Service Data Sheet

RSA® CyberCrime Intelligence Service

At a Glance

— Gain insight on the machines, network resources, access credentials and business data that may have been compromised by malware

— Identify gaps in existing security policies and controls – and learn which ones are working succesfully

— Remediate incidents of potential data exposures, employee identity theft and infected corporate machines

— Educate employees about risky online behavior and the potential impact of malware infections

Organizations face multiple challenges in understanding and addressing the growing threat of malware. The use of remote access to corporate resources is growing and being extended to new users. New applications and services are being offered over the Internet. Employees' online behavior beyond the perimeter has become difficult to monitor – from the sites they visit and activities they perform to the programs they download on to their corporate-issued computer. These are only some of the changes that are creating knowledge gaps for security managers.

At the same time, cybercriminals are setting their sights on high-profile targets through sophisticated spear phishing campaigns with the intention of installing malware on corporate resources. Botnets are also becoming a concern for the enterprise and are of particular interest because they can be used to propagate malware to other systems on the network.

RSA®
The Security Division of EMC

As malware is becoming harder to detect, security professionals need to understand the risks they face and the proper policies to maintain in order to mitigate the impact to their organization.

Service Description

The RSA® CyberCrime Intelligence Service provides information on corporate machines, network resources, access credentials, business data and email correspondence that may have been compromised by malware.

The RSA CyberCrime Intelligence Service delivers insight in a variety of forms including:

– **Raw data relevant to the organization**, recovered directly from malware log files. This includes a feed of all recovered Trojan log files.

– **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.

The RSA CyberCrime Intelligence Service helps security professionals gain the information they need to:

– Educate and inform security executives of the potential risks posed by malware

– Identify gaps in existing security policies and controls as well as insight into the policies and controls which are performing successfully

– Identify and assess corporate resources and data at risk of exposure to malware

– Remediate incidents of potential data exposures, employee identity theft and infected corporate machines

The CyberCrime Intelligence Service Enhances Data Security

The RSA CyberCrime Intelligence Service helps security professionals to identify the gaps in existing processes and adjust or create new controls and policies within their infrastructure to prevent data loss.

For example, organizations using a security information and event management (SIEM) solution such as RSA enVision® platform can adjust their policies and rules to monitor for unusual activity. To demonstrate, consider dozens of employees have been identified to be infected with malware. With the RSA enVision platform, a watch list can be created for infected employees to monitor for unusual authentication or access control issues such as access attempts to unauthorized systems. If unusual activity is detected, enVision event management will automatically send an alert to a security analyst for investigation and remediation.

The RSA CyberCrime Intelligence Service can also be used to adjust data policies and controls. Organizations using a data loss prevention solution such as the RSA® Data Loss Prevention Suite might use the information to evaluate existing data security practices and apply new policies. For example, a new policy might be created that prevents files containing specific types of data such as credit card numbers or U.S. Social Security numbers to be emailed outside the network unless the data is encrypted.

About RSA

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.

Corporate Data Captured by Trojans

The distribution of malware has extended well beyond the financial market and is increasingly affecting industries such as healthcare, government, insurance, telecommunications and education, just to name a few.

The types of information being captured in Trojan log files can be detrimental to businesses. For example, a myriad of VPN credentials that enable access to corporate applications like webmail accounts and CRM resources are being collected. As a result, organizations are put at higher risk for data loss.

Other data such as intellectual property, sensitive financial data and business plans, healthcare records, marketing research and corporate bank account details are also being captured.

Cybercriminals are just beginning to understand the value of the non-financial data collected through Trojan infections. RSA has witnessed a sharp increase in the number of posts in the underground attempting to sell this data to other criminals. Given the rapid evolution of the criminal underground, organizations should be aware of the potential risks to sensitive business data and be prepared to adjust existing policies and controls or create new ones in order to mitigate future threats.

RSA®
The Security Division of EMC

www.rsa.com

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

CYBERC DS 0140