



RSA® FraudActionSM Anti-Trojan Service

At a Glance

- Proactively identify crimeware that is targeting your organization and your online users
- Understand how the crimeware operates through detailed analysis of infection points, command-and-control servers, and drop sites
- Block access to known infection points
- Shut down infection points and drop zones that collect stolen credentials

It has been stated that Trojans accounted for nearly half of all new malware variants detected in 2006. With the rise of advanced threats such as Trojans – and specifically crimeware – organizations continue to confront the challenge of protecting the sensitive personal data of their online users. While phishing attacks can be damaging and expose sensitive data, they are typically waged against a specific target or set of targets, and require the user to take action on a fraudulent site. Financial Trojans – or crimeware – on the other hand, silently infect online users' computers for the purpose of stealing valuable data for later use or hijacking users' secure sessions, then carrying out fraudulent activity after the user has logged off.

Furthermore, it is not uncommon for financial Trojans to remain undetected for months, as evidenced by the "Gozi" Trojan. So how can organizations protect their users from being attacked by Trojans?

The RSA® FraudActionSM Anti-Trojan Service provides a proactive, comprehensive approach to helping organizations fight back against the threat of crimeware and Trojans – by mitigating it at the source.

The Anti-Trojan service addresses two types of financial Trojans:

- **Identity theft:** Crimeware designed to steal credentials such as usernames or passwords that can be used to commit fraud at a later date
- **Funds transfer:** Crimeware designed to automatically transfer funds through a user's own browser session after successful login

FraudAction Anti-Trojan helps organizations to:

- Identify what crimeware is targeting their users
- Analyze how the associated crimeware operates
- Block access to known infection points on the web to minimize the impact on their online users
- Shut down infection points and drop zones that collect stolen credentials

How does it work?

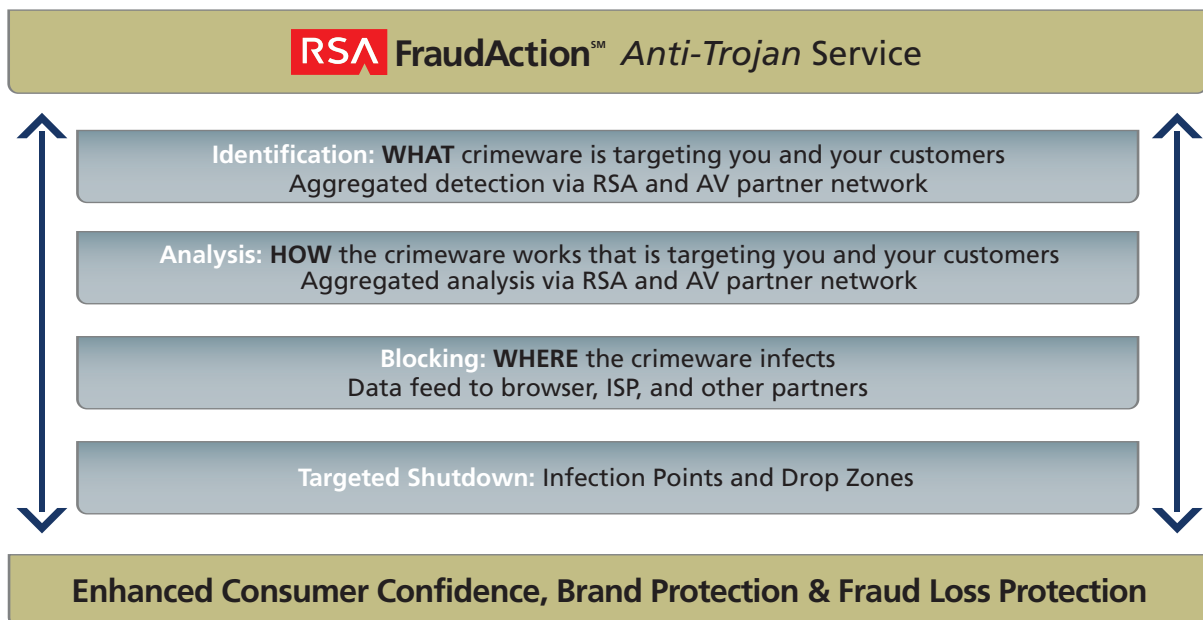
Through the exclusive RSA 24x7 Anti-Fraud Command Center (AFCC) and an extensive global partner network, RSA delivers a layered approach to identifying, analyzing, blocking, and shutting down crimeware attacks.

Identification and Analysis

By combining the data identified by RSA's Anti-Fraud Command Center and our partner network of anti-virus providers, RSA is able to identify what crimeware is targeting your organization and your customers, and then carry out a comprehensive analysis of how the crimeware operates.

By understanding how crimeware is infecting users and how it is being controlled via command-and-control and identifying where stolen credentials are dropped, proactive steps can be taken to mitigate the threat.





Blocking and Shutdown

When a site is identified and confirmed to be distributing crimeware, the AFCC, through its established partnerships with nearly 4,000 ISPs, registrars, browser developers, and enterprise gateway partners around the globe, works on a 24x7 basis to block and shut down infection points that distribute Trojans and also shut down known drop sites where stolen credentials are sent. In addition, the AFCC provides multi-lingual translation support in over 150 languages to further enhance its ability to quickly shut down known infection points and drop sites.

The RSA FraudAction Anti-Trojan service provides a holistic approach to fighting the threat of crimeware.



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

The Security Division of EMC

©2007 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, the RSA logo and FraudAction are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

ANTITROJ SB 0407