The In's and Out's of Content Filtering

Dr. Eugene Schultz, CISSP, CISM
Chief Technology Officer
Emagined Security
Eugene.Schultz@emagined.com

Webinar
June 29, 2010

Introduction

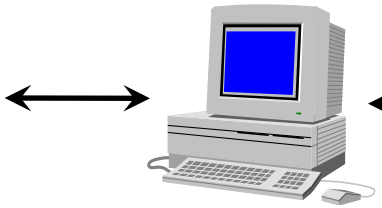
EMAGINED SECURITY

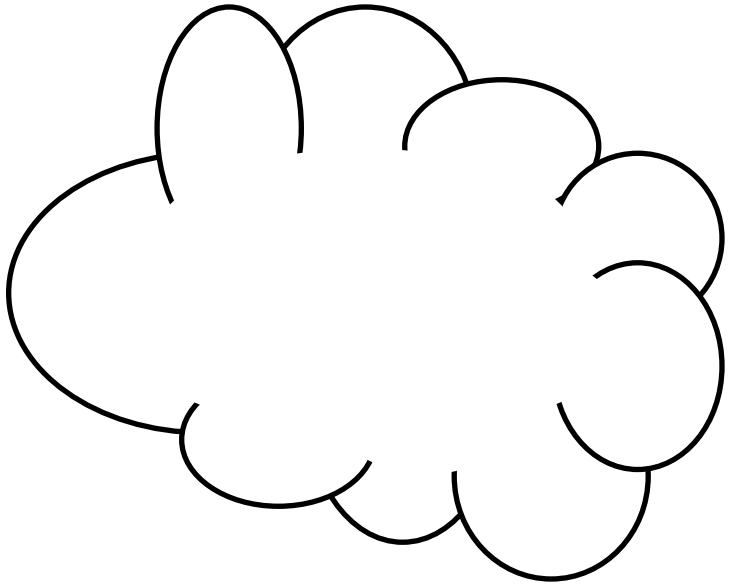
- *Content filtering* is a method by which content is blocked or allowed according to analysis of its content, rather than its source, type of protocol used to transmit the content, or some other criteria
  - Performed by applications at the gateway, desktop, and/or Internet that stop traffic in route and inspect it
  - Alert is sent whenever inappropriate content is detected
  - Most content filters also preserve content for inspection by security or other staff
- Can be unidirectional or bidirectional
- Two types of logic
  - Inclusive (most common)
  - Exclusive

Gateway-based content filtering

EMAGINED SECURITY

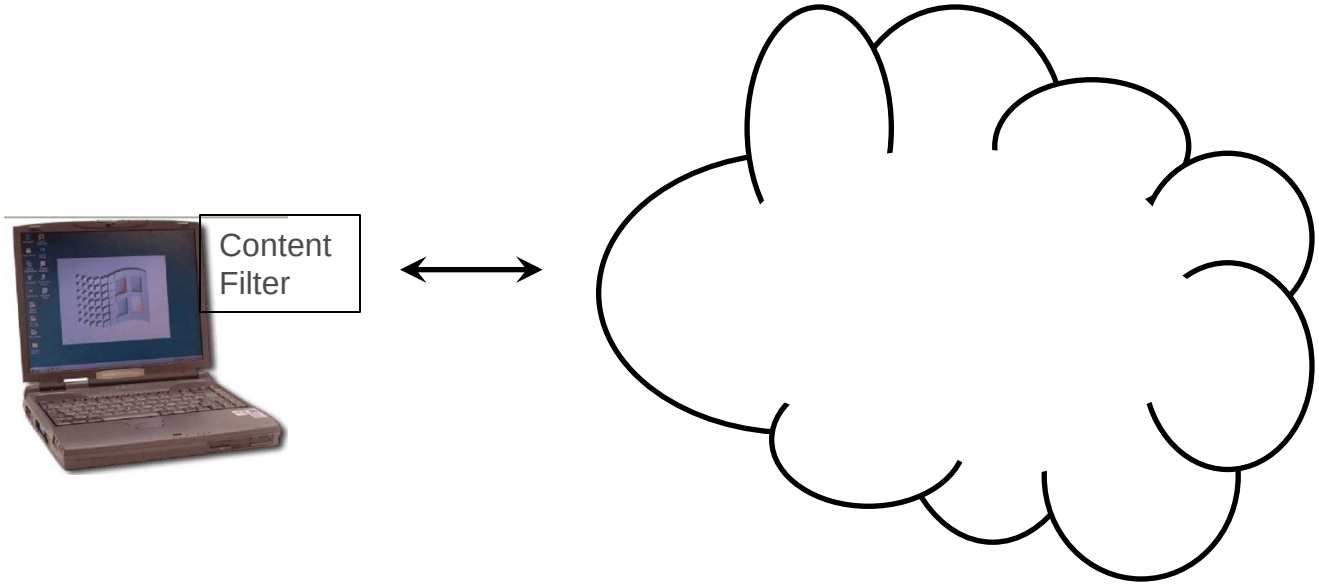
Enterprise Network





Host-based content filtering

EMAGINED SECURITY



Major purposes (1)

EMAGINED SECURITY

- Stopping employees and contractors from visiting inappropriate sites
- Preventing access to malicious Web sites
- Providing ability to enforce provisions of information policy and standards
- Providing ability to comply with external compliance standards (e.g., PCI-DSS)
- Preventing extrusion of sensitive/proprietary information
- Reducing “net loafing”
- Reducing TCO (when compared to manually monitoring content)

Major purposes (2)

EMAGINED SECURITY

- Reducing TCO (when compared to manually monitoring content)
- Reducing legal liability in numerous ways (see next slide)
- Others…

Content filtering and legal issues

EMAGINED SECURITY

- Lawsuits—an everyday occurrence in today's organizations
- Examples of content-related scenarios that lead to lawsuits
  - Employee downloads offensive Web content in the presence of other employees
  - Employee sends email containing sexually-explicit attachment
  - Employee leaks critical information that falls into the hands of competitor—stockholders find out and then sue
- Use of content filtering enterprise wide = exercise of due diligence, the best defense against lawsuits in which negligence is charged

Possible downsides

EMAGINED SECURITY

- Censorship
- Potential invasion of privacy
- No content monitoring tool is perfect
- Encrypted content may not be able to be analyzed
- Cost of content filtering product and maintenance
- Cost of monitoring operations
- Endpoint overloading

Radical changes on the attack front (1)

EMAGINED SECURITY

- Commonly occurring attack methods have changed substantially over the last five to ten years
  - “Frontal assault hacks” used to be common
  - With motivation for cyberattacks having changed so substantially, attack methods have changed accordingly
- Today’s attacks
  - Are much more subtle
  - Target applications (Web, Microsoft Office, Adobe Acrobat and Flash Player, and more)
  - Often involve sending many small pieces of content that must be reassembled by the destination host

Radical changes on the attack front (2)

EMAGINED SECURITY

- Today's more subtle attacks have substantially changed the nature of intrusion detection
  - Less reliance on conventional IDSs (and IPSs) per se
  - More reliance on very small indicators of attacks
  - More reliance on discovery methods that are more labor-intensive

Today's "hacks"

EMAGINED SECURITY

4K attachment containing exploit code sent with message

Attachment arrives with message

User opens attachment, which exploits Office vulnerability

Attachment causes browser to visit URL

Malicious web server injects exploit code

Exploit code exploits vulnerability to gain superuser-level access and install tty sniffer

Compromised host initiates connection to attacker's host

Attacker now gets all tty traffic and can remotely control compro-mised host

Today's "hacks"

EMAGINED SECURITY

Malicious web server injects specially crafted spyware

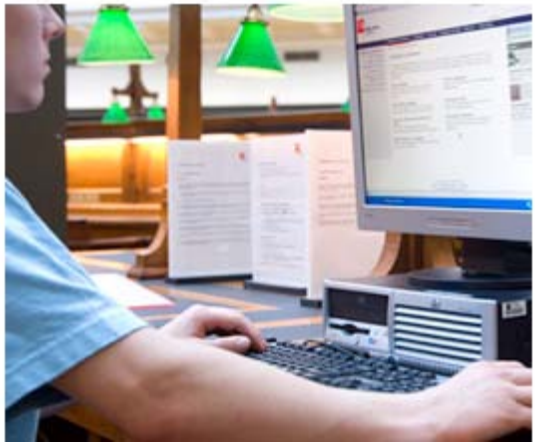
Connection is redirected to malicious Web site

Spyware waits for banking transactions, captures PINs and other data

User clicks on what appears to be a completely innocuous web link

Spyware makes encrypted connection to malicious web site with a variable IP address

Spyware sends encrypted banking data in a slow and gradual manner



Evasion of content filtering

EMAGINED SECURITY

- Many techniques for evading content filtering exist
  - IP address spoofing
  - Sending content through proxy servers
  - VPNs that use transport mode
  - Alternative encoding of content
  - Much more…
- A content filter must be aware of and defeat these techniques

The evolution of content filtering

EMAGINED SECURITY

- Content filtering has become increasingly sophisticated over the years
  - Started with simple string searches and blacklisting of certain source IP addresses
  - Some of today's content filters use extremely sophisticated logic (e.g., Baysian logic, grey listing, and more)
- Has become a major method of preventing extrusion of sensitive/proprietary data
  - Cost effectiveness compared to other methods is a particular advantage
- Reporting has become extremely flexible and sophisticated

Major requirements for a content filtering tool

EMAGINED SECURITY

- Easy installation and configuration
- Minimal performance impact
- Policy-based filtering
- Accuracy
  - High true positive rate
  - Low false alarm rate
- Management via central console
- Easy-to-use and highly informative reporting
- Preservation of and easy access to information regarding blocked content

Conclusion

EMAGINED SECURITY

- It is extremely important to thoroughly understand the pros and cons of content filtering from the standpoint of
  - Business
  - Information technology
  - Information security
- Failure to use content filtering will increasingly amount to lack of due diligence
- Be sure to carefully analyze content filