Malware Risk Reduction: Best Practices

Nevis Networks

Persistent LAN Security Solutions

Executive Summary

Malware incidents have increased exponentially in recent years. According to a recent CSI/FBI study, malware outbreaks continue to represent the most costly security threats for enterprises today, despite the wide use of anti-virus software[1]. Additionally, attacks are targeted at smaller user groups with a financial motive. Increasing sophistication of the attack requires comprehensive detection and mitigation techniques. This is an in-depth perspective of the malware landscape and includes recommendations on best practices in security to reduce the impact of malware on enterprise LAN. It is intended for both business and technical readers who want to gain an overall understanding of malware, its causes and impact.

1 Malware Overview

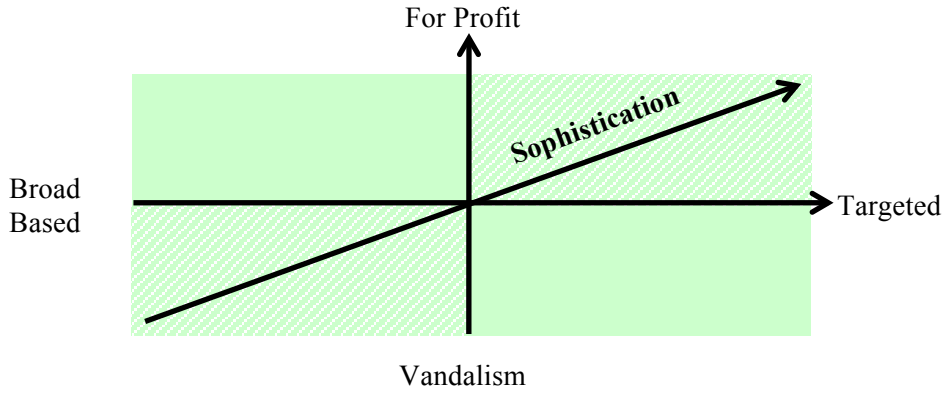
Malware is a generic term used for malicious software and consists of different categories including worms, Trojans, backdoors, rootkits and BOTnets. They all have common behavior, which includes installation without a user's consent with intent to attack the targeted host or surrounding network. Most malware programs exploit published vulnerabilities in commonly used applications. As bugs are unfortunately inevitable in the software, so is the malware. But patching the system with the latest updates is not adequate as some more sophisticated forms of malware may appear legitimate to the host operating system.

- **Worms and viruses**: Worms and viruses represent a common form of malware. Primarily intended to cause network disruption, these are sometimes used for commercial purposes such as "spammer viruses" like the Sobig and Mydoom viruses. The infected computers are used as proxies to send out spam messages.
- **Trojans and Rootkits**: As the name suggests, Trojans are programs that camouflage themselves as legitimate programs. This class of malware can perform activities such as collecting data and sending it to a cyber criminal, destroying or altering resident data with malicious intent, causing the computer to malfunction, or using a machine's capabilities for malicious purposes. Rootkits take this a step further by masking the malware from routine malware searches by security software. Rootkits can significantly prolong the lifespan of a malicious program resident within an infected system.
- **BOTnets**: BOTnet is a fairly new phenomenon which refers to a network of infected computers remotely controlled by a hacker. Using BOTnets, attackers can launch different types of attacks or engage in other types of malicious activity.
- **Spyware**: Spyware refers to other unwanted programs that install themselves on a user's computer. This includes keyloggers and adware which can monitor the infected host's and logged in user's behavior and report it back to the malware writer.

2 Trends in Malware

Malware incidents have increased exponentially in recent years. The effects of malware can range from mere annoyances to organized crimes causing serious losses. In such cases, malware can shut business down through a DoS attack or by a worm, which causes the targeted system to shutdown or via organized BOT attacks.

[1] 2006 CSI/FBI Computer Crime and Security Survey



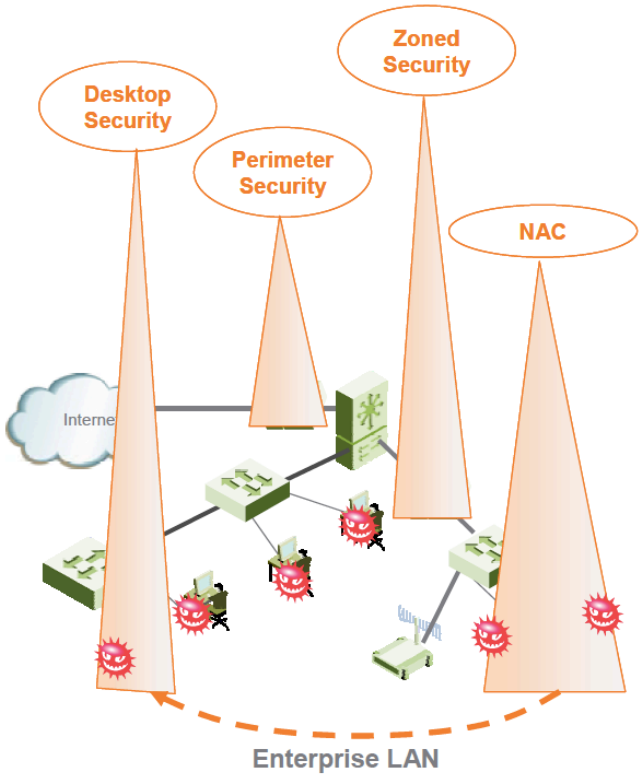
As the graph indicates, there is a shift of focus represented by the following trends:

- Malware for profit
- Targeted attacks
- Increasingly sophisticated blended threats

The financial motivation has contributed significantly to the increase in the spread of malware. Additionally, customized attack patterns represent a much more widespread, clever and insidious attacker profile. For example, malware that is targeted at a small group of Internet users and often leads to financial gain is becoming more popular than the mass mailing email worms of the last few years.

Earlier malware programs were written by script kiddies and were riddled with software bugs and as a result were not very successful. Today's for-profit virus writers are full-time employees who are experts in programming.

3 Today's LAN Security Solutions



Most enterprises use desktop security software such as Anti-virus and Anti-spyware to take care of email-borne worm attacks. For the perimeter, typically a firewall and IPS is deployed which is primarily intended to keep outside attackers out of the network.

To bring security closer to the user some companies have taken perimeter security devices such as Firewall and IPS and embedded them within the LAN. However, this solution is very expensive and difficult to manage.

NAC is looked upon as another layer of security but alone it acts simply as an extension of desktop security controls. It may perform a compliance check before the system is connected to the network; however, once the host gains network access, there is no inspection of the traffic for any possible threats.

These solutions have very limited visibility and are not scalable. Additionally, when deployed along with other solutions they become extremely complex and error prone. While perimeter and zoned security lack comprehensive user awareness, desktop security and NAC lack full network visibility – resulting in an incomplete architectural solution.

As a result, if a malware-based exploit results from a "briefcase bypass" where an employee takes a laptop home and gets infected with malware – this can easily propagate to other users in the network without being detected or prevented.

4 Best Practices for Risk Reduction

Best practices for reducing malware risks include the following:

- Checking the endpoint systems before they connect to the network
- Pre-authenticate the user before they are allowed access to the network
- Create enforceable access control policies such that user have specific access based on their role in the organization
- Early and accurate detection of an attack
- Effective containment of the attack
- Identification of the source of attack at user/MAC level
- Remediation of the affected resources
- Logging and detailed reporting for forensic analysis
- Deployable with minimal impact on network performance

5 Nevis Solution

Nevis provides a "Personal DMZ" solution purpose-built with high performance LAN security in mind that goes beyond the traditional NAC feature set. Nevis uses a combination of proactive and reactive security measures for effective detection and containment of malware.

- *Endpoint Integrity check* - the clientless endpoint security check ensures that an endpoint is compliant with the organization's security policy before it gains network access. A clientless approach eases administration and reduces maintenance and installation overhead. Since it is clientless, it is easy to deploy for guests and contractors as well as employees without additional administrative effort.
- *User Authentication* - User or guest authentication supporting multiple authentication mechanisms including 802.1x, Kerberos, and captive portal.
- *Access Control* - Fully user-aware, LANenforcer enforces identity-based access control policies to all authorized and guest users. This restricts network and resource access and prevents intellectual property data leakage risks.
- *Malware Detection* - LANenforcer offers inline packet inspection of traffic for any possible malware threats as well as network anomalies. Using a combination of different detection techniques such as signature matching, protocol anomaly, behavioral anomaly and traffic anomaly allows for proactive detection of known and unknown attacks – including zero-day exploits.

- *Effective containment* - LANenforcer supports highly granular, per-user policies and has the ability to quarantine or block the user based on suspicious activity or host configuration settings. By creating a Personal DMZ™, the containment domain is effectively reduced to a single user.
- *Remediation* – Authorized users and guests that do not meet the security policy are guided through remediation steps in order to gain network access.
- *Deployability* - Seamlessly integrating within a transparent mode, LANenforcer provides 10 Gbps security performance with all the security features enabled.
- *Reporting* - The management interface provides detailed reporting for forensic analysis and compliance mandates.

6 Summary

The rise of sophisticated malware incidents requires an advanced and comprehensive security strategy that can effectively detect and contain malware before it has a chance to spread beyond an individual user. Stopping threats at the front door via NAC is not adequate to assure complete threat detection within the LAN. Nevis' 'Personal DMZ' is the only comprehensive LAN security solution that can stop threats at the source.

About Nevis Networks

Nevis Networks provides innovative LAN security systems designed to help corporations protect information privacy and integrity, ensure network availability, and maintain regulatory compliance. Nevis LANenforcer product family integrates NAC with the deepest threat containment at wirespeed to create a "Personal DMZ" around every user on the LAN.

Nevis Networks
Sai Trinity Unit 6, 6th Floor East Wing,
Survey no 146/2/1A+2B/1
Pashan Circle, Pashan,
Pune 411021, INDIA
http://www.nevisnetworks.com