



The Security Division of EMC

RSA Solution Brief

RSA FraudAction™ Service for Government Agencies



Government agencies are more vulnerable to cyber threats than ever before. Online criminals, digital spies and other malicious actors have new tools at their disposal and are becoming more capable than ever before. While financial institutions have traditionally been the primary focus of online attacks, government agencies are becoming a new favored target because of the wealth of sensitive data they collect and store.

In addition, new types of online threats such as Trojans, man-in-the-middle attacks and key-loggers are becoming more widespread through activities such as the increased use of social networking sites and sophisticated spear phishing attacks targeted at government employees.

There are a number of motivations for cyber attacks against the government as criminals seek to:

- Steal credentials of citizen-facing and government employee portals
- Collect personally identifiable information that can facilitate the commission of identity theft and account takeover
- Commit digital spying and information theft to acquire classified government data
- Inflict damage on critical infrastructure and information systems

The RSA FraudAction™ service is geared toward mitigating the impact of phishing, pharming and Trojan attacks that occur in the online channel. Offered as an outsourced, managed service, the RSA FraudAction service allows organizations to minimize resource investment while deploying a solution quickly. And with cyber attacks originating from all over the world, it delivers an integrated network of global partners dedicated to providing protection against malicious threats.

At the core of the FraudAction service is RSA's exclusive Anti-Fraud Command Center (AFCC). An experienced team of fraud analysts work 24x7 to identify, block, shut down and investigate cyber attacks. The Anti-Fraud Command Center has been leading the way through results, achieving several milestones and announcing major fraud discoveries. Accomplishments include:

- The shut-down of nearly 300,000 cyber attacks in 140 countries
- An extensive network of over 10,000 hosting entities and partners to enable the quick detection, blocking and shut-down of malicious websites
- Pioneered the first anti-Trojan and anti-pharming service in the industry
- The announcement of several major intelligence findings including the discovery of caches of stolen credentials and insight into the latest technologies and tactics being used by cybercriminals

The Anti-Fraud Command Center has shut down nearly 300,000 cyber attacks in 140 countries.



RSA FraudAction Anti-phishing Service

Phishing remains a growing threat to organizations across the globe. The number of phishing attacks identified by RSA in 2009 increased 16 percent from 2008. And just as attacks continue to grow, so does their level of sophistication. To demonstrate, in the RSA 2010 Global Online Consumer Security Survey, three out of ten consumers stated that they had been the victim of a phishing attack, despite the fact that awareness of the threat doubled in just two years.

RSA uses a rigorous process to mitigate the threat and impact of phishing attacks. Fraud analysts work cross-functionally across a number of tasks including detection, phishing analysis, blocking and shut-down. The Anti-Fraud Command Center has established relationships with over 10,000 web hosting service partners and some of the world's leading browser developers and ISPs — Microsoft, AOL, Netscape, EarthLink, Google Chrome, Mozilla FireFox and Safari — to ensure the fastest blocking and shut-down of phishing sites.

RSA FraudAction Anti-Trojan Service

The lack of noticeable effect is one of the main issues that organizations encounter in their ability to detect Trojans. In addition, a Trojan is designed to be “silent,” and infected users are likely to be completely unaware of its presence on their computer. It is not uncommon for some Trojans to remain undetected by most anti-virus software for months. For example, in one study, researchers found that the Zeus Trojan, one of the most prolific pieces of malware in use today, was only detected 23 percent of the time by updated anti-virus applications*.

RSA offers a dedicated team of analysts focused solely on service delivery for customers of the RSA FraudAction Anti-Trojan service. Because of the specialized nature of the tasks they perform, Trojan analysts are typically more technically-oriented and require additional advanced training.

The Anti-Fraud Command Center pioneered the first anti-Trojan and anti-pharming service in the industry.


They work with an extensive network of partners to detect Trojans in the wild and a number of blocking partners — including leading ISPs; Internet browsers; e-mail providers; anti-virus, anti-spam and firewall firms and web hosting providers — to ensure the fastest blocking and shut-down of identified Trojan infection, update and drop points.

RSA FraudAction Intelligence

The RSA FraudAction Research Labs work alongside analysts at the Anti-Fraud Command Center and is staffed by top-of-the-line researchers who are dedicated to studying the latest technology, tools and tactics being leveraged by cybercriminals. This team is assigned to tackle any new threat that general fraud analysts are not trained or prepared to address and serves as the source for many of RSA's major intelligence discoveries.

One of the objectives of the FraudAction Research Labs is to build the tools and processes that enable fraud analysts to handle the newest threats for RSA customers. For example, if a new Trojan class is identified, FraudAction Research Labs will investigate it to learn how it operates and determine the best methods for mitigation. Next, the Labs create the tools and processes for addressing the Trojan so that analysts will have the protocol to handle future attacks involving new variants of the same Trojan class.

* Source: Trusteer



RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, governance & risk management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2010 RSA Security LLC. All Rights Reserved.
RSA, BSAFE, SecurID, FraudAction, the RSA logo, RSA Security are either registered trademarks or trademarks of of EMC Corporation in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies.

FAGOV SB 0210



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC