RSA

RSA FRAUDACTION™ 360

SOLUTION BRIEF

RSA FRAUD & RISK INTELLIGENCE

RSA

TABLE OF CONTENTS

AT A GLANCE

24/7 end-to-end protection against phishing, Trojan and mobile rogue app attacks

Intelligence reports and feeds on latest online threats and fraud trends

Access to detailed attack reports via an online dashboard and API

Complete external threat mitigation—no integration required; simple and quick setup process

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

– Trojan kits are more sophisticated and easier to obtain

– Rogue mobile apps infiltrate public app stores

In the past year, FraudAction Services:

– Handled over 500,000 phishing attacks targeting its customers

– Recovered 100s of millions of compromised credentials and financial information (credit cards, mule accounts, etc.)

– Analyzed over 4.8-million malware samples

The need to have protection against these different types of attacks is critical because they are becoming more and more interrelated —most Trojans now have a mobile app component.

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.

FRAUDACTION THREAT REPORTS

RSA FraudAction Service customers receive Threat Reports on intelligence such as fraud trends, new scamming methodologies, new cybercrime tools and services offered in the underground.

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.

FRAUDACTION 360

In order to defend against today's complex attack schemes, FA360 combines all the threat vectors into an all-inclusive external threat management service for complete fraud protection against phishing, Trojan attacks, and rogue apps. 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

PHISHING DETECTION AND SHUTDOWN

RSA FraudAction Service 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. 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 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 multi-lingual capabilities to enable the quick shut down of fraudulent sites on a global scale. To date, RSA has been responsible for shutting down more than 800,000 fraudulent sites hosted in more than 187 countries.

" By implementing the RSA FraudAction service, 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."

DAVID LORENC, DIRECTOR, DIRECT BANKING, ˇCESKÁ SPORˇITELNA

TROJAN ANALYSIS

RSA FraudAction Service 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

The FraudAction Service 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 anti-virus firms, intelligence operations and Internet gateways.

When a FraudAction service 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.

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 AFCC initiates the site shut down with the cease-and-desist procedure through interaction with ISPs, web hosting facilities and domain registration providers.

DEFENSE AGAINST ROGUE APPS

RSA FraudAction Service 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 organization's customer base 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 shut down 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.

CYBER INTELLIGENCE

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

Complimentary feeds and reports from the FraudAction Cyber Intelligence service are included in the FraudAction 360 service without any additional fee to provide the holistic, 360°, end-to-end threat detection and response service. These threat reports and data feeds can be easily integrated into other backend systems such as RSA Web Threat Detection.

FraudAction 360 Intelligence Deliverables:

- **IP Feed:** Daily list of comprised of IP addresses of proxies/SOCKS, RDPs, open source proxies,
  bad IPs, and fraudster IPs
- **Email Feed:** Daily list of compromised corporate and personal employee email addresses and spam emails
- **Mule Accounts Feed:** comprised of mule accounts recovered by RSA intelligence analysts and Trojan researchers
- **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

RSA

www.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, go to www.rsa.com.