SUBMISSION NO. 66

SOPHOS

simply secure

INQUIRY INTO CYBER CRIME

SUBMISSION TO STANDING COMMITTEE ON COMMUNICATIONS: INQUIRY INTO CYBER CRIME

Sophos Pty Ltd
Level 11, One Elizabeth Plaza
North Sydney, NSW 2060.
Ph: 02 9409 9100
www.sophos.com.au

ABOUT SOPHOS

Sophos is a world leader in IT security and data protection. We offer organisations complete protection and control – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, policy abuse and data leakage, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. Our vision, commitment to research and development, and rigorous attention to quality have enabled us to maintain strong year-on-year growth and the highest levels of customer satisfaction in the industry.

SOPHOS SECURITY THREAT REPORT

Every six months, Sophos publishes its Security Threat Report by examining the threat landscape over the last six months, and predicting emerging cybercrime trends for the next six months.

It was reported in our latest report that in 2009, attacks have expanded. Even as the number of web-based malware attacks outweigh the attacks through email, financially motivated cybercriminals are turning their attention to Web 2.0 platforms such as Facebook and Twitter and alternative programs and tools such as Adobe Flash and PDFs.

Businesses adopting new technologies, and workers bringing software and devices into the workplace to facilitate communication and information-gathering, are giving hackers new opportunities for exploitation.

Sophos receives 40,000 unique suspicious files every day — accounting for 28 unique files every minute, 24 hours a day. Independent testing agency, AV-Test.org, currently counts over 22.5 million unique samples of malware in its collection — compared to 12.3 million in June 2008, demonstrating that the scale of the problem has almost doubled.

It's clear that the global criminal operation has reached such a level that it's a true "conveyor belt of crime." To defend against these attacks, businesses must strengthen defenses and get proper malware protection in place.

Today, most companies have guarded their email gateways and broadened their defenses against email-borne malware and malicious spam. Consequently, cybercriminals are developing techniques to infect machines behind-the-scenes by embedding malicious code on innocent websites and luring victims to them.

The Sophos Security Threat Report (July 2009 version) is available at:
http://www.sophos.com/security/topic/securitythreatreport-2009.html

PREAMBLE

Thank you for the opportunity to respond to this committee. The challenge of cybercrime is significant and the threat will continue to evolve. Increased consumer education, technical protection and worldwide legislative responses must therefore follow.

The huge range of detailed submissions to this committee highlights the challenges that face us – while there is no 'silver bullet', there are a range of actions that will assist. Three suggestions have been documented below; however, these by no means should be considered the complete answer. As Sir Winston Churchill once said, "this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning." There is much to do and this task will require not only perseverance and tenacity, but also collaborative action.

KEY RECOMMENDATIONS

Sophos considers that protection cyber crime would be enhanced by:

- Security built into the NBN
- Improved protection from phishing attacks
- Improved identification and neutralisation of Australian zombies and botnets

PROPOSAL 1: SECURITY BUILT INTO THE NBN

Background

The NBN will expose new internet users to cybercrime at faster speeds than most homes and businesses currently enjoy. It is important both practically and politically that a base level of security is built into early planning, rather than added in at a later date after problems are encountered. Consideration should be given to the establishment of a set of guiding security principles that are required of any organisation whose applications are run across the NBN. These principles should be broadly based and not prescriptive in defining how security should be achieved, as the internet applications (and future cybercriminal attacks) will continue to evolve.

Overview

As an example of a potential security-focused application that could be developed for the NBN, there exists a range of technical software components that could assess the security posture of a computer requesting to access the network. Based on the results of this assessment, preordained automatic actions could be undertaken, that will ensure a higher level of security, for that session. A slightly more detailed description is offered below.

Components

A. NAC (Network Access Control) – the assessment tool

There are three elements of the security posture that need to be considered and assessed with NAC (Network Access Control) like functionality.

1. Is there an active and up-to-date anti-malware solution?
2. Is the operating system patched to a suitable level?
3. Is there a firewall present and turned on?

» (A more complex extra question is what applications are installed and are these correctly patched? – consider this a potential stage two)

B. Anti-malware – the protection tool

» Anti-virus
» Anti-spyware
» Host Intrusion Protection Software (HIPS)
» Application control (minimise the number of applications)
» Buffer Overflow Prevention System (BOPS)

Process and function

On logging into the network, the NAC application is triggered and automatically downloaded. The NAC functionality then assesses the endpoint in regards to security (refer NAC above). Based on this endpoint posture, various actions are taken, for example:

» The endpoint is well protected so a session can commence.
» The firewall is found to be turned off and is activated.
» The anti-malware is found to be out-of-date so new updates are downloaded.

If the security posture of the machine is unacceptable or remains unknown, it would be assumed to be insecure and anti-malware software would be required to be installed, prior to a session being instigated.

PROPOSAL 2: IMPROVED PROTECTION FROM PHISHING ATTACKS

Background

Sophos (and our industry competitors) are conducting an 'arms race' with the writers of bank phishing scams. For example, a number of recent phishing campaigns targeting Australian banks have used malware that has drastically morphed in each individual campaign, making the malware more difficult to detect generically.

Overview

Companies that provide scanning and blocking solutions that protect end-users from phishing use a range of techniques, combining two main functions:

- Assess the reputation of the sending IP address.
- Examine the message to detect phishing emails.

Additional protection could be achieved using an allow-listing ('whitelisting') approach.

If whitelisting was implemented, email filtering software could then aggressively block anything purporting to be from an Australian bank that does not originate from that specific bank's IP range. To do this, we need to be sure that all IP addresses for all bank mail servers are known. This must include the IP addresses for any third party servers who might send mail on the bank's behalf.

Request - Proposal

If a list of the IP ranges and domain names for all legitimate sites was made available for all Australian banks use, to enable more accurate detection against future attacks. It is proposed that this data would be centrally consolidated and all (approved by APCA or another organisation that represents Australian banks) security companies would be able to access this information. In addition, it would be beneficial to know some detailed elements of legitimate bank correspondence.

Similar idea at an ISP level

This suggestion may sound similar to one involving provision of this same IP range data to an ISP. This arrangement between an ISP and a bank could help block phishes from reaching customers of that specific bank who use that specific ISP. Unfortunately, it will not assist customers of that specific bank who use a different ISP or customers of other banks who use that ISP. For this approach to work all banks would have to contact all ISPs. There is no problem with this occurring within ISPs, as the answer to cybercrime will have many components, though it is believed that this would only protect a subset of customers.

PROPOSAL 3: IDENTIFICATION AND NEUTRALISATION OF AUSTRALIAN ZOMBIES

Background

There are millions of computers around the world that have been compromised by cybercriminals and these now form part of large zombie networks or 'botnets'. Most of these seem to be computers at home or in small businesses, where there is often a lower level of security and technical awareness, and higher resistance to spending money on security software. So-called 'botmasters' have control over these computers, and can instruct them to carry about numerous cybercriminal activities, such as:

- Sending spam.
- Attacking other PCs to infect them in turn.
- Acting as anonymising proxies.
- Stealing data from the PC.

All these activities can take place without the owner of the computer being aware of this hijack. In 2005 ACMA initiated the Australian Internet Security Initiative (AISI) which is covered in detail in their submission - we are highly supportive of this initiative and believe with further support and publicity, headway will be made.

No data is available to show how many AISI reports actually result in clean-up. (Anecdotal information suggests that customers are often dismissive or defensive when contacted.) This would indicate that the problem needs end-user education, and may even require coercive powers.

Overview

As a majority of cybercriminal activity emanates from botnets, a reduction in the number of compromised computers worldwide will have a valuable impact. Unfortunately, the botnets in Australia are a small proportion of the botnets worldwide.

Because most major security vendors identify the IP numbers of many bots through traffic caught in their spam traps, they can use this to minimise spam by rejecting emails from known-bad senders. This filtering is referred to as *reputation filtering* and is built into most solutions together with other detection technologies. There is a high commercial value to security companies of this data so it would be unlikely that there would be open sharing between competitors.

Proposal

It is suggested that all interested security vendors (to be approved by ACMA or another government body) consider mechanisms to enhance the sharing of information on these botnets.

With suitable Federal legislation, with mandated remediation or suspension, with national education initiatives, and with appropriate resources within government and ISPs, it would be possible to place additional pressure on these hijacked computers to be cleaned up. If successful, this would reduce the number of Australian-based bots, benefitting internet users not just in Australia, but all over the world.

Although ACMA / AISI is already tackling this problem, with additional co-operation as described above, Australia could be seen to be leading the world in anti-botnet activity, and to encourage such a process to be rolled out as worldwide best practice.

CONCLUSION

Without the instigation of preventative measures, computer users will continue to face challenges in securing and controlling their environment, as criminals attempt to capitalise on new technology to make money and cause disruption. Developing and abiding by best practices can work to minimise the chance of future attacks. Sophos believes that with investment and commitment from all stakeholders concerned to provide education, technical protection and support towards the prompt adoption of worldwide legislation; the fight against cyber crime will prevail.

Sophos would like to again thank the Committee for the opportunity to provide this submission. For further information, please contact Rob Forsyth, Managing Director, Sophos, Asia Pacific.