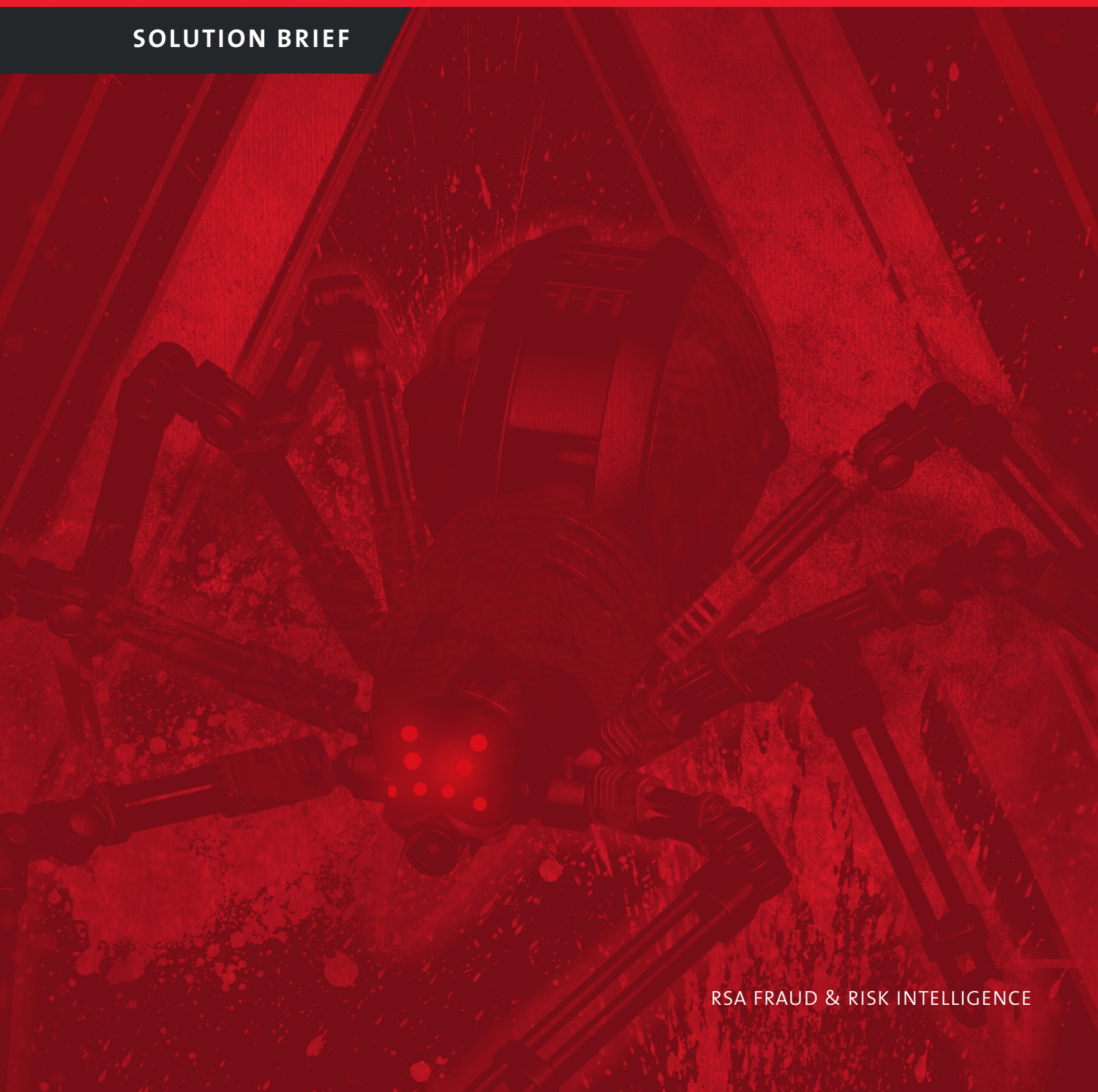
RSA

FraudAction Cyber Intelligence

SOLUTION BRIEF



RSA FRAUD & RISK INTELLIGENCE

RSA

TABLE OF CONTENTS

INTRODUCTION

As part of FraudAction 360 (FA 360) and FraudAction Cyber Intelligence (FA CI), customers are entitled to a range of intelligence feeds, all gleaned from RSA's FraudAction intelligence operation.

