

Data Center Security in a World Without Perimeters

September 19, 2006

Dave McGinnis

Director of MSS Architecture

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™

- **Securing the Data Center**
 - What threats are we facing?
 - What are the risks?
- **Protection Strategies**
 - Tools & Systems
 - Finding a Solution
- **Questions and Discussion**

Securing the Data Center: The Threats

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™

What's it like out there?

- Almost all vulnerability research is done **underground**.
- Successful and powerful exploits have a long lifespan.
- Dangerous exploits can be released **immediately** after vulnerability disclosure.
- Electronic “evolution” and the hacker threat.
- Who's attacking us and **why?**
 - Amateur – joy riding
 - Skilled – curious, notoriety
 - Professional / Independent – monetary
 - Organized Crime Affiliate – monetary



The New Threat Landscape

- New threats no longer fit in neat buckets
- Classical definitions inadequate

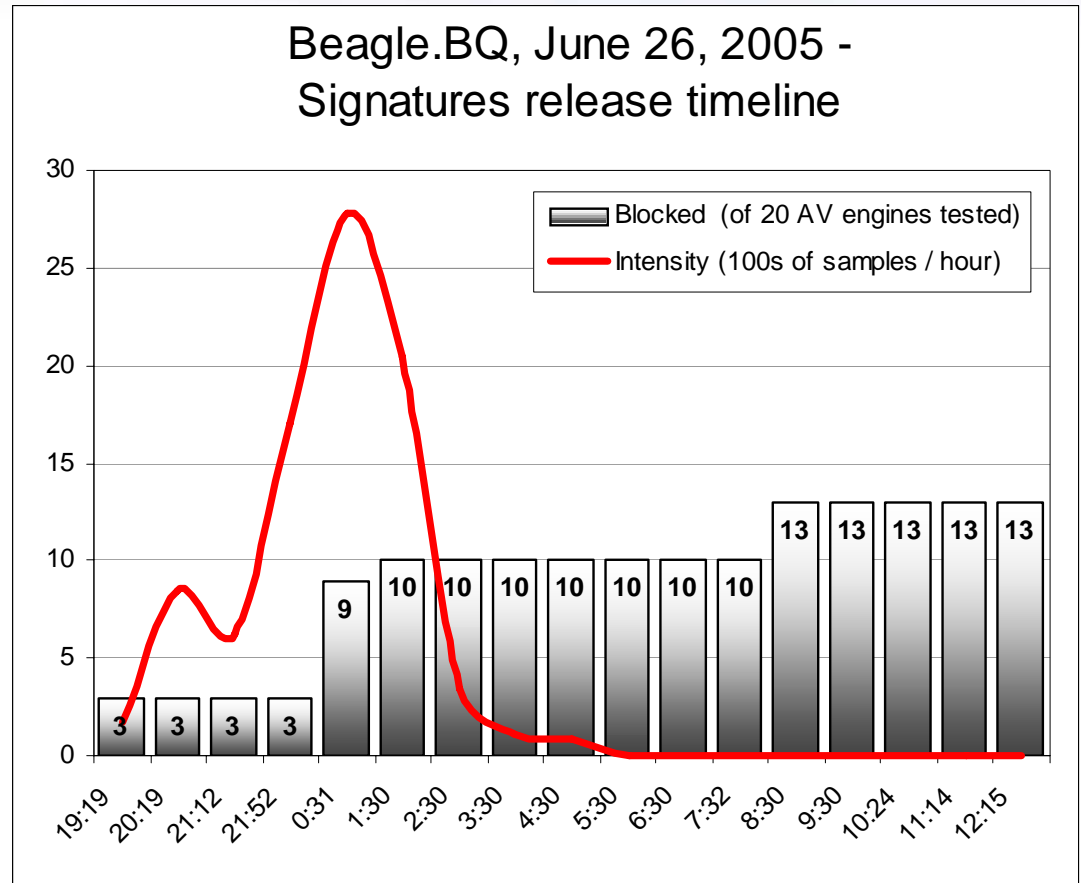
Virus	Keylogger	Worms
Screen Capture	Spyware	Malicious Macros
Trojan	Backdoor	Rootkit
Dialers	Botnet	Adware

- Blurring of divisions between the classic definitions
- Best or most successful distribution techniques now adopted by all “flavors”



Typical Attacks

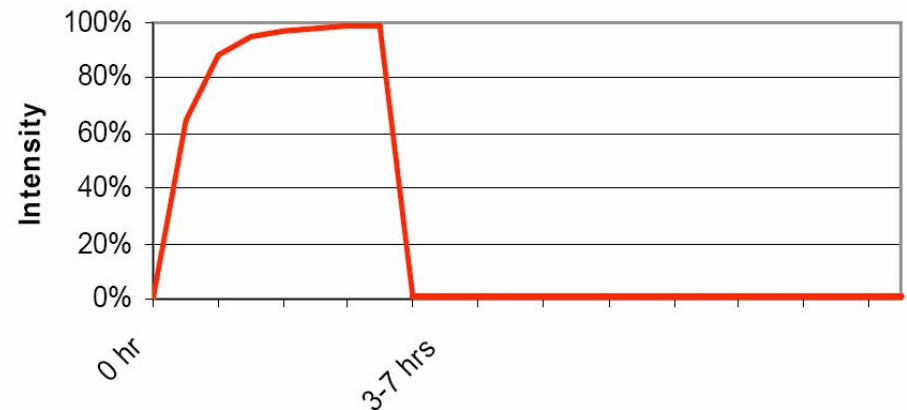
- Delay in developing signatures
- Takes time to harvest samples to manually investigate
- Average **10hrs** for signatures (AVTest.org)



Undiscovered Variants: Short-Span

- Short-Span attacks
- Combines distribution methods of spam with malware
- Designed to infect many computers before update is available
- Entire attack is completed in a few hours
- Protection available after the attack useless

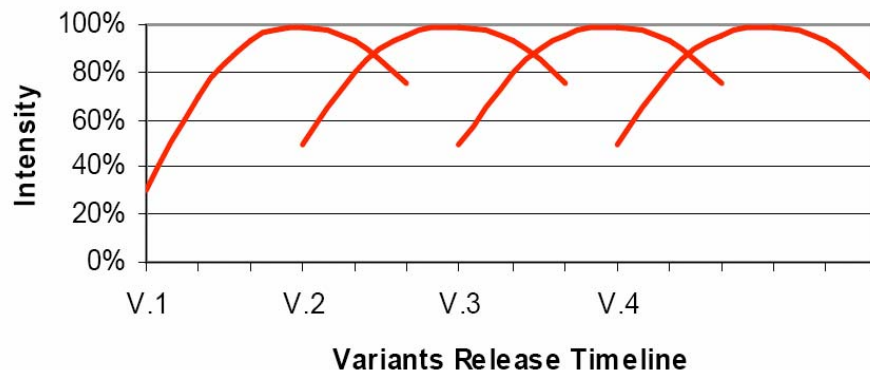
Figure 1b: Short-span attack



Undiscovered Variants: Serial Variants

- Serial Variant attacks
- Extends the window of possible infection
- Generates a number of minor variants and releases at closely spaced intervals
- Spam-based technique
 - Millions released in each wave
 - Broad and immediate impact with each variant
- Bagle-Mania on May 31st 2005 was an example of this

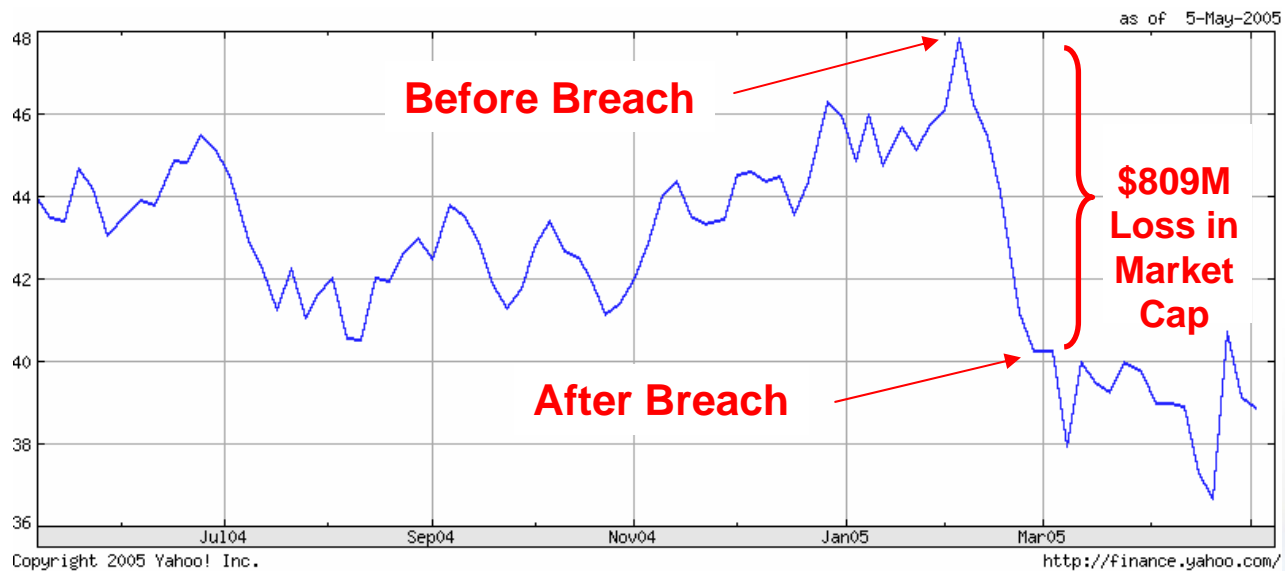
Figure 1c: Serial variants attack



Securing the Data Center: The Risks & Challenges

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™

Valuing "Reputational" Damage

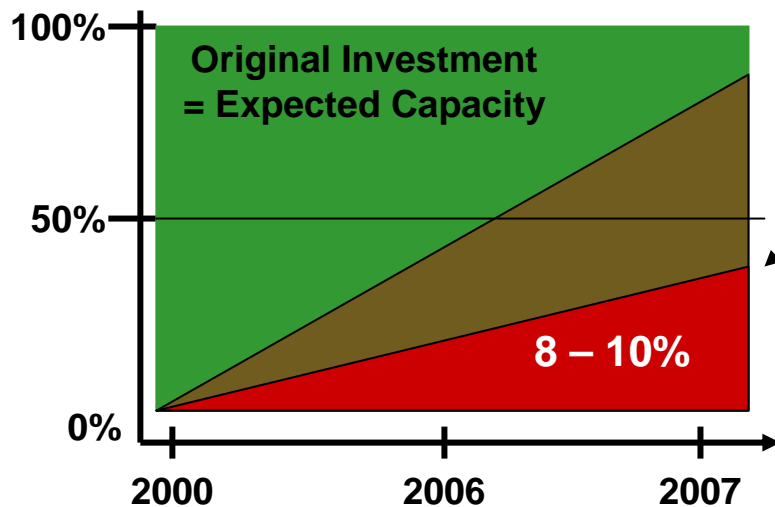


What's at Risk?

Network Resource Drain

“Worms have changed the equation. For many **carriers**, worms and viruses represent at least 30% of their traffic - - by 2006, such malicious traffic will represent more than 50% of all network traffic...”

Greg Young – Gartner / The Near Future of Network Security June 2005



The Measure for Internal Networks is Around 8-10%

What's Driving This?

BOTS - - Your Network is a Target Simply Because it is a Network!

Information Security Challenges

Management & Monitoring

Cost Intensive

- Requires 24x7x365 coverage
- A single seat requires 6 – 9 resources
- Requires multi-lingual workforce
- Requires sophisticated analysis tools to accurately identify threats
- Requires facilities and backend systems to manage

Requires Special Skills and Training

- Requires detection, analysis and resolution skill sets
- Requires investigative skills
- Requires emergency response capabilities for resolution
- Requires on-going training



Information Security Challenges

Operational Requirements

Security Intelligence

- Latest threat, viruses, behaviors
- Understanding of the latest attack methods and trends
- Security **Intelligence** and Advisories
- Discovery of security vulnerabilities – High Risk Advisories

Emergency Response

- Requires a plan, course of action for remediation
- Understanding of **how to respond**
- Losses from clean-up
- Comprehensive forensic capability and litigation support
- Security **best practices** to minimize damage & contain incidents



Securing the Data Center: Protection Strategies

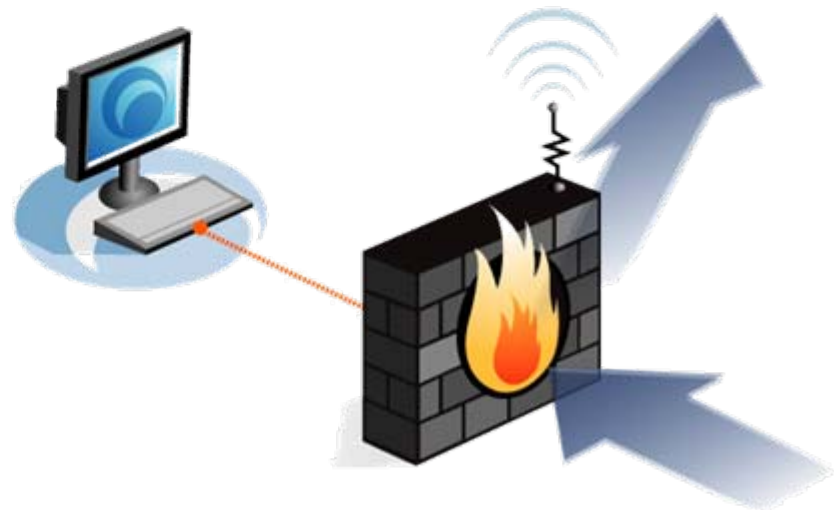
Tools & Services

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™

Firewalls



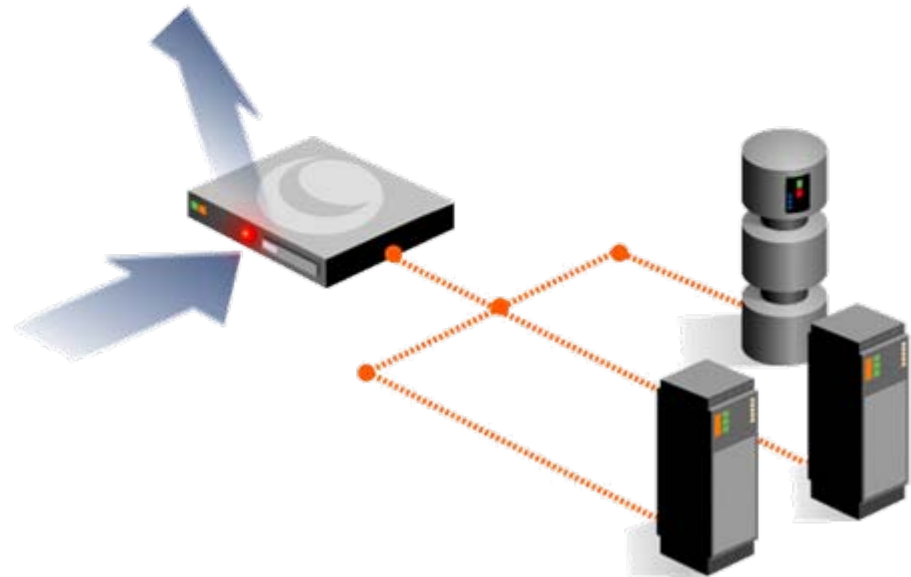
- What is it?: Access control point, VPN termination (site & client).
- Key Factor to Success: Policy change management.
- Little Known Fact: Varying size and flexibility of firewalls allows for more customized deployments.



Intrusion Prevention Systems



- What is it?: Inline protection device, typically deployed internally to protect against network threats.
- Key factors to success: What is detected? How it can be mitigated?
- Little known fact: IPS still requires 24x7 real-time monitoring.



Server/Host IPS



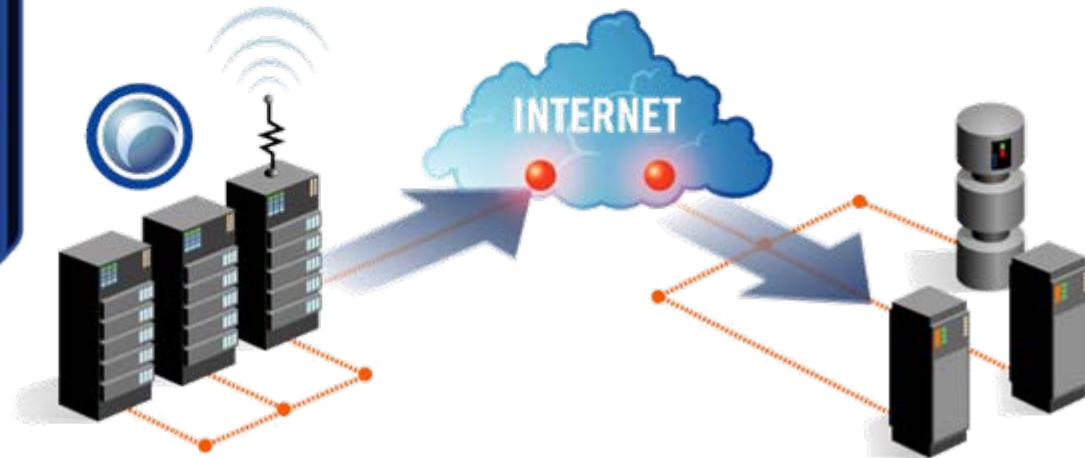
- What is it?: In-stack protection software against server/host threats.
- Key factors to success: What is detected? How it can be mitigated? What are the impacts to the server?
- Little known fact: Server/Host IPS provide the most customized level of protection for servers & hosts.



