SOLUTION BRIEF

RSA® FRAUDACTION™ 360

AT A GLANCE

End-to-end protection against phishing, Trojans, rogue mobile apps and social media threats, from detection to shutdown

Intelligence reports and feeds on latest online threats including new fraud trends

Access to detailed attack reports via the RSA FraudAction dashboard—the online reporting portal

INTRODUCTION

The online channel has never experienced such an innovative, globally integrated crime network as the one it faces today. Criminals have the most advanced technologies at their disposal and operate a sophisticated underground economy:

- Phishing continues to grow
- Trojans are more sophisticated and easier to obtain
- Rogue mobile apps infiltrate public app stores
- Social media is riddled with fake business pages

To date, RSA® FraudAction™ has:

- Shut down over 1 million cyber attacks
- Identified over 1 billion cyber attacks globally
- Recovered hundreds of millions of compromised credentials

The need to have protection against these different types of attacks is critical because they are becoming more and more interrelated—Trojans often have a mobile app component. Social media has become a new haven for fake business pages, created by cybercriminals to mislead consumers.

For complete fraud protection, organizations are challenged either to manage multiple vendors—multiple service metrics, budget requirements and different business relationships, as services for different threat vectors are provided by different vendors—or they have to be selective and prioritize one threat vector over others and take the risk of becoming vulnerable to certain attack types.

RSA FRAUDACTION 360

In order to defend against today's complex attack schemes, RSA FraudAction 360 combines all the threat vectors into an all-inclusive external threat management service for complete fraud protection against phishing, Trojan attacks, rogue apps and social media threats. Additionally, customers can gain deeper insight into emerging threats with intelligence reports that provide visibility into the cybercrime underground.

EXTERNAL THREAT MITIGATION

With an all-encompassing service, organizations can:

- Deploy fewer in-house resources to manage external threats
- Obtain full fraud protection without leaving any threat vector uncovered
- Manage only one vendor budget for 24/7 anti-fraud operations

The RSA FraudAction 360 external threat management service offers the following components:

- Anti-Phishing
- Anti-Trojan

- Anti-Rogue Mobile App
- Social Media Threat Protection
- Select RSA FraudAction Cyber Intelligence Data Feeds and Reports

ANTI-PHISHING

RSA FraudAction detects and mitigates phishing attacks. The service is designed to help organizations respond to an attack when it takes place and perform detailed forensics following an attack.

MONITORING AND EARLY DETECTION

RSA employs multiple early detection strategies including monitoring customers' weblogs. RSA FraudAction detection resources enable our analysts to scan billions of URLs per day, including customers' abuse mailboxes, and perform both automated heuristic and manual qualification of suspicious URLs.

REAL-TIME ALERTS AND REPORTING

Once a suspicious URL is confirmed to be a threat, customers are immediately notified and can monitor the latest threat information and status in real time via the RSA FraudAction dashboard. The online reporting portal also provides shutdown timeframes as well as industry and geographic trends.

EXCLUSIVE SITE-BLOCKING NETWORK

RSA has become the first line of defense for over 96% of the world's web traffic with its blocking feed for users of all major internet browsers, including mobile browsers and customers of leading data security providers and ISPs. As soon as the attacks are identified, near real-time feeds of phishing sites are sent to these organizations, which enable them to block phishing sites within minutes of their detection.

SHUTTING DOWN PHISHING SITES

RSA leverages its long-standing relationships with over 16,000 different hosting authorities and its multilingual capabilities to enable the quick shutdown of fraudulent sites on a global scale. To date, RSA has been responsible for shutting down more than 1 million fraudulent sites hosted in more than 187 countries.

ANTI-TROJAN

RSA FraudAction detects and mitigates the damages caused by Trojan attacks. The service is designed to identify malware threats, respond to an attack when it occurs and minimize the threat by blocking end-user access to the attack's online resources.

IDENTIFICATION AND ANALYSIS

RSA FraudAction has formed a network of partners in order to achieve a high level of detection. This network includes organizations in several technology areas, including consumer antivirus firms, intelligence operations and internet gateways.

RSA FRAUDACTION THREAT REPORTS

RSA FraudAction 360 customers receive threat reports on intelligence, such as fraud trends, new scamming methodologies, new cybercrime tools and services offered in the underground.

