Information Security Brief

Mazu Profiler 7.0: Network Behavior Analysis Grows Up

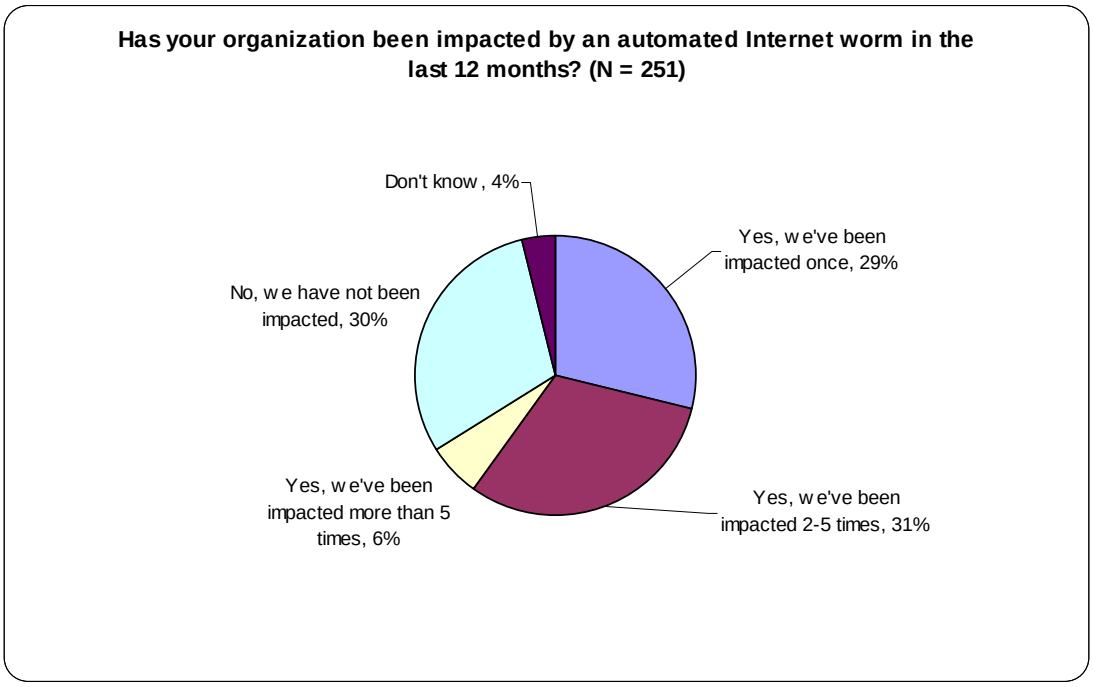
Date: September, 2006
Author: Jon Oltsik, Security Analyst

Abstract: Network Behavior Analysis (NBA) systems started to gain attention in response to the destructive worm storms of 2003, but this is old news today. What do NBAs do for an encore? They expand their coverage and functionality deeper into security, networking and applications to meet the demanding requirements of enterprise customers. This is exactly what Mazu Profiler 7.0 is designed to do.

Before 2003, network security was synonymous with perimeter security. If you could block intruders from penetrating the network, the risk associated with a security breach or network interruption was assumed to be quite low. This mindset made network security relatively easy. Install a perimeter firewall and IDS, write a few firewall rules and then monitor this infrastructure to deal with changing conditions and alerts.

Border-centric security strategies got a rude awakening in 2003, the year of the worm storm. By August, three major worm storms, SQL Slammer, MS Blaster and SoBig compromised systems, disrupted network traffic and caused billions of dollars in damage. Companies large and small suffered through multiple worm storms and their related impacts (see Figure One). Security and networking professionals scrambled to plug gaping network holes. Unfortunately, when they looked for help from security solutions they found a confusing array of point tools, in-line scanners, and immature management systems. This forced over-burdened CISOs to piece together solutions, re-configure networks and hope for the best.

Figure One: Worm storms were a Major Problem in 2004



The Dawn of Network Behavior Analysis (NBA)

Large organizations' network security woes were a blessing in disguise for NBA vendors like Mazu Networks of Cambridge, MA. For years, Mazu and others evangelized the benefits of their end-to-end network security solutions to myopic CISOs, only to be met by blank stares. The worm storms of 2003 suddenly made NBAs make a lot of sense. Security executives recognized the value of NBA systems. Why? Unlike existing security tools, NBAs:

- **Monitor traffic across the network.** Most companies implement chatty IDS or expensive IPS devices on a few network segments, but the worm storm attacks demonstrated that this kind of isolated security left most of the network invisible and unprotected. NBA systems capture and analyze network flows, making it easier and more economical to monitor and secure the entire enterprise network.

- **Baseline the network based upon behavior and history.** Unlike signature-based devices, NBA systems build statistical models based upon network behavior over time. Which clients and servers converse? What ports and protocols do they use? By capturing this data, NBA systems were designed to quickly identify network vulnerabilities or anomalous behavior. This was especially valuable for discovering rogue network nodes, such as wireless access points, or spotting suspicious traffic patterns like reverse tunneling.

- **Provide a wealth of actionable information.** Perhaps the biggest benefit of NBA systems was that they acted as a nexus for network behavior information. When a problem was suspected, the NBA provided a real-time picture of network traffic for analysis by security and network operations staff. This saved critical time in determining root cause, identifying all affected nodes and remediating any problems.

Savvy CISOs and network operations managers understood the NBA system benefits, which led to NBA market growth, more deals and wider implementations. Companies that initially implemented NBA systems on LAN segments expanded them across global networks. In a sea of tactical security tools, NBA became one of the few true enterprise security solutions.

Mazu Profiler 7.0: The NBA Market Matures

Enterprise penetration certainly carries the potential for sales activity and revenue growth, but it also comes with an engineering burden and commitment to constant product improvement. To succeed in the enterprise market, vendors must expand the scope of their original designs and continually improve their product scale, interoperability and functionality. Vendors whose products meet these challenges can become enterprise solutions leaders, while those that fall behind may quickly become ripe for replacement.

In the NBA market, Mazu Network appears to be making the transition from network security management to enterprise solution provider. To ESG, this progression is not a surprise. While Profiler was often purchased by the security team, network engineers and operations often realized the value of a product that monitored network behavior, traffic patterns and application flows and became Mazu fans themselves.

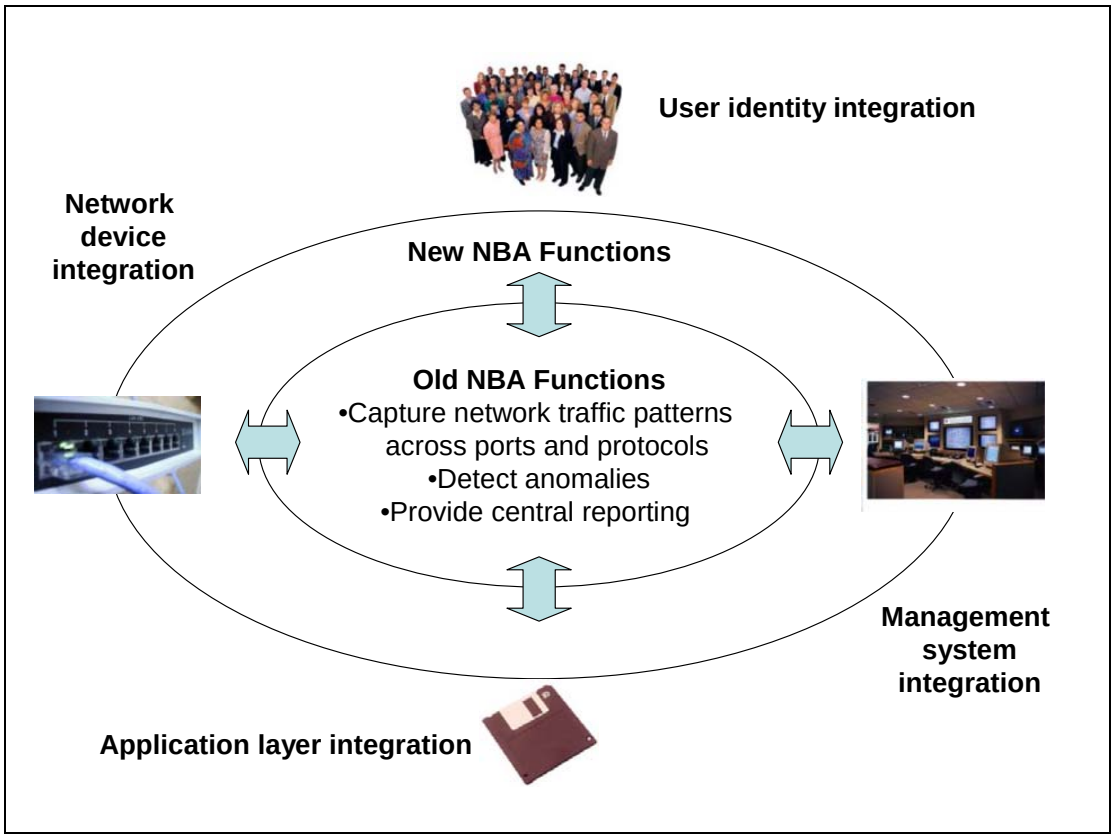
In September 2006, Mazu introduced the latest revision of its NBA system, Mazu Profiler 7.0. ESG believes that the enhancements in this release demonstrate a maturation of the NBA market, as they were obviously added in response to the Mazu enterprise installed base's requirements. Profiler 7.0 expands the NBA universe in three primary areas (see Figure Two):

1. **More visibility into applications and content.** Network security tools tend to focus on network layers 1-4 of the OSI stack, but hackers have figured out ways to circumvent network defenses by tunneling attacks and communications through open ports and protocols. Mazu Profiler 7.0 alleviates this risk by inspecting packet content all the way up to layer 7. With layer 7 knowledge, Mazu can detect web application attacks in real-time or inspect the content associated with tunneled "low and slow" reconnaissance.

2. **Increased visibility into network route paths.** Mazu has always had the ability to determine the IP addresses associated with host-to-host communications, but couldn't dig into details about network route paths. This left a little bit of guesswork when a compromised host suddenly began scanning the network. Profiler 7.0 can now see network route paths down to the device and interface level. When a chatty server is detected, Profiler can pinpoint the port it is connected to, so administrators can immediately disconnect the device, remove it from a VLAN or throttle traffic.

3. **Integration with user identity.** In the past, Profiler identified end-points by IP or MAC addresses; not user identities. Of course, IP addresses are dynamically allocated through DHCP, making the association between users and IP addresses tenuous at best. The new version of Profiler eliminates this shortcoming by integrating with Microsoft Active Directory. In this way, Mazu can capture the relationship between IP addresses and users and preserve this information for future audits or investigations.

Figure Two: The New NBA Universe



4. **Enhanced integration with other management tools.** Enterprises need management tools that share information with other management tools. Mazu Profiler 7.0 improves the better hooks into vulnerability management, Security Event Management (SEM) and Network Management Systems (NMS). As part of this improved integration, Mazu created an API that allows SEM and NMS platforms to access its treasure chest of rich contextual data. ESG believes that this integration effort is essential. When the network misbehaves, Mazu users can: 1) Aggregate events and information from SEM and NBA, 2) Provide network behavior information to the NOC and 3) Determine whether network nodes have been patched against specific types of attacks.

ESG believes that Mazu Profiler v7.0 can be seen as a microcosm of the security industry. In the past, the security infrastructure was composed of numerous independent point tools, but now large organizations want enterprise-class coverage and functionality from a few leading vendors. If it continues to innovate, execute and service its enterprise customers, Mazu may gain a permanent seat at the enterprise security table.

The Bottom Line

ESG believes that as NBA systems evolve, they will become an essential component of a new Network Security Architecture (NSA) (for more information, see the ESG White Paper, *The New Network Security Architecture* (NSA), June, 2006.

Mazu has been one of the leading NBA players for a number of years, sporting an impressive list of global customers. It is apparent that these firms like Mazu's product, but need it to do more. With Profiler 7.0, it appears that Mazu responded to its customers' needs. For years, Sun Microsystems' tag line was "the network is the computer," a prescient statement in 1982, but an obvious reality today. Now the network needs security protection across the enterprise as well as up and down the OSI stack. Mazu is one of a few vendors who seem to understand this.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Solution Centre
DATA: AVAILABLE – MANAGEABLE – SECURE

Solution Centre Limited
Vickers House
Priestley Road
Basingstoke, RG24 9NP.
Tel: 01256 818600
Fax: 01256 819600
E-Mail: sales@solutioncentre.co.uk
www.solutioncentre.co.uk