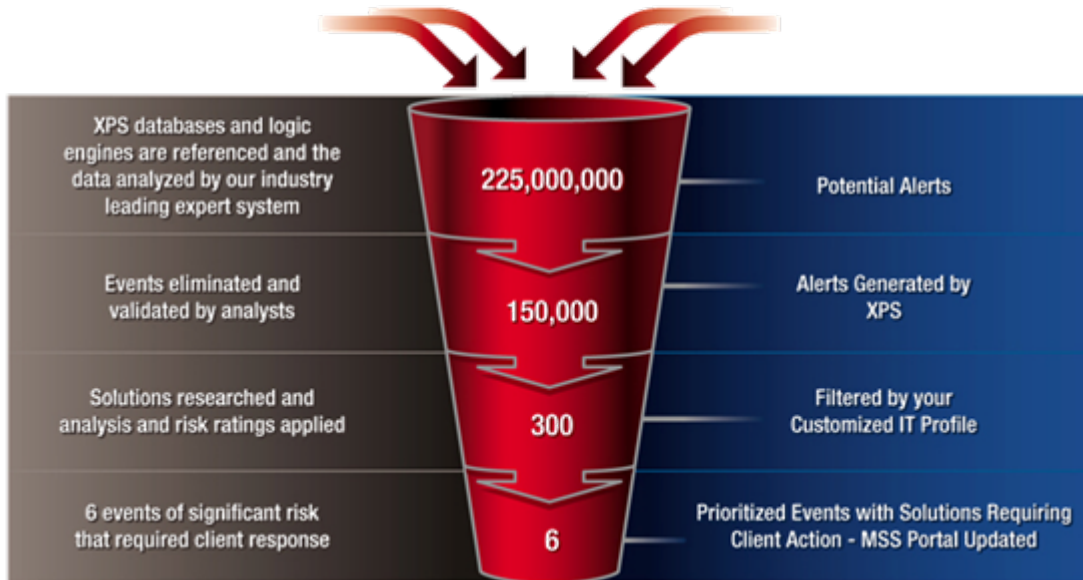
Vulnerability Management



- **What is it?:** A complete process for discovering and vulnerability remediation.
- **Key factors to success:** What is detected? How it can the threats be remediated?
- **Little known fact:** Most organizations know they have problems, but few actually solve the core issue.



Aggregation & Correlation Engines



- **What is it?:** Collection, aggregation, correlation and sound storage of security logs and events for monitoring, management and forensics.
- **Key factors to success:** How does it scale? How much additional infrastructure and cost is incurred?
- **Little known fact:** These systems have the capability to save or spoil the day.

Managed Security Services



- **What is it?:** Outsourced security monitoring and management.
- **Key factors to success:** How experienced is the provider? Can the MSSP solution scale (# devices, global reach)? Cost.
- **Little known fact:** MSSPs are not all the same. Buyers must perform due diligence prior to signing up.

Professional Security Services

- **What is it?:** Outsourced security consulting services such as penetration testing, policy and solution development.
- **Key factors to success:** How experienced is the provider? Cost.
- **Little known fact:** Professional consulting services are not limited to pre-solution work, they can be used in an ongoing fashion to ensure security posture maintenance.

Securing the Data Center: Protection Strategies

Finding a Solution

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™

Identifying a Solution

- ❑ **Assess the needs of the workforce.**
 - ❑ What applications will be hosted in the data center?
 - ❑ How will the users access the systems?
 - ❑ What data will be stored in the center?
- ❑ **Define security posture.**
 - ❑ Where on the risk spectrum is acceptable?
 - ❑ How much security is required?
 - ❑ Are there regulatory issues that need to be addressed?
 - ❑ How often is this posture to be reviewed?
- ❑ **Consider the tools and services available.**
 - ❑ Does the hosting center provide secure solutions?
 - ❑ Will your solution at the center be shared?
 - ❑ If so, what level of customization is allowed?

Designing a Solution

- ❑ **Determine operational capabilities.**
 - ❑ What is required of the operational team?
 - ❑ What internal resources will be dedicated to security?
 - ❑ Are there solutions available from the data center?
 - ❑ What other external parties can provide the solution?
- ❑ **Design the solution.**
 - ❑ Determine which tools meet requirements.
 - ❑ Decide on in-house or outsourced implementations.
 - ❑ Where do the experts fit? Find the balance.
 - ❑ Balance the ideal solution with costs.
- ❑ **Select tools & vendors.**
 - ❑ Utilize product and service trials/demos.
 - ❑ Visit service facilities. Meet your outsourced team.



Questions?

Thank you!

 **INTERNET|SECURITY|SYSTEMS®**
Ahead of the threat.™