ABOUT RSA'S FRAUDACTION INTELLIGENCE OPERATION

Our operation is comprised of a dedicated team of analysts who monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels where cybercriminals congregate to sell/buy services and tools and exchange knowledge.

Leveraging highly-skilled, multi-lingual expertise and years of underground presence, FraudAction analysts have been "grandfathered" into forums as trusted players. Our analysts cover activity in forums of different languages including English, Russian, French, Arabic, Spanish, Portuguese and others.

The forums vary in size, traffic volume and prestige. In many cases, the forums monitored by analysts are closed forums that require admission fees and "vouching" by a senior member(s). Some of the exclusive forums monitored by RSA are closed to new users and are considered by cybercriminals to be more secure exchange platforms.

FRAUDACTION CYBER INTELLIGENCE

FA CI is offered in 3 distinct tiers of service. Tiers vary in depth of content and coverage.

TIER 1: GENERAL INTELLIGENCE

Primarily designed for organizations interested in feed-based, automated intelligence consumption.

TIER 2: TARGETED INTELLIGENCE

For organizations that require the additional layer of proactive (human) investigation into deep-web sources.

TIER 3: ADVANCED INTELLIGENCE OPS

Offered to FraudAction 360 customers only, the tier provides holistic and comprehensive insight into the threat landscape as it relates to your brand and business operation—including deep visibility into attack-related data.

Comparison of Tier Offerings

		TIER 1	TIER 2	TIER 3
GENERAL	Threat Reports*	√	√	√
	IP Feed*	√	√	√
	Email Feed*	√	√	√
	e-Commerce Item Drops*	√	√	√
	Banking Mule Accounts*	√	√	√
	Enterprise Blacklists: Malicious Hosts	√	√	√
	Enterprise Blacklists: URL patterns	√	√	√
TARGETED	Compromised Credit Cards*		√	√
	Credit Card Store Previews		√	√
	Consumer: Compromised Credentials*		√	√
	Enterprise: Compromised Resources		√	√
	Consumer: brand specific Intel		√	√
	Enterprise: resource-specific Intel		√	√
ADVANCED OPS	On-Demand Research**			√
	ThreatTracker**			√

*Provided to FraudAction 360 customers

**Only available for FraudAction 360 customers

FraudAction Cyber Intelligence Tier 1:
GENERAL INTELLIGENCE

FA CI T1 is designed for organizations interested in feed-based, automated intelligence consumption. Feeds are available in several formats and can be integrated into different backend appliances/systems. The nature of intelligence is mostly general and includes complimentary access to Threat Reports that provide insight into emerging cybercrime threats and trends. The following is a breakdown of deliverables and their content.

THREAT REPORTS

Type:	General – Cyber-fraud industry alerts
Content:	Leveraging RSA highly-skilled expertise and nearly a decade of knowledge about fraud and the fraudsters' underground involvement, the RSA Team is very adept at maintaining a longstanding and watchful presence in the different cybercrime communities it monitors
Frequency:	Ad-hoc
Format:	PDF
Encryption:	Encrypted ZIP, PGP
Delivery:	Email
Categories:	RSA FraudAction customers receive Threat Reports on intelligence such as fraud trends, new scamming methodologies, new cybercrime tools and services offered in the underground. Threat Reports notify customers about new vulnerabilities that have been discovered or are in current use by cybercriminals in their attempts to target organizations.

IP FEED

Type:	General, however may contain corporate IPs
Content:	IPs/domains hosting malicious online activity and thus present a risk to your infrastructure.
Frequency:	Daily
Format:	CSV, XLS, EDS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP
Categories:	The feed contains different IP categories as listed below: – Proxies/SOCKS – proxies are used to facilitate access to content on the World Wide Web in order to provide anonymity to the individual using it. The IP addresses in this category are published or traded among fraudsters in the underground, and are used to hide the source of their fraudulent activity. – Open Source Proxies – IP addresses that are published on websites that offer free proxies. Although a legitimate service, it is often used also by fraudsters as a way of hiding the source of their fraudulent activity. – RDPs – RDP stands for Remote Desktop Protocol allowing remote connection to a Trojan-infected machine by the fraudster that hacked it.

This category is comprised of PC system coordinates (IP address and port number) that were publicly exposed and posted in the underground along with their login passwords.

- Bad IPs – IP addresses allegedly engaged in malware distribute activity, the likes of: spamming, DDoS, Phishing, malware, online scams and other gray-area web activities.
- TOR Nodes - TOR is free software for enabling online anonymity.

This category is comprised of IP addresses gathered from open source resources that share IP addresses of TOR exit nodes. Although a legitimate service, it is often used by fraudsters as a way of hiding the source of their fraudulent activity.

Customers can also choose to receive only specific categories.

Recommendations: Customers are advised to:

1. Monitor incoming communication from IP addresses of all categories as they may be utilized by fraudsters and other machines seen in the wild used for malicious activities.
2. Specifically for IP addresses in the "RDP" category, also monitor outgoing communication from these IPs, as the infected system may reside within the corporate network.

EMAIL FEED

Type:	General, however may contain corporate emails
Content:	Email addresses that have been shared on both underground and open source forums or gathered from Trojan logs. These emails are more likely to be in the hands of fraudsters and used in fraudulent activity.
Frequency:	Daily
Format:	CSV, XLS, EDS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP
Categories:	The feed contains different email categories as listed below: – Fraudster emails – email addresses that are in all probability used by fraudsters, collected from: – Lists published in the underground by hackers/fraudsters who hack into other forum member databases or hack the user databases of online CC shops – Lists published on open source public text sharing sites such as Pastebin.com – Database leaks caused by hacktivists – Lists extracted from underground forums reporting fraudsters who stole from others ('rippers') – Spam emails – Email addresses shared by fraudsters with fellow fraudsters, to be utilized in spam campaigns. As such, these emails are more likely to be targeted by Phishing and "Spear Phishing" emails.

- Compromised emails – Legitimate email addresses which are published along with their passwords and are therefore more likely to get exploited by fraudsters for identity theft or corporate network access
- Captured email Contacts- email addresses that were captured by malware from the contact lists of infected user PCs and as such are in the possession of botmasters who may use them to target your organization with Spear Phishing and malware-laden correspondence.

Customers can also choose to receive only specific categories.

Recommendations: Customers are advised to search for these emails within their user base and employees database.

1. When found in the user base - slightly increase the risk level of accounts associated with those email addresses.
2. When a corporate email is found in this list, based on the category, you may consider notifying the employee to be on alert as they are more likely to receive phishing emails.

E-COMMERCE ITEM DROPS

Type:	General
Content:	Physical mailing addresses to which 'reshipping mules' accept items purchased with stolen payment cards, and from which they forward them to their accomplices. Fraudsters who commit e-commerce fraud will typically conduct a change of billing address (COB) to match the shipping address.
Frequency:	Ad-hoc
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations:

Customers are advised to:

1. Flag and monitor transactions that involve these drop addresses, particularly changes matching a payment card's billing address with a drop address (COB) from the feed.
2. Bank accounts or payment cards used in connection with these addresses should be monitored for fraudulent activity.

BANKING MULE ACCOUNTS

Type:	General, however may contain accounts held at your bank
Content:	Bank accounts used to receive funds from compromised accounts.
Frequency:	Ad-hoc
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: Customers are advised to:

1. If the mule account is not held at your bank, block or monitor any outgoing transaction made to these accounts, as the account transferring the funds may have been compromised.
2. If the mule account is held at your bank, per your bank's policy, you can either close the account or leave it active for monitoring purposes. Monitoring incoming transactions to the mule account may reveal the compromised account, monitoring outgoing transactions from the mule account may reveal additional accounts involved in the fraud ring.