RSA FraudAction threat reports notify customers about new vulnerabilities discovered or in current use by fraudsters, cash-out methods or any other methods fraudsters use in their attempts to target organizations.

When an RSA FraudAction partner detects malware, the Trojan's information is sent to the RSA Anti-Fraud Command Center (AFCC) for investigation. Expert analysts perform static and dynamic analysis, which uncovers triggers, communication points and other data, as well as the Trojan's modus operandi on an infected system. When possible, Trojan drop points are monitored in an attempt to recover end-user credentials that have been compromised.

SHUTDOWNS

RSA works on behalf of customers to shut down fraudulent sites connected to each attack's infection points. After the fraudulent sites are uncovered and analyzed, the RSA AFCC initiates the site shutdown with the cease-and-desist procedure through interaction with ISPs, web hosting facilities and domain registration providers.

ANTI-ROGUE MOBILE APP

RSA FraudAction helps organizations reduce fraud losses by taking action against malicious or unauthorized "rogue" mobile apps. The service monitors all major app stores, detects apps targeting organizations' customer bases and shuts down unauthorized apps—reducing threats to organizations' reputation and financial losses due to mobile app fraud.

MONITORING AND DETECTION

The service delivers constant visibility into mobile app stores, providing a proactive online defense for organizations. Continuous monitoring of apps stores helps organizations to stay ahead of potential threats and be aware as soon as an unauthorized app surfaces.

SHUTTING DOWN ROGUE APPS

After detection and shutdown approval, RSA initiates the removal of the rogue app. The service ensures customers' control over apps representing their organization, allowing only apps issued and/or authorized by the organization to be available in the app markets. The service also ensures that customers and hundreds of millions of online mobile app users are prevented from accessing phishing, malware and other unauthorized apps even before the rogue apps gain exposure and popularity within the app stores.

SOCIAL MEDIA THREAT PROTECTION

Social media has emerged as an integral communication fabric that weaves together your organization's brand and associated service offerings with clients. As threat vectors have emerged through new social threads, cybercriminals are abusing social media pages to conduct fraud or initiate a fraud scheme. Organizations are challenged with the task of persistently monitoring for risk across digital channels, including social media, as manual, in-house options struggle to address risk management needs.

CUSTOMER FEEDBACK

"By implementing the RSA FraudAction, we have accelerated our ability to neutralize phishing attacks from weeks to just a few hours. We have also averted millions of Czech crowns-worth of fraud losses, which is great news for us and – more importantly – our customers."

-Large European FI

RSA FraudAction is designed to provide visibility into social media pages and help organizations distinguish between authorized business pages and potentially hazardous ones. By monitoring social media, RSA FraudAction identifies pages that are directly linked to fraudulent activities targeting your organization, or attempting to mislead your clients by presenting themselves as your organization and/or affiliates. RSA FraudAction enables organizations to rapidly remediate social media fraud threats before severe, long-lasting damage occurs.

RSA FRAUDACTION CYBER INTELLIGENCE

The RSA FraudAction Cyber Intelligence operation provides insight into cybercrime trends and in-depth investigations into fraud methods and operations within the global cybercriminal underground.

Complimentary feeds and reports from the RSA FraudAction Cyber Intelligence Tier 1 service are included in RSA FraudAction 360 without any additional fee. These threat reports and data feeds can be easily integrated into other back-end systems.

RSA FRAUDACTION 360 INTELLIGENCE DELIVERABLES:

- **IP Feed:** Daily list comprised of high-risk IPs, such as proxies/SOCKS and RDPs
- **Email Feed:** Daily list of compromised corporate personal employee email addresses and spam emails
- **Mule Accounts Feed:** Comprised of mule accounts recovered by RSA intelligence analysts
- **Item Drops Feed:** Comprised of physical mailing “drop” addresses to which “reshipping mules” accept items purchased with stolen cards
- **Credit Card Feed:** Comprised of compromised credit/debit card details traced in the underground
- **Quarterly Newsletter:** Global phishing statistics and Trojan statistics as well as an overview of reported trends from the past quarter
- **Threat Reports:** Report findings on new attack methods and trends from the cybercrime underground

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 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, go to rsa.com.

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