RSA White Paper

Malware and the Enterprise

Understanding the Potential Impact of a Trojan Infection

The rise of malware in the enterprise creates many challenges and risks to security professionals. Trojans, in particular Zeus/Zbot, Limbo, Torpig/Mebroot/Sinowal and SilentBanker, are silently capturing a wide variety of data and credentials from online users, including critical business information. As the distribution of malware has been seemingly targeted at online consumers, many organizations lack awareness of the potential risks posed by corporate-infected resources. Organizations must understand to what degree malware has begun to compromise enterprise-related information so that policies and controls can be adjusted accordingly to prevent data loss.

RSA®

The Security Division of EMC

Contents

The division between the consumer and the enterprise is slowly disappearing. Consumers are also employees, and employees conduct personal business and check personal email accounts from corporate workstations.

The Line between Consumer and Enterprise Disappears

The evolution of malware is well-documented by the anti-virus industry and security researchers. Regular reports and blogs have been published, including by the RSA FraudAction Research Lab, that highlight the latest threats and newest features and functionality being created by malware developers. In addition, the increasing use of social networking sites to proliferate malware has made it a "top of mind" threat for most online users. In a recent global consumer survey[1], more than 80 percent of consumers expressed awareness of Trojans.

Malware, however, has long remained viewed as a consumer-oriented issue and a problem to be solved by financial institutions looking to preserve customer confidence and reduce fraud losses. This position is logical given the history of malware and its traditional existence to be used to steal online banking credentials (both retail and commercial), credit card information and other data such as usernames and passwords to popular consumer-oriented online portals. Even today, cyber criminals are primarily using Trojans to capture this information for the purpose of committing fraud and identity theft.

The division between the consumer and the enterprise is slowly disappearing. Consumers are also employees, and employees conduct personal business and check personal email accounts from corporate workstations. Similarly, as organizations make access available to a wider array of resources over the Web via technologies such as SSL VPNs, the variety of computers touching the corporate network expands to include personal machines such as the family computer.

The dual use of computers for personal and business purposes opens the door for Trojan infections on corporate-issued endpoints and the opportunity for cyber criminals to capture additional data such as VPN credentials that enable access to corporate applications like webmail accounts and CRM resources. As a result, organizations are facing an increased risk of data loss.

Little attention has been focused on the crossover impact and potential risks malware could pose to the enterprise. As organizations, particularly larger ones, have advanced Security Operations programs with clearly defined policies and multiple technologies in place to protect both networks and end users, there is a sense of existing security measures are "good enough" to prevent against the threat of Trojans. However, the rapid evolution of malware has created possible gaps with the current security controls and policies designed to protect corporate resources and monitor employee behavior.

Risk Outpaces Controls

The traditional view of malware is that a Trojan is still largely delivered as a visible file, often found in email attachments. While still used to some degree today, there are extensive response strategies in place to address this view, ranging from mail filtering products to security policies for attachment delivery. Yet the effectiveness of enterprise controls that are designed to filter out potential threats before they even reach the endpoint are questionable. For example, in October 2009, researchers conducted a study[2] that sent a spoofed LinkedIn invitation email that appeared to come "on behalf of Bill Gates" to users in different organizations. The fake message evaded major email security products and controls at the organizations tested 100 percent of the time.

Malware infection is not just limited to propagation through spam. Cyber criminals have developed a response strategy, elevating the popularity of the drive-by download method[3]. The sites known as the "usual suspects" – pornography, gambling and pharmaceuticals – remain the most likely avenues for infection. However, fraudsters have invested considerable effort in exploiting legitimate sites (usually via advertising) including popular news sites, social networks and celebrity fan pages to increase the volume of infection.

The next line of defense to prevent infections through methods such as drive-by downloads is an updated anti-virus application. However, their ability to prevent infection is even being called into question as malware itself is becoming harder to detect. Several studies have been conducted to determine the ability of anti-virus programs in detecting Trojans and other malware variants. One study, for example, found that up-to-date anti-virus applications only detected the Zeus Trojan 23 percent of the time[4].

[1] RSA 2010 Global Online Consumer Security Survey

[2] "Major Secure Email Products And Services Miss Spear-Phishing Attack," *Dark Reading*, October 2009

[3] A program that is automatically downloaded to a user's consent without their consent or knowledge. The download can occur by simply visiting a website.

[4] *Trusteer*

As the ease of infection rises and front-line defenses become less effective, malware creates additional risks for Security Operations to be concerned with providing the nature of employee browsing behavior. The reality for security managers (particularly for organizations that issue laptops to employees) is they have little visibility into the online activities conducted by their employees when they are disconnected from the network. The level of risk increases significantly for organizations which allow anytime, anywhere network access – and even more when partners and other third parties are granted access privileges.

This conversation resonates among CISOs and security managers. What has been missing is an evaluation of the challenges posed by malware and a quantification of the risk.

Quantifying Malware Risk

As a by-product of its RSA FraudAction Anti-Trojan services, RSA has visibility into a significant volume of data captured by malware, including previously mentioned variants such as Zeus, Sinowal, Limbo and SilentBanker. In an effort to quantify the risk malware poses to the enterprise, RSA analyzed a segment of data under the conditions shown in the table below.

Search Profile	U.S. Fortune 500 ["F500"] for 2009[5] domains (e.g., emc.com)
Search Profile Qualifiers	– Only one domain per company (e.g., only emc.com and not rsa.com or vmware.com) – <20 well-known consumer-focused brands excluded due to sheer volume of data
Timeframe	– One calendar month, late 2009[6]
Data Set	– Zeus version 2
Items of Interest	– Email addresses using the domain in question (e.g., employee.name@emc.com) – Records of compromised PCs ("bots") accessing domain (e.g., proof that infected machine visited something under the emc.com domain)

Upon completion of the analysis, results were then organized by their respective company, and then ordered in descending order by the number of employees of each organization[7].

NOTE: *RSA regards this pool of data as rather shallow. A timeframe of one month creates obvious limitations on the amount of data available for the study, while only searching for one domain per company narrows the search considerably given the nature of companies in the Fortune 500.*

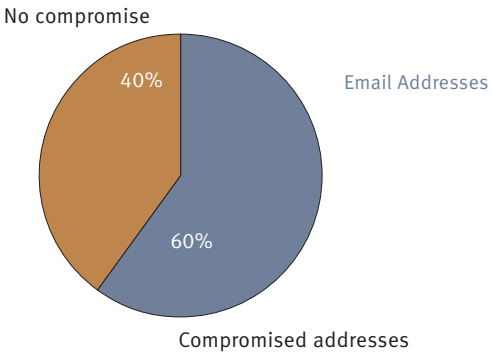
The reality for security managers is that they have little visibility into online activities conducted by employees when disconnected from the network

[5] http://money.cnn.com/magazines/fortune/fortune500/2009/full_list/
[6] 31 days; month not specified in interest of preserving anonymity of data
[7] Employee counts referenced from Hoover's Inc., a D&B Company (www.hoovers.com)

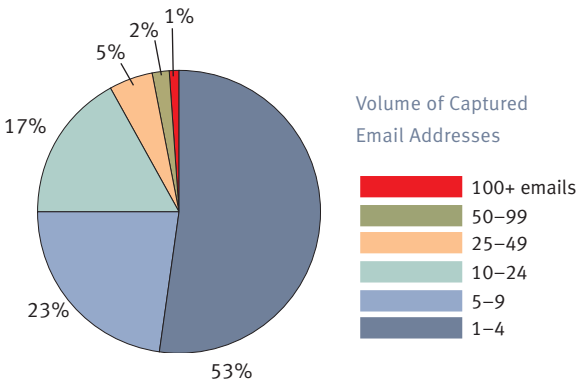
Results

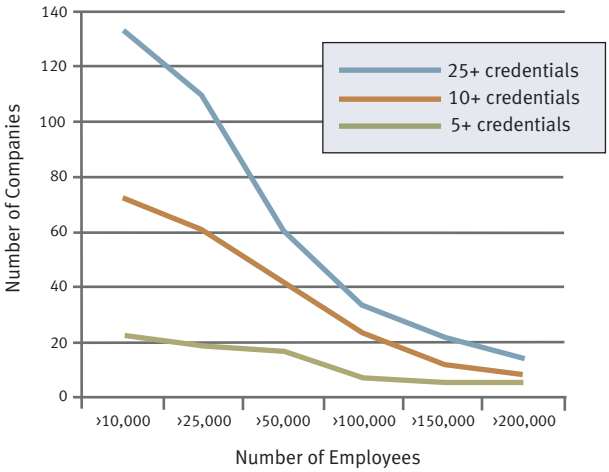
Email Addresses

RSA's analysis demonstrated that compromised email addresses representing 60% of the F500 (email addresses from 299 companies) were identified in the pool of data.



Of the companies that had email addresses captured by malware, 47% had five or more email addresses captured and 8% had 25 or more email addresses captured.