ENTERPRISE BLACKLISTS: MALICIOUS HOSTS

Type:	General
Content:	Host names that have been part of malicious online activity and thus present a risk to your infrastructure. A resource reported on the hosts list is attributed a category and one (or more) sub-categories: – Category defines the type of malware resource involved and can associate a host with a Trojan C&C Server, Trojan configuration file, Trojan drop zone, Trojan infection point, TOR node and others... – Sub-categories provide additional information when available and can include any description in connection with the category such as application protocol, affected port, Trojan family name and others... Each host can be attributed more than one sub-category, depending on the context it was reported in.
Frequency:	Daily
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: The data can be used to quickly and efficiently expose internal resources that are communicating to potential malware resources.

1. The feed should be imported into internal systems that monitor Internet traffic for your organization, using them to block/flag traffic going to malicious hosts and those that correspond with suspected patterns reported.
2. Check into the communication streaming from devices on your network that are found to be communicating with hosts associated with malware resources or other illicit activity.
3. For hosts and patterns connected with a specific malware family, look into devices on your network that may be infected and should be disconnected and cleaned.

ENTERPRISE BLACKLISTS: URL PATTERNS

Type:	General
Content:	The URL Patterns report is an easy to integrate blacklist, reporting URL patterns detected as part of resources that facilitate malicious online activity, and thus present a risk to your infrastructure. Trojans and exploit packs sold commercially in the underground, or privately operated by cybercriminals, oftentimes create the same paths on the resources they are launched through. URL patterns are telling of malware communication resources because Trojans' setup wizards often create the same folders for all deployments, which are rarely modified by botmasters. The patterns thereby allow for tracking of resources that are part of known botnets, and attribute them to a specific Trojan family. The URL Patterns report will present the patterns in context, showing the typical path alongside a category and a sub-category. – Category defines the type of malware resource involved and can associate a host with a Trojan C&C Server, Trojan configuration file, Trojan drop zone, Trojan infection point, TOR node and others... – Sub-categories provide additional information when available and can include any description in connection with the category such as application protocol, affected port, Trojan family name and others... Each pattern can be attributed more than one sub-category, depending on the context it was reported in.
Frequency:	Daily
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: The data can be used to quickly and efficiently expose internal resources that are communicating to potential malware resources.

1. Feed the reports to internal systems that monitor Internet traffic for your organization, using them to block/flag traffic going to malicious hosts and those that correspond with suspected patterns reported.
2. Check into the communication streaming from devices on your network that are found to be communicating with hosts associated with malware resources or other illicit activity.
3. For hosts and patterns connected with a specific malware family, look into devices on your network that may be infected and should be disconnected and cleaned.

FraudAction Cyber Intelligence Tier 2:
TARGETED INTELLIGENCE

This tier is designed for organizations that require the additional layer of proactive (human) investigation into deep-web sources. Tier 2 includes all Tier 1 deliverables (see above) with the addition of highly-targeted (relating directly to your brand) threat feeds. Furthermore, our analysts proactively investigate and research deep-web sources in search for intelligence relating to your brand.

COMPROMISED CREDIT CARDS

Type:	Targeted - Customer-specific based on customer's BIN numbers
Content:	Compromised Credit/Debit card numbers traced in the underground and open source
Frequency:	Ad-hoc
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: Customers are advised to:

1. Validate the card information provided
2. Immediately block the credit/debit cards recovered as these details are accessible to fraudsters. The card details may be used to commit fraud

CREDIT CARD STORE PREVIEWS

Type:	Targeted - Customer-specific based on customer's BIN numbers
Introduction:	Automated Credit Card Stores sell credit/debit card data to fraudsters in the underground. Fraudsters browse through a shop's credit card "catalog" which includes partial information on the compromised card (e.g. six-digit BIN, cardholder's name and address). Once a card is purchased, the store reveals the complete credit card information for the use of the purchasing fraudster. Data is sent as recovered from the store, (i.e. the partial information that is visible without purchasing the cards).
Content:	Partial card details obtained from both known and newly-discovered underground online shops. An automated parser periodically downloads new card previews from these stores, which are then delivered to customers via the feed.
Frequency:	Ad-hoc
Format:	CSV, XLS There are two columns in the CC Previews Feed Excel spreadsheet: six-digit BIN followed by ten "o"s; and the BIN along with any info that was attached to it (e.g. cardholder name, address, and issuer).
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: In many cases issuers can use the partial information to trace the compromised cards' full details. The early tracing of cards is part of mitigating future fraud attempts.

