

# REDXRAY<sup>®</sup> Supply Chain Maritime Support Program

<b>INTRODUCTION</b>	<b>2</b>
<b>REDXRAY</b>	<b>3</b>
<b>REDXRAY SERVICE</b>	<b>4</b>
<b>TARGET MARKETS</b>	<b>5</b>
<b>SHIPPER OPPORTUNITIES</b>	<b>6</b>
<b>DATA SETS</b>	<b>7</b>



## COMPANY

# Introduction

## How Secure Is Your Shipping Supply Chain?

REDXRAY® can identify threats against your ships, ports, networks, supply chain, customers or target companies/agencies daily.

Please consider taking advantage of Red Sky Alliance services that include checking our backend databases for emails subject lines that spoof data points all along the transportation supply chain; our research specifically identifying vessel names. Key words in these collection searches scan subject lines with identifying wording of containing Motor Vessel (MV) and Motor Tanker (MT) and numerous other vessel designations in the subject line or any transportation supply chain entity.

We can offer maritime supply organizations

- Daily cyber threat notifications for all enrolled entities (portfolio) on one dashboard.
- Notifications on only breach activity daily, so users do not have to look for changes or new breach activity on entire portfolio.
- Avoid cyber breaches from supply chain members and help protect members at the same time.
- The competitive advantage of offering a unique service
- Third party notification support helps with ongoing CMMC compliance.

- Red Sky Alliance also has the capabilities to provide services to collect spoofed emails in our data sets for any identified point along the entire transportation supply chain. Or provide a direct API of raw data to strengthen a company's analytical tools.

- Sample report can be found at:

<https://redskyalliance.org/transportation/vessel-impersonation-and-supply-chain-report-february-2024>

Backed by over 8.9 billion high-quality, high confidence indicators of compromise, the service delivers a daily report covering the following threat types: Botnet Tracker, Breach Data, Keylogger Records, Malicious Emails, OSINT Records, Sinkhole Traffic, Phishing, Dark Web, and more. REDXRAY is designed for personnel from the C-Suite to the Level 1 cyber analyst.



PRODUCT

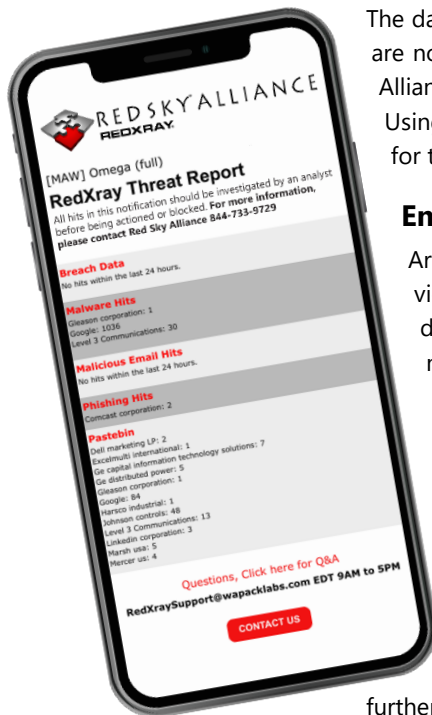
# REDXRAY®

**REDXRAY® Is  
An Automatic  
Cyber Threat  
Notification  
Service Provided  
By Red Sky®  
Alliance**

Our easy-to-understand and explain REDXRAY® allows you to better protect your fleet and associated companies from targeted cyber threats. Your team can decide what will be best for both parties:

- **Shippers** can view their entire fleet portfolio on one dashboard.
- **Users** can view only notified changes instead of having to pour over all content for every enrolled client. Saves time and resources every day.
- **Managers** can receive notifications and advise a supply chain member of needed actions; member can receive them if desired.
- **RedXray** can help with on-going compliance for CMMC and NIST-800-171.
- **Team members** can manage the entire service and let supply chain members know that the best cyber threat service protects them.

The daily 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. 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.



## Email Notifications

Are your SOC analysts overwhelmed by another "pane of glass" to log in to every day and view? To help prevent some of the "noise" that analysts have to deal with, REDXRAY provides daily notification emails. If REDXRAY does not have any hits, the security team does not need to spend time logging in and sifting through yesterday's data. This extra time can be spent bolstering your security posture or focusing on other threats. A cyber analyst should investigate all hits when using REDXRAY.

## Indicator Packages

You have used REDXRAY to notify your team of a threat. They have logged in and viewed the threat details. Now what? Using the Indicator Package feature, REDXRAY-Plus users can export indicators in an organized CSV format for further use. Wouldn't it be nice to be able to efficiently blacklist a known group of keylogger attacker servers to prevent keylogger activity on your network? Want to create custom blacklists or export data for further analysis? REDXRAY-Plus customers have the ability to do all of this quickly and effectively, saving crucial time for cyber analysts and security personnel.

## Cyber Threat Index

A cyber threat index score allows companies to assign a rating level (score) to the threats facing their companies. A high score indicates a high level of malicious activity, whereas a low score indicates less malicious activity. This score is adjusted with the time filter, which allows for additional trend analysis, and recent threat tracking.

## PRODUCT

# REDXRAY® Service

**REDXRAY®** is a daily cyber threat notification service that requires no hardware or software installation (MFA authenticator app required for login). Once a supply chain member is on board, they can begin viewing the threats facing their company within minutes. Although many “competitors” have large quantities of threat data, REDXRAY focuses on providing high-quality targeted cyber threat intelligence specific to our clients. These are not generic threats that “may or may not” cause issues or common threats seen in a particular industry. REDXRAY identifies problems that need to be addressed immediately.

## Cyber Detector

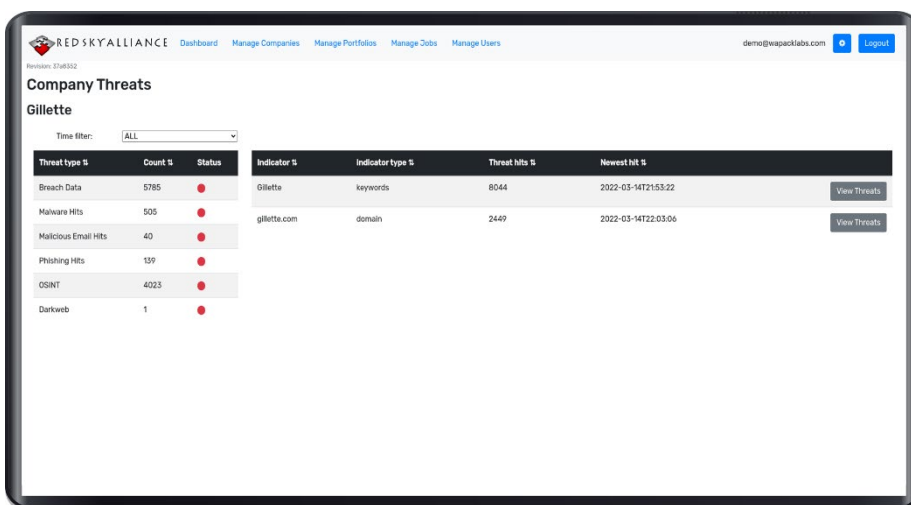
Think of it as a smoke alarm/CO detector in your house. Without it, you would not be aware of smoke, CO, or other dangers. REDXRAY email notifications contain information that you need to know and require action. We have used the simple “Green is good” “Red needs attention” format, so members of senior management can quickly see if anything needs attention (today). Cyber threat analysts can view detailed threat indicators and use the provided intelligence for investigation and mitigation.

## No Hardware or software is Required

REDXRAY detects cyber threats from outside the company’s network and does not require a network connection to the entity or require the installation of any hardware or software. REDXRAY should not be confused with services that protect or notify of threats already inside an entity’s network, such as SIEMs, Firewalls, ASAs, etc. The service can be used to collect cyber threat reporting without the target organization knowing about it. This is an essential feature for protecting supply chains’ key business partners. REDXRAY can report on any entity’s domain anywhere in the world. Red Sky® Alliance collects all of the cyber threat details for additional investigation by cyber threat professionals and has archived intelligence from sources that are no longer online. There are multiple service/support levels, dashboards, distributor opportunities, and price points for REDXRAY, beginning at just \$500.00 per month for daily email notifications.

## Protection

What we are offering is another layer of protection for business owners. Antivirus and firewall software solutions claim to block all threats, but this is hardly the case. Using the data from REDXRAY, companies can prevent further intrusion or other cyberattacks such as account takeover. This is the value of REDXRAY notifications. The enrolled entities receive a daily email identifying cyber threats to their businesses. Are you compliant if your breach data is showing up routinely in the collections?