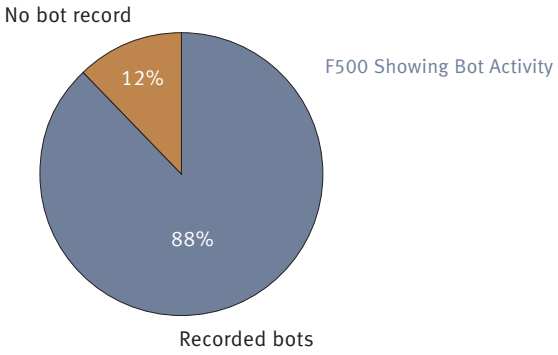


Companies with less than 75,000 employees appeared to have the highest ratio of compromised email addresses to employee counts. For example, in the chart below, more than 40 companies with employee counts in excess of 50,000 had ten or more email addresses captured by malware.

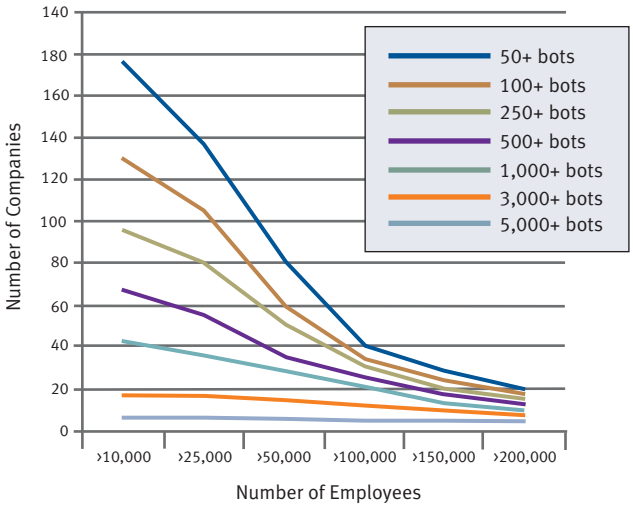
Botnet activity was connected to 88% of the U.S. Fortune 500 domains. In other words, domains individually representing 88% of the Fortune 500 were shown to have been accessed to some extent by computers infected by the Zeus Trojan.

Botnets

RSA's research demonstrated botnet activity connected to 88% of the U.S. F500 domains. In other words, domains individually representing 88% of the F500 were shown to have been accessed to some extent by computers infected by the Zeus Trojan.



Again, companies with less than 75,000 employees appear to have the highest ratio of botnet activity to the number of employees. For example, more than 60 companies with employee counts in excess of 50,000 had evidence of 100 or more unique connections from machines infected by malware.



Analysis

Based on the results of the data we analyzed, it is clear that there are a high number of corporate machines being used for work purposes that are infected with malware.

On the surface, this data does not necessarily infer a high-risk incident that requires immediate action. Evidence of a bot-infected machine connecting to a domain does not necessarily mean there is a Trojan operating in the background to siphon out corporate data. A corporate email address captured by a Trojan does not equate to compromised VPN login credentials.

Deeper consideration highlights that these small sets of data provide actionable intelligence. An email addresses would likely only be used by an employee for identification purposes which means a Security Manager can logically conclude the employee is working from a machine infected by malware. Similarly, evidence of botnet activity is likely associated with information such as an IP address which can be traced back to an infected machine. Such evidence provides security managers with the means necessary to research and remediate malware-related issues.

Malware Risk: The CISO's View

Information on compromised email addresses or evidence of botnet activity on the network is undeniably valuable. However, it is most critical for the CISO to understand the extent of the risk to the overall organization so that action can be taken to adjust existing policies and controls (or more importantly, establish ones not currently in place) to help mitigate future threats. This information is also enables CISOs to increase internal awareness and enhance their efforts to educate employees on corporate security policies.

It is most critical for the CISO to understand the extent of the risk to the organization so that action can be taken to adjust existing policies and controls (or, more importantly, establish ones not currently in place).

Conclusion

By analyzing just a small set of data, RSA has discovered a considerable volume of enterprise-related data being captured by malware. What cyber criminals can do or are doing with this information once it lands in their hands is still to be determined. Despite this, there is a demonstrated need for organizations to understand the level of risk and exposure they face from malware infections and to assess whether they have the appropriate technology, controls and procedures in place to mitigate future threats.

About RSA

RSA, the Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control; 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.

Intelligence has no value unless it is actionable. The results of RSA's study prompt CISOs and other security professionals to ask several important questions such as:

- How much do I know about my remote employees' activities?
- How can I be sure it is a legitimate employee performing the activities I am monitoring?
- How much insight do I have to what is flowing in and out of my network?
- What is the value of my data that is potentially being put at risk?
- What level of education is necessary to provide to my employees about online threats and the risk their activities pose to the organization?

These are just some of the questions that CISOs need to be asking as part of assessing their established policies and controls and to identify any gaps that may exist in their current infrastructure.

The Security Division of EMC

www.rsa.com

CYBER WP 0410