Customers are advised to review the compromised card previews and to attempt to trace their full details using the extracted data. It is then recommended to do the following:

1. Verify whether the cards are truly "fresh" (they have yet to be used to commit fraud).
2. Block the compromised cards, or closely monitor their transactions.
3. Notify the affected cardholder as per the bank's policies.
4. Search for common denominators of all or most of the cards (such as a common demographic profile of cardholders). Such details may enable tracing.

CONSUMER: COMPROMISED CREDENTIALS

Type:	Targeted - based on customer's login URL
Content:	As part of RSA's FraudAction operation it monitors Trojan drop servers on a continuous basis. Any data, that has been captured by the Trojan, and that relates to your CUSTOMERS will be reported to you via the compromised credentials feed. For each record reported, you will see a raw text column which includes the unparsed data as it was recovered from the drop server.
Frequency:	Ad-hoc
Format:	CSV, XML Our system is capable of parsing the raw data (as retrieved from the drop site) into readable fields (or parameters). If you would like the system to parse specific fields (for example, your website requires your end-user to fill in custom login fields), you can provide the field names as they appear in the HTML form, and our system will attempt to parse them.
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, FA Dashboard Portal

Recommendations: There are 2 methods you can use to attempt to identify compromised end users:

1. Searching for the actual login credential sets within the raw data. The way to identify this data within the raw data varies based on the specific Trojan family involved.
2. Pairing the stolen date along with IP, and cross referencing with the incoming traffic to the website (login page).

Customers are advised to use the details in these alerts to trace affected accounts of customers infected with Malware. In general, it is advised to closely monitor these accounts for outgoing transfers, in an attempt to identify mule accounts or block them according to your policies

ENTERPRISE: COMPROMISED RESOURCES

Type:	Targeted – based on internal resources
Content:	As part of RSA's FraudAction operation it monitors Trojan drop servers on a continuous basis. Any data, that has been captured by the Trojan, and that relates to your EMPLOYEES and/or INTERNAL RESOURCES will be reported to you via the compromised credentials feed. For each record reported, you will see a raw text column which includes the unparsed data as it was recovered from the drop server.
Frequency:	Ad-hoc
Format:	CSV, XML
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, FA Dashboard Portal

Recommendations: There are 2 methods you can use to attempt to identify compromised end users:

1. Searching for the actual login credential sets within the raw data. The way to identify this data within the raw data varies based on the specific Trojan family involved.
2. Pairing the stolen date along with IP, and cross referencing with the incoming traffic to the website (login page).

Customers are advised to use the details in these alerts to trace affected accounts of employees infected with Malware.

CONSUMER: BRAND SPECIFIC INTEL

Type:	Targeted – based on keywords
Content:	The RSA team continuously monitors cybercriminal communication chatter for specific mention of your brands. Once such chatter is identified, we send out an alert, and depending on its severity and credibility, investigate further to provide you with as much information as possible on the threat. The alerts will provide classification information including severity and credibility as well as the targeted channel, geography, and indicators when they are available.
Frequency:	Ad-hoc
Format:	PDF alerts and CSV/XLS Bulletins
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: The alerts will include recommendations when applicable

ENTERPRISE: RESOURCE-SPECIFIC INTEL

Type:	Targeted – based on internal resource identifiers
Content:	The RSA team continuously monitors cybercriminal communication chatter for specific mention of your organization. Once such chatter is identified, we send out an alert, and depending on its severity and credibility, investigate further to provide you with as much information as possible on the threat. The alerts will provide classification information including severity and credibility as well as the targeted channel, geography, and indicators when they are available.
Frequency:	Ad-hoc
Format:	PDF alerts and CSV/XLS Bulletins
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP

Recommendations: The alerts will include recommendations when applicable

FraudAction Cyber Intelligence Tier 3:
ADVANCED OPS

Tier 3 is offered to FraudAction 360 customers only, and provides holistic and comprehensive insight into the threat landscape as it relates to your brand and business operation via the ThreatTracker report. The ThreatTracker report fuses intelligence gathered from phishing and malware attacks together with our deep-web operation; the report provides visibility across attack vectors, attack clusters and the personas behind these attacks. The tier includes all tier 1 and 2 deliverables with the addition of ad-hoc on-demand research which you can request at any time.

ON-DEMAND RESEARCH

Type:	Targeted- based on customer request
Content:	On-demand Research provides you with the ability to request cybercrime research or investigations - on demand. Our visibility into the deep web can help with external fraud indicators such as: IP address, an actor's handle, or a specific Anonymous op. Our team of experienced researchers will leverage proprietary technology to search a variety of data sources for further intelligence. We can also maintain an active monitor that will send an alert whenever a finding is made.
Frequency:	Per request
Format:	PDF
Encryption:	Encrypted ZIP, PGP
Delivery:	Email

Recommendations: The research report will include recommendations when applicable

THREATTRACKER

Type:	Targeted – based on customer cyber attacks
Content:	The ThreatTracker report provides a holistic and insightful view into the threat your organization faces by consolidating data gathered from our Phishing, malware, and cybercrime intelligence operations. The data is correlated and contextualized to deliver insight into three key areas:

Threat Clusters

With Phishing and malware attack volumes constantly rising, it becomes increasingly difficult to assess the risk associated with each attack. Does each Phishing attack carry the same level of risk? Is a specific Trojan attack considered a more significant threat than another? With the increase in attack volumes, more noise is generated in the system and assessing risk becomes challenging.

RSA takes a holistic approach to assessing the threat (or risk) level by gathering and correlating data points from across the different attacks, identifying commonalities, and connecting attacks together based on numerous similarities and advanced correlation algorithms into a Threat Cluster. The Threat Cluster represents an attack campaign targeting your organization. By clustering attacks together, we can better understand the severity of a single attack and of the entire cluster.

The ThreatTracker report provides insight into specific clusters, as well as graphs showing cluster trends over time.

Threat Vectors

After identifying the Threat Clusters, we further analyze each attack, and the entire cluster itself, to better understand the method(s) by which the threat actor will attempt to defraud your organization.

By analyzing the data elements requested in phishing and malware attacks, and correlating them with our underground intelligence, we are able to indicate the probable vector (online banking, telephone/call center, ATM, etc.) the attacker will leverage to complete his attack.

Furthermore, Threat Vectors will alert you to anomalous data elements requested in attacks, which can provide insight into new attack tactics being tested by fraudsters.

Threat Actors

Through our detailed analysis of attacks, and by leveraging our human intelligence operations, we work to identify the actors behind the attacks targeting your organization. As we piece the evidence together, we create actor profiles and attribute attacks to specific attackers. Once identified, we continue to track and monitor the actor's activity, and report on any new findings we come across.

The ThreatTracker is a powerful tool that can allow organizations, at a glance, to better understand the threats they face, assess them, and plan mitigation steps accordingly.

Frequency:	Monthly
Format:	PDF
Encryption:	Encrypted ZIP, PGP
Delivery:	Email

Recommendations: The report will include recommendations when applicable

ABOUT FRAUDACTION

RSA FraudAction is a managed threat intelligence service which provides global organizations with 24x7 protection and shutdown against phishing, malware, rogue mobile apps and other cyber attacks that impact their business. Supported by 150 analysts in RSA's Anti-Fraud Command Center, the RSA FraudAction service analyzes millions of potential threats every day and has enabled the shutdown of more than one million cyber attacks. For more information, contact FAS.Inquiries@RSA.com.

RSA®

www.emc.com/rsa

ABOUT RSA RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, visit www.rsa.com.