THE RSA® ANTI-FRAUD COMMAND CENTER

Solution Brief

RSA

EMC²

The RSA Anti-Fraud Command Center (AFCC) addresses online fraud threats such as phishing, pharming and Trojan attacks on behalf of RSA customers. The AFCC is staffed with over 130 analysts and is part of the Online Threats Managed Services (OTMS) group which is responsible for carrying out all aspects of the RSA FraudAction service.

The AFCC has been leading the way through results, achieving several milestones and announcing major fraud discoveries. Some of the accomplishments of the RSA Anti-Fraud Command Center include:

- The shutdown of over 500,000 online attacks across 185 countries
- An extensive network of over 13,000 hosting entities and partners to enable the quick detection, blocking and shut down of fraudulent websites
- Pioneered the first anti-Trojan and anti-pharming service in the industry
- The announcement of several major intelligence findings including the new technologies and tactics being used by cybercriminals

Service Delivery Process

The AFCC consists of eight teams. Seven teams are staffed with fraud analysts that handle all service delivery for customers of the RSA FraudAction anti-phishing service and one team is staffed with analysts that are focused solely on service delivery for customers of the RSA FraudAction Anti-Trojan service. The AFCC works 24x7 — 365 days a year.

Anti-phishing

The AFCC uses a rigid process to mitigate the threat and impact phishing attacks have on our customers. Fraud analysts that work for anti-phishing customers work cross-functionally across a number of tasks including detection, phishing analysis, blocking, shutdown and forensics and credential recovery. The AFCC has established relationships with over 13,000 web hosting service partners and some of the world's leading browser developers and ISPs such as Microsoft, AOL, Netscape, EarthLink, Google Chrome, Mozilla FireFox and Safari to ensure the fastest blocking and shutdown of phishing sites.

Anti-Trojan

The AFCC has 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 more technically-oriented and require additional advanced training.

Trojan analysts 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 fasting blocking and shutdown of identified Trojan infection, update and drop points.

Training and Certification

RSA fraud analysts serve as the front line of defense in the battle against cybercrime for RSA FraudAction customers. As a result, RSA fraud analysts undergo a rigorous training and certification process in order to deliver the best results to our customers. Analysts are provided with in-depth training in all aspects of online fraud and are required to become certified which can take up to two months. Additional training is conducted for Trojan analysts because of the complex nature of the threats they handle. This process can take another one to two months.

Fraud Intelligence

RSA's fraud intelligence operations consist of three core teams: RSA FraudAction Research Labs, RSA Fraud Intelligence, and RSA Cybercrime Intelligence.

RSA FraudAction Research Labs

The RSA FraudAction Research Labs work alongside AFCC fraud analysts and is staffed by top of the line researchers who are dedicated to ongoing research into 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 Lab is to build the tools and processes that enable fraud analysts to handle the newest threats for customers. For example, if a new Trojan class is identified, FraudAction Research Labs will research the Trojan to learn how it operates and determine the best methods for mitigation. Next, they 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.

RSA Fraud Intelligence

In addition to the Research Lab, a dedicated team of fraud intelligence agents monitor and participate in key underground forums, IRC chat rooms, and other communication channels where cybercriminals congregate to sell and exchange tools such as Trojan and phishing kits and information obtained from cyber attacks. Through regular engagement and direct communication within these forums, RSA Fraud Intelligence agents are able to uncover pointed intelligence findings and get insight into new methods for committing fraud.

Leveraging highly-skilled expertise and years of underground involvement, RSA Fraud Intelligence agents have been "grandfathered" into forums as trusted players. Most agents have military experience and are multi-lingual which allows us access insight into forums including English, Russian and German. Each of these forums vary in size, traffic volume, and prestige, and their members vary in their level of sophistication. In many cases, the forums monitored by RSA Fraud Intelligence agents are closed forums that require admission fees and "vouching" by a senior member. Some of the exclusive forums monitored by RSA are now closed for registration for new users and are considered by cybercriminals to be more secure exchange platforms.

The FraudAction Intelligence team coordinates and triangulates data with other RSA systems, such as the RSA eFraudNetwork®, VBV/MCSC registrations and transactions, and the Anti-Fraud Command Center data repository. This team also collaborates with law enforcement agencies worldwide.

RSA CyberCrime Intelligence

Trojan log files regularly reveal a wide range of information across a number of organizations that can potentially jeopardize the confidentiality of their intellectual property, expose network security to malicious intrusions, and put other high-value assets at risk. Malware is prolific on corporate machines, and when undetected, has the capability of collecting a myriad of credentials that enable access to internal applications like email accounts and CRM resources, as well as an organization's VPN.

RSA has witnessed a sharp increase in the number of posts in the underground advertising for sale this exact type of compromised data to other cybercriminals. Given the rapid evolution of the cybercriminal underground, organizations should be wary of the potential risks posed to sensitive business data, and be prepared to adjust existing policies and controls, or create new ones, in order to mitigate their exposure.

To identify corporate data that may have been compromised due to malware infections and enable an organization to take remedial action, RSA CyberCrime Intelligence agents retrieve raw Trojan logs from criminally-operated, automated caches. Their work is based on collaboration with other RSA research teams; FraudAction Research Labs works to obtain Trojans logs and an R&D staff develops tools for parsing (decrypting) the raw data, and a specialized system aggregates it, enabling the issuing of customer-specific queries.

After retrieving a query, RSA CyberCrime Intelligence agents thoroughly review the raw data for actionable information. The team scours through decrypted data to identify Trojan communication points that may require blocking from within the organization. Sensitive corporate access credentials are aggregated and reported, as well as leaked email correspondence, and other exfiltrated data. Similarly, employees' personally-identifiable information, IP addresses, and payment information are also extracted and shared, facilitating timely action by the organization to prevent further risk.

Pursuant to analysis, recovered information is provided as three different data sets:

– Documentation of recovered communication, including emails

– Employee data. This includes a list of any data related to an organization's employees, including login credentials and email addresses.

– Resource data. This includes a list of any recovered data related to an organization's resources, including the IP address of infected machines and compromised domains.

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.

AFCC SB 1211

www.rsa.com

RSA

EMC²