RED SKY ALLIANCE Dashboard Manage Companies Manage Portfolios Manage Jobs Manage Users demo@wapecklabs.com Logout

Company Threats

Gillette

Time filter: ALL

Threat type #	Count #	Status	Indicator #	Indicator type #	Threat hits #	Newest hit #
Breach Data	5785	●	Gillette	keywords	8044	2022-03-14T21:53:22
Malware Hits	505	●	gillette.com	domain	2449	2022-03-14T22:03:06
Malicious Email Hits	40	●				
Phishing Hits	139	●				
OSINT	4023	●				
Darkweb	1	●				

PROGRAM

# Target Markets

**Defense Contractors**

**Suppliers**

**Sub-contractors**

**Commercial**

**High Technology**

**Transportation**

**Government  
Agencies & Dept**

**Communications**

**X-industry**

**REDXRAY<sup>®</sup>** sales can be targeted at any supply chain, as all businesses are under constant cyber-attacks. Red Sky<sup>®</sup> Alliance follows and writes articles that are industry segment specific. Market segments include:

See a sample report here:

<https://redskyalliance.org/xindustry/debriefing-russia-s-cyber-attacks-against-ukraine>

The reporting and articles can be found at <https://redskyalliance.org>. Portal access and use of the content are provided at no charge to all visitors. Access and weekly cyber threat presentations are no charge. Please invite your cyber teams to join and use the content.



## PROGRAM

# Opportunities For Shippers

**Effortless Accessibility**

An enrolling entity, such as a shipping company, broker, or insurance carrier, could offer to their client base the daily reporting service of REDXRAY® for a monthly fee. Online enrollment and credit payment services are available. Depending on the sales distribution method, a dashboard will be made available for the distributor to add/remove new entities from the REDXRAY service.

The wholesale price of an enrolled entity's daily notification is US\$ 300.00. Brokers and shippers can mark up the price for their commission. The suggested retail price for the REDXRAY service plus commission is US\$ 500.00. This is a recurring monthly revenue (RMR) program, so the monthly commissions can increase as more entities (companies and URLs) are added.

For special cases/industries/opportunities, Red Sky Alliance will consider a less than US\$ 300.00 wholesale price, but this will be by exception only based on total volume.

**Training**

Training for distributors, salespersons, and customers is available at no charge to the distributor. Training can be delivered via webinars and live training sessions using scheduled GoToMeeting sessions.

**Support**

First-level technical support via email and telephone 888-RED-XRAY for brief customer questions (10 minutes). Hours are 9:00 A.M. to 5:00 P.M. Eastern Time. Additional support is billed by the hour. Extreme instances that require Incident Response are billed to the customer at \$300 an hour. Email support is available at REDXRAYsupport@wapacklabs.com.

## Additional Offers For Distributors (Enrolling Partners):

**Two (2) weeks free trials are available but require full enrollment and credit card payment**

**Tutorial on How to write a cyber threat assessment available at no charge. Text and video formats**

**World-class enterprise software services backed by AWS and other software industry leaders.**

**Red Sky® Alliance is a highly respected Information Security/Cyber Threat Intelligence Corp. Founded August 26, 2011, in St. Louis, MO.**

**Website collateral, HTML pages, white paper and online enrollment portal(s) are available.**

**Billing/invoice options: Red Sky Alliance or distributors can collect monthly fees and pay another party by the 5th of the next month.**

**Distributors/ Agents have no restrictions on industry segments or geographic territory limitations to offer REDXRAY services.**

**Clients include: AT&T, Motorola, Citi, Bloomberg, Travelers Insurance, DTCC, The OCC, and Corning**

SOURCES

# Data Sets

DATA SET

## Monitor Botnets

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

### Monitor Botnets Action Items

**1**

Use network diagnostic tools to validate the finding. Identify any internal systems communicating with the botnet or proxy server IP address identified in the result. Tools will help you determine how widespread a potential malware infection may be.

**2**

If there is no use case for your organization to be communicating with the identified malicious IP address, add it to your firewall, IDS, or IPS block list.

**3**

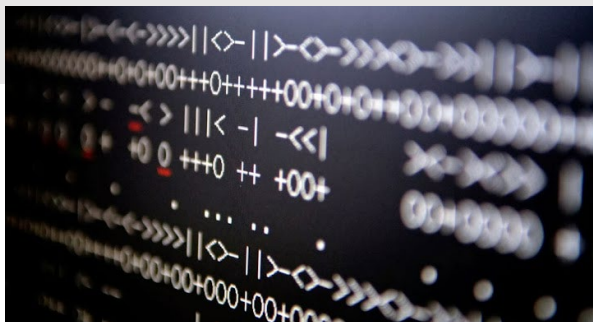
If there is no use case for your organization to be communicating with the identified malicious IP address, add it to your firewall, IDS, or IPS block list.

**4**

Determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

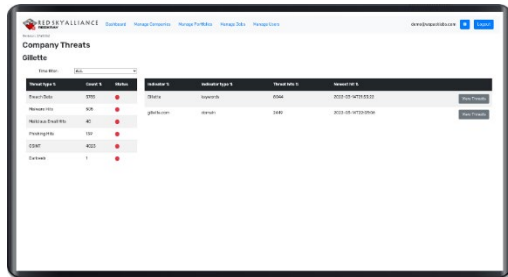
**5**

Ensure all antivirus and OS updates have been applied to the affected systems



## DATA SET

# Data Breach Research



Company Name	Breach Date	Breach Type	Breach Size	Breach Severity	Breach Status
Company A	2023-01-15	Database	10GB	High	Resolved
Company B	2023-02-20	Web App	500MB	Medium	Open
Company C	2023-03-10	API	2GB	High	Resolved
Company D	2023-04-05	Cloud Storage	1TB	Critical	Open
Company E	2023-05-01	Internal Network	100GB	Medium	Resolved

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. REDXRAY contains the raw breach data so you can easily see what type of data has been exposed. If the breach data includes passwords, then Red Sky<sup>®</sup> 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..

## Data Breach Action Items

### 1

Activate multi-factor authentication for affected user accounts to reduce the efficacy of leaked account credentials.

### 2

For recently dated breach data, force password resets for affected user accounts.

### 3

Audit the raw breached password to determine if password policies enforce adequate length and complexity requirements.

### 4

Audit for password re-use of leaked account credentials.

### 5

For older breach data, check the date of the last password change for the affected user accounts to determine the probability that the password may still be in use. Force a password change if in doubt.





DATA SET

## Compromised Keylogger

**A Keylogger Hit Means Your Domain Or IP Address Appeared In A Keylogger Output File.**

**This could mean one of the following things:**

- An email address was observed in clipboard data on an infected computer. For example, a user infected with keylogger malware cut & pasted an email address belonging to your organization. The raw source data can be investigated to determine the best course of action. 1) Keylogger malware runs on your network.
- A username and password belonging to an employee were captured by a keylogger.
- An email address was observed in clipboard data on an infected computer. For example, a user infected with keylogger malware cut & pasted an email address belonging to your organization. The raw source data can be investigated to determine the best course of action.

## Compromised Keylogger Action Items

**1**

Determine if the organization's chosen antivirus solution is effective against the associated malware.

**2**

Conduct a network hunt for indicators of compromise associated with the identified keylogger and remove them if found.

**3**

Use the finding to identify the host system and user account infected with the keylogger.

**4**

Force password changes for all accounts for users who use a system infected with a keylogger.

**5**

Disable any user accounts identified in the finding as infected with a keylogger.

**6**

All account credentials used by all users on this system to log in to other systems have a high probability of being captured and exfiltrated.

**7**

Disable any user accounts used to log in to the host system identified in the finding as infected with a keylogger.

**8**

Force password changes for any user accounts used on the host system identified in the finding as infected with a keylogger.

**9**

Reenable user accounts after password changes have been completed or create new accounts for the affected users..

**10**

Ensure all antivirus and OS updates have been applied to the affected systems.

## DATA SET

## Malicious Email 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 Action Items

**1**

Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.

**3**

If the email was sent FROM your organization, analyze the email header data to determine if the information was spoofed or if the email legitimately originated from your organization. If it legitimately originated from your organization, audit your email.



DATA SET

## Proprietary Sinkhole Collection

A sinkhole hit means your IP was observed in weblogs from our sinkhole server. Similar to the botnet tracker hits, it means that communication to a malicious domain was observed. The nature of that communication needs to be determined from the raw sinkhole record. If the sinkhole is a result of a malware infection, then the information should be referred to incident responders

### Proprietary Sinkhole Action Items

**1**

Use network diagnostic tools to validate and identify any internal systems communicating with the malicious domain identified in the result. This will help you determine how widespread malware infection may be.

**2**

Add the malicious domain to your firewall, web proxy, IDS, or IPS block list.

**3**

Assess systems associated with the IP address identified in the finding and remove any malware or unauthorized proxy software.

**4**

Conduct a network hunt for indicators of compromise associated with the identified malware on your organization's IT assets and remove them if found.

**5**

Ensure all antivirus and OS updates have been applied to the affected systems.

DATA SET

## Identifying Phishing Emails

When you want to know if someone was using your company's domain to commit phishing attacks against customers or even employees? CTAC is a service developed and owned by Red Sky® Alliance, of both primary sourced indicators and open-source indicators from dozens of sources. Each hit from this collection should be individually analyzed as each source has a different context. According to CSO Online, 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

### Identifying Phishing Emails Action Items

**1**

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

**2**

Consider notifying supply chain partners and customers about phishing domains and links that appear to be impersonating your organization.

## DATA SET

## Source Code Secrets

Disclosure of sensitive information can be found with Source Code Secrets. The Source Code Secrets dataset is available to users who want to monitor Github, GitLab, and Bitbucket for accidental disclosure of sensitive information. Sometimes, programmers will purposely or accidentally add credentials such as API keys, cryptography keys, or usernames & passwords for third party services to their publicly visible software repository without thinking about the security implications.

Source Code Secrets data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments

### Source Code Action Items

**1**

Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.

**3**

If the email was sent FROM your organization, analyze the email header data to determine if the information was spoofed or if the email legitimately originated from your organization. If it legitimately originated from your organization, audit your email.



## DATA SET

## Dark Web (REDPANE)

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 sites and a few select surface web cybercrime sites. Using dark web data, analysts can learn about what 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 contains 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 cyber-attacks.

Dark Web data can be used for any/all industry segment investigation including critical infrastructure Defense Industrial Base Sector and all commercial segments.

### Dark Web Action Items

**1**

Investigate to see if your company's data or network access is for sale on the dark web.

**2**

Are there threats against your company officers or locations posted?

**3**

Are there ransomware threats or ransomware payments posted?

**4**

Track hacker network penetration methods or malware that is for sale.

DATA SET

## 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.

### OSINT Action Items

**1**

Using a sample of any malicious attachments identified in the finding, determine if the organization's chosen antivirus solution is effective against the associated malware. If not, conduct a network hunt for indicators of compromise associated with the identified malware.

**2**

If the email was sent to your organization: audit the targeted user's email account and client computer to determine if the malicious email was read and if any malicious attachments were downloaded.



## Red Sky® Alliance

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

**Founded in 2011** by the developer of the world's first enterprise payment server that allowed for credit card transactions on the Internet in 1996. Red Sky focuses on identifying cyber threat actors, incidents, and trends; documenting tactics, techniques, and procedures; and putting that information into the proper context for both executive decision-makers and front-line defenders.

**Red Sky is a cyber threat intelligence firm.** The analysts on our cyber threat team are investigating emerging threats and delivering them to clients in the format that they request: text, email, dashboard and API. The technical intelligence team mines Red Sky's proprietary collections, underground forums, and the dark web. The findings are then divided into nine (9) data sets that are constantly updated. New sources are continually being researched and added to our collections. Our approach allows clients to choose between both raw and finished targeted intelligence reporting. The final product can be in form of reports, feeds delivered via API and services such as REDXRAY'S family of services and the Cyber Threat Analysis Center (CTAC), both of which were developed and owned by Red Sky.

**Jim McKee, Founder & CEO, 01 March 2024**

**For More Information Contact Us:**

**844-492-7225**

[jmckee@wpacklabs.com](mailto:jmckee@wpacklabs.com)

**Red Sky Alliance Corporation**

1815 Central Park Drive, Suite 337 Steamboat Springs, CO 80487 USA  
www.redskyalliance.com 603-606-1246

Red Sky® Alliance and REDXRAY® are Registered Trademarks of  
Red Sky Alliance Corporation

4/23/2024

© 2024 Red Sky Alliance Corporation. All rights reserved.

