RSA® FRAUDACTION™ ANTI-TROJAN SERVICE

Proactive protection against Trojans and malware

AT-A-GLANCE

- Proactive protection against Trojans and malware 24x7, 365 days-a-year
- Dedicated team of Trojan experts provide round-the-clock analysis and real-time shutdown of Trojan attacks
- In-depth research and reverse-engineering of crimeware
- Comprehensive blocking network to prevent new users from infection
- Actionable data including recovered credentials and money mule accounts
- Proven results with more than 500,000 fraudulent online resources shutdown

DATA SHEET

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. Trojans and crimeware can be directly attributable to their flourishing business. Trojans are becoming increasingly popular for two primary reasons – increased consumer awareness and the accessibility of crimeware.

- **Increased consumer awareness** – Consumers are becoming educated about the threat of phishing and are more likely to be able to spot a suspicious email requesting their personal information resulting in lower yields for criminals that harvest credentials through this method.
- **Easily accessible crimeware** – Sophisticated crimeware is becoming increasingly available for purchase in the underground, with publicly traded Trojan kits being offered to fraudsters along with user manuals and customer support giving beginner-fraudsters all the assistance they require to launch Trojan attacks.

RSA® FraudAction™ Anti-Trojan Service

The RSA FraudAction service is a proven solution that stops and prevents phishing, pharming and Trojan attacks that occur in the online channel. Offered as a managed service, the FraudAction solution allows organizations to minimize resource investment while deploying a solution quickly. It is supported by the RSA Online Threats Managed Services organization, a team of experienced analysts dedicated to staying abreast of the latest trends in online fraud, providing customers with the most up-to-date information.

The RSA FraudAction Anti-Trojan Service, a core part of the FraudAction solution, is focused on preventing Trojan attacks. The service is designed to respond to an attack when it occurs, and minimize the threat by blocking user access to the attack's online resources. When feasible, personal access credentials are recovered, enabling the blocking of compromised accounts before they are used to commit fraud.

The primary features of the FraudAction Anti-Trojan Service include:

- Near real-time identification and alerts of new attacks
- Detailed Trojan analysis including URL triggers, method of operation, and infection, drop and update points
- Real-time scanning of new attacks and notification of attacks' detectability by anti-virus software
- FraudAction Dashboard portal provides attack summaries and status updates
- RSA Global FraudAction Blocking Network

- Targeted shutdown of infection, drop and update points
- Credentials recovery evidence & data extraction
- Mule Harvesting
- Countermeasures – baits
- In-depth reports on the features, functionality and modus operandi of new crimeware.

Features

Identification and Analysis

One of the main issues that directly affects the ability of financial institutions to detect crimeware is the lack of noticeable effect. Financial Trojans often do not receive the same industry attention as other types of malware and spyware. Also, because crimeware is designed to be "silent," victims are much less likely to even be aware of its presence. It is not uncommon for financial Trojans to remain undetected by most anti-virus software for months.

The FraudAction Anti-Trojan 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.** These partners have widespread deployment of anti-virus software on personal computers, giving them the ability to detect crimeware "in the wild" as it attacks consumers.
- **Intelligence operations.** These partners detect crimeware threats by browsing through known malicious websites and social networking forums, many of which are located in the Internet "underground."
- **Internet gateways.** These partners are situated on the major hubs of Internet e-mail traffic and can provide early detection for crimeware by scanning billions of e-mails each day.
- **Automated crawling partners.** These partners are focused on detecting crimeware via "honey-pots" and proactive web crawling. Web crawling has the capability of detecting unknown variants that have yet to be categorized as outbreaks.

When a FraudAction service partner detects malware, the Trojan's analysis is sent to the RSA Anti-Fraud Command Center (AFCC). The Trojan is then processed by an automatic analysis engine which attempts to match the crimeware to a known Trojan "family." Further manual analysis performed by expert analysts enables the extraction of triggers, communication points and other data, as well as the identification of a Trojan's modus operandi on an infected system. Additional in-depth investigation of new and current crimeware codes, including the reverse-engineering of Trojan attacks, is performed by the RSA FraudAction Research Lab.

Dashboard Portal

The RSA FraudAction service provides customers with an attack (incident) overview report as well as access to the detailed attack reports in Web-based dashboard. The overview includes details of all known attacks and their critical information in one easy-to-view layout. Using the dashboard, authorized users at a financial institution can securely access and view the overall situation of all attacks simultaneously and in real-time.
The incident report includes the following information:

- Attack ID
- Attack detection time
- Trojan family
- Infection, drop & update points
- ISP/Registrar
- Trojan characteristics
- Mitigation steps taken
- Operational report

GROWING THREAT:

Man-in-the-browser Attacks

A man-in-the-browser attack occurs when a Trojan is installed on a user's computer that is capable of intercepting and/or interacting with the user's online transactions in real-time. Unlike a phishing attack, where the user is directed to a fraudulent website, a man-in-the-browser attack occurs simply when the user enters a URL into their browser – or clicks on a stored bookmark – independent of being triggered by a prompt such as an e-mail or other notification.

It operates in similar fashion to session-hijacking / funds-transfer malware in which the wiring out of funds occurs in real-time, and isn't otherwise focused on simply stealing credentials (such as an online banking username/password or credit card number) for use at a later time. A man-in-the-browser attack is a type of man-in-the-middle attack, but is done in the browser and closer to the user rather than on the traffic stream. A man-in-the-browser attack is more difficult to detect and prevent, however, because the action is actually occurring on the user's machine.

Additionally, an operational report is uploaded to each new incident on the dashboard. This cumulative report contains all incidents to date and the following information (in addition to the data provided by the incident report):

- MD5 hash
- File size
- Main functionalities
- Trigger type
- Specific Triggers
- Real time AV scan results

FraudAction Blocking Network – Preventing Access to Known Infection Points

Based on blocking feeds provided by RSA, access to confirmed crimeware sites is blocked by partners in the Global FraudAction Blocking Network. This blocking provides a first line of defense to 90% of the world's web traffic and prevents hundreds of millions of end users from landing on known malicious sites.

The FraudAction Blocking Network includes leading:

- ISPs
- Internet browsers
- E-mail providers
- Anti-virus firms
- Anti-spam firms
- Firewall firms
- Enterprise content filters

Once a crimeware strain has been analyzed and deemed malicious, the relevant resources are provided to the FraudAction Blocking Network Partners in order to prevent and block access to identified infection, drop and update points. By blocking these resources, the risk to online banking consumers is greatly reduced.

- Blocked infection points decrease the chances of additional victims getting infected.
- Blocked update points lower the chances of infected victims being redirected to new, updated locations.
- Blocked drop points effectively prevent any victims who might already be infected from transmitting their credentials to the criminal.

Shutdown

The faster a crimeware attack is mitigated the less damage it causes. However, shutting down fraudulent infection points, update points, drop sites and drop e-mails is more complicated than it seems. Issues such as foreign working hours, foreign holidays and language barriers must be taken into consideration. In most cases, crimeware is much less "visible" than phishing and more complex to detect due to numerous inherent stealth mechanisms coded into crimeware's functionality.

Before the process of shutting down a crimeware attack begins, there are several factors to consider, such as the ability to recover credentials and the risk of triggering crimeware evolution (resulting in more complex crimeware variants). Based on these factors, the RSA Trojan Lab will make a decision whether or not to start the shutdown process. The AFCC works on behalf of financial institutions to disable attacks by shutting down the fraudulent websites through interaction with ISPs, web hosting facilities and domain registration providers.

To date, the AFCC has successfully shut down over 500,000 fraudulent sites around the globe. The AFCC addresses the hurdles presented by foreign language barriers and is capable of submitting cease and desist forms in over 15 languages including Arabic, Dutch, German, Japanese, Russian, Chinese, English, Hungarian, Korean, Spanish, Czech, French, Italian, Romanian and Swedish. It also offers multilingual support and real-time translation services in more than 150 languages. With extensive multi-lingual capabilities, RSA is able to shut down a fraudulent site quickly, regardless of where the attack is being hosted.

By working with top financial institutions worldwide and monitoring multiple attacks, RSA has been able to establish and capitalize on long-standing relationships with some of the world's largest ISPs and registrars. Utilizing the AFCC to contact ISPs/Web hosting/Registrars and initiate the cease-and-desist procedure also speeds up the process of shutting down fraudulent sites in order to reduce the overall impact of an attack.

Credentials Recovery: Data Extraction & Evidence

The AFCC conducts an extensive investigation during and after an attack occurs in an attempt to extract additional valuable information. In some cases, the AFCC manages to retrieve the actual list of compromised personal information, as well as counts of submitted information, the IP address of victims, the crimeware binaries and more.

Investigations take place in parallel to the other remediation steps. In cases where the AFCC is able to extract the compromised data, a financial institution can immediately take action by suspending the compromised accounts and contacting customers that have been affected by the attack. This invaluable information allows financial institutions to significantly reduce the damage inflicted by crimeware and in turn, position their organization as one that proactively protects its customers against online attacks.

Extracted compromised information is also important for working with the law enforcement community. Due to a lack of resources, some law enforcement agencies may not handle a case without proof that it is big enough to potentially harm a large number of victims. The information is collected in legal ways only and stored using a set of tools that maintains the integrity of the data for use by the financial institution at a later date.

Mule Harvesting

Man-in-the-browser (MITB) attacks enable cybercriminals to perform unauthorized online transfers in real-time to mule accounts – illegitimate accounts which are established to receive stolen funds. The FraudAction Anti-Trojan service enables enhanced mitigation for MITB attacks by providing customers with information on mule accounts. The FraudAction Research Lab recovers mule accounts from Trojan resources including:

- Trojan configuration files
- Trojan binaries
- Update point administration panels
- Drop sites

By having the details on mule accounts, financial institutions can block any future transactions attempted to a mule account, thereby mitigating the threat posed by MITB Trojan attacks. Consequently, if a customer is infected with a MITB Trojan that is connected with a specific mule account reported by RSA, any efforts to transfer funds to that mule account will be prevented.

Baits Countermeasure

The baits countermeasures are designed as a proactive countermeasure against online fraud. Baits serve to "mark" attackers' online resources, allowing the targeted entity to block future fraud attempts made from culprits' systems. The baits countermeasure feeds a crimeware application with a limited amount of dummy responses which can be tracked to detect fraudulent activity. By tracking perpetrators' fraudulent activity from the login phase to an account's 'cashout,' the targeted banking channel is uncovered, and its potential vulnerabilities revealed. This enables the targeted entity to take appropriate mitigating measures, such as modifying security systems and procedures.

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.