alliance services are needed to quicken the pace of your internal protections or can be used by your MSSP to better protect your valuable company data. The convenience of our datasets and services is that you do NOT need a downloaded application, purchase hardware or add any new connection(s) to your network(s). Set-up is extremely easy with a high degree of built-in security. Our team has worked years to make our processes easier and quicker all for your benefit.

Company

Red Sky Alliance is a Cyber Threat Analysis and Intelligence Service organization. For questions, comments or assistance, please contact the office directly at 1-844-492-7225, or feedback@redskyalliance.com

Reporting: https://www. redskyalliance. org/
Website: https://www. redskyalliance. com/
LinkedIn: https://www. linkedin. com/company/64265941

Weekly Cyber Intelligence Briefings:

REDSHORTS - Weekly Cyber Intelligence Briefings

https://attendee.gotowebinar.com/register/5993554863383553632

For More Information Contact Us:
844-492-7225
jmckee@redskyalliance.com

www.redskyalliance.com Corporate website
www.redskyalliance.org INFOSEC website

REDSKY ALLIANCE