SOLUTION BRIEF

RSA® FRAUDACTION™ CYBER INTELLIGENCE

TABLE OF CONTENTS

ABOUT THE RSA FRAUDACTION INTELLIGENCE OPERATION

The RSA FraudAction intelligence 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 and buy services and tools and exchange knowledge.

Leveraging highly skilled, multilingual expertise and years of underground presence, RSA FraudAction analysts have been "grandfathered" into forums as trusted players. Our analysts cover activity in forums of different languages, including Chinese, 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.

RSA FRAUDACTION CYBER INTELLIGENCE

RSA FraudAction Cyber Intelligence is offered in three distinct tiers of service, which 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

This tier includes all tier 1 and 2 deliverables with the addition of ad hoc, on-demand research.

COMPARISON OF TIER OFFERINGS		TIER 1	TIER 2	TIER 3
GENERAL	Threat Reports	√	√	√
	IP Feed	√	√	√
	Email Feed	√	√	√
	E-Commerce Item Drops	√	√	√
	Banking Mule Accounts	√	√	√
TARGETED	Compromised Credit Cards		√	√
	Credit Card Store Previews		√	√
	Compromised Credentials		√	√
	Brand-Specific Intel		√	√
	Enterprise Blacklists: Malicious URLs		√	√
ADVANCED	On-Demand Research			√

RSA FRAUDACTION CYBER INTELLIGENCE TIER 1: GENERAL INTELLIGENCE

This tier is designed for organizations interested in feed-based, automated intelligence consumption. Feeds are available in several formats and can be integrated into different back-end 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 long-standing 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
Content:	IP addresses that are more likely to route fraudulent traffic, extracted from cybercrime and fraudster-published lists
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, which allows 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. – 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
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: – 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 that are published along with their passwords and are therefore more likely to get exploited by fraudsters for identity theft or corporate network access Customers can also choose to receive only specific categories.
Recommendations:	Customers are advised to search for these emails within their user base and increase the risk level of accounts associated with those email addresses, per the company's security policy.

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 (COB) address to match the shipping address.
Frequency:	Ad hoc
Format:	CSV, XLS, EDS
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
Content:	Bank accounts used to receive funds from compromised accounts
Frequency:	Ad hoc
Format:	CSV, XLS, EDS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP
Recommendations:	Customers are advised to block or monitor any outgoing transaction made to these accounts, as the account transferring the funds may have been compromised.

RSA 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, EDS
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, EDS There are two columns in the CC Previews Feed Excel spreadsheet: six-digit BIN followed by ten "0"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.

COMPROMISED CREDENTIALS

Type:	Targeted—based on customer's login URLs
Content:	As part of the RSA 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.
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 two 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 data, 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 end users 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

BRAND-SPECIFIC INTEL

Type:	Targeted
Content:	The RSA team continuously monitors cybercriminal communication channels in order to pick up compromised data or chatter specific to your brands. Alerts may include cash-out methods, compromised corporate email accounts, mule accounts held at your bank and more.
Frequency:	Ad hoc
Format:	Varies depending on findings (PDF or CSV/XLS)
Encryption:	Encrypted ZIP, PGP
Delivery:	Email, SFTP
Recommendations:	The alerts will include recommendations when applicable.

ENTERPRISE BLACKLISTS: Malicious URLs

Type:	General
Content:	URLs participating in online malicious activity and may present a risk to your infrastructure This feed is intended to be used for network traffic blocking, filtering and investigation. To better evaluate risk levels, the feed includes additional insights on the threat as detailed below: • "Liveness" tests are performed for each reported URL, allowing us to determine and report its status. • Classification is provided whenever available and may include the following indicators: malware type, name and known affected operating system (e.g., Trojan:Win32/Kovter). • Hash values are provided when possible and include the ssdeep along with the MD5 hash. To support different preferences of consumption, customers may choose between two reporting options: 1. Incremental—reports only on new URLs, online and offline, identified since the last feed was dispatched. 2. Accumulative—reports on known URLs from the past 120 days. Customers who choose this option will receive two files, one containing known online URLs and one containing URLs that became offline in the last seven days.
Frequency:	Daily
Format:	CSV, XLS
Encryption:	Encrypted ZIP, PGP
Delivery:	Email (Incremental Only), SFTP
Recommendations:	In order to use the blacklists effectively, the following best practices are recommended: Import the reports into internal systems that monitor internet traffic to and from your organization. Set up rules to help identify and block or flag traffic to/from malicious hosts and/or that correspond with suspected URLs. If you have identified a device that is communicating to a malicious host/URL, it may be infected and should be investigated and remediated accordingly. Use the classification when applicable to further help identify the malware in question and evaluate its risk.

RSA FRAUDACTION CYBER INTELLIGENCE TIER 3: ADVANCED OPS

Tier 3 provides holistic and comprehensive insight into the threat landscape as it relates to your brand and business operations leveraging advanced research capabilities. The tier includes all tier 1 and 2 deliverables with the addition of ad hoc, on-demand research.

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, a specific anonymous op or specific malwares and phishing kits. Our team of experienced researchers will leverage proprietary technology to search a variety of data sources for further intelligence.
Format:	PDF
Encryption:	Encrypted ZIP, PGP
Delivery:	Email
Recommendations:	The research report will include recommendations when applicable

ABOUT RSA FRAUDACTION

RSA FraudAction is an external threat management service that provides global organizations with 24x7 protection and shutdown against phishing, malware, rogue mobile apps, rogue social media business profiles and other cyber attacks that impact their business. Supported by 100+ analysts in the RSA 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.

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 rsa.com.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.