

Malware and Cybercrime: Detection, Prevention and Impact of Malware

by Andy Wood, November 2011

Abstract

This paper explains about the technologies available to detect and prevent malware and the impact that malware has on an organisation. It further explores two of the latest technical advances in malware detection and prevention.

1. Introduction

Malicious code, known as malware, is one of the hottest topics in computer security for organisations today. There are millions of compromised web sites that launch drive-by download exploits against vulnerable hosts. Within seconds of connecting to them, victim machines become host to malicious software such as key loggers which record key strokes such as username and passwords, or credit card details and forward them to the cyber criminals. Other types of malware such as bot programs cause the victim to become a member of a larger collection of compromised systems that cyber criminals can control for illegal activities, such as denial of service attacks or large volume spamming – all without the victim being aware.

2. How can malware be detected

Malware can be detected through a number of technologies, the most common being through an anti-virus product which uses signature based detection. This method of detection has been in existence since the mid 80's and is capable of detecting simple forms of malware that are static or do not incorporate any form of stealth technique. Unfortunately the cyber criminals have evolved from this technique by incorporating many new technologies in to their malware, such as polymorphic and metamorphic code that causes the code to change. This has led to newer detection technologies such as heuristics which uses 'characteristics' or base patterning of malicious activity to determine if an activity is malware [1]. Recent advances in malware have resulted in technologies such as rootkits being used to hide the malware from the OS and subsequently the AV engine.

3. How can the impact of malware on an organisation be minimised?

It is impossible to completely remove malware threats to an organisation by technology alone. The software and hardware vendors are constantly in a 'catch up' situation, reacting to the advancement in malware technologies. To successfully address malware within an organisation it needs to be a multi-vector approach covering data governance, technology and user education.

3.1 Data Governance

By identifying and understanding what information within an organisation is critical, such as credit card information, corporate research and trade secrets, security efforts and investments can be better focused to ensure their protection [2].

3.2 Technology

There are a number of technologies available such as on and off premise filtering of eMail and web traffic; active and passive network intrusion devices monitoring malware on the wire, host based anti-virus and even host based intrusion detection and prevention (IDS/IPS) which monitors system API calls, memory buffers and the TCP/IP stack.

3.3 User Education

According to security experts Ed Skoudis and Lenny Zeltser

"More often than not, end users of our systems activate viruses simply because they don't know any better. You need to help them help you, and educate your users about the importance of protecting data". [3]

By training users on the threats that exist on the internet, via eMail and via social engineering (which can lead to a user visiting a compromised website), the user will be more informed about staying protected against malware threats and also aware on what to look out for and report back to their security team.

4. Host based technologies to prevent, detect and remove malware infection.

There are a number of technologies available to detect, prevent and remove malware infection; some have been mentioned previously in this paper. There are many new technologies being developed to improve or redefine the way we detect and prevent malware, but here I would like to address two different technologies, namely 'whitelisting' and 'beyond the OS' analysis.

4.1 Whitelisting

Previously a method of preventing certain applications or behaviours has been to add them to a blacklist, which the security tool (AV, IPS/IDS, FIM etc.) would then prevent from execution. However with the sheer volume of threats being developed globally on a daily basis, this task becomes insurmountable. Therefore, by reversing the idea to only allow those applications and behaviours you know are safe, malicious activity can be prevented from executing on the host [4].

4.2 Malware Analysis Beyond the OS

The latest developments by malware authors are to compromise or evade the host based security tools, and even the OS (i.e. rootkits). Advanced malware, such as the Agobot for example, contain malicious logic that can detect and remove more than 105 anti-virus processes [5][6]. This is achieved because the anti-virus product is installed and running within the very host the AV is monitoring.

So the obvious solution would be to monitor the host from the "outside", by creating the host within a "guest VM" of the physical host. There have been a number of technological developments with 'beyond the OS' malware analysis covering this methodology [6][7][8][9], and further enhancements on it, such as multiple engines at the hardware, host and guest levels. The engines will monitor host network traffic, processes, memory, files and of course each of the components of the AV solution to prevent compromise.

4.3 Removal of Malware

For signature based detections that capture the entire malware 'string', AV products can offer an option to clean the file, which will remove the signature content; or delete the file. For heuristic based detections it becomes more difficult as there is no defined string of code to remove.

5. Conclusion

Malware detection and prevention is going to be a problem for organisations for some time to come, and possibly will never truly be eliminated. However its risk and impact can be reduced within an organisation with a carefully planned end to end system of data governance, policy, technology and user education.

6. References

- [1] Heuristic Techniques in AV Solutions: An Overview - <http://www.symantec.com/connect/articles/heuristic-techniques-av-solutions-overview>
- [2] ComputerWorld UK - Malware: If you can't beat it <http://www.computerworlduk.com/advice/security/3289630/malware-if-you-cant-beat-it-learn-to-live-with-it/>
- [3] SKOUDIS, E. and ZELTSER, L. (2004) Malware: Fighting malicious code. New Jersey: Pearson Education, p.63
- [4] McAfee – Whitelisting paper - http://www.sans.org/reading_room/analysts_program/McAfee_09_App_Whitelisting.pdf
- [5] Agobot et al technical details - <http://www.stanford.edu/group/security/securecomputing/alerts/windows-phatbot-26mar2004.html>
- [6] Stealthy Malware Detection Through VMM-Based "Out-of-the-Box" Semantic View Reconstruction - <http://www.csc.ncsu.edu/faculty/jiang/pubs/CCS07.pdf>
- [7] Ether: Malware Analysis via Hardware Virtualization Extensions - http://ether.gtisc.gatech.edu/ether_ccs_2008.pdf
- [8] McAfee DeepSAFE - <http://www.mcafee.com/uk/solutions/mcafee-deepsafe.aspx>
- [9] McAfee Security Beyond the OS - <http://www.mcafee.com/us/resources/white-papers/wp-security-beyond-the-os.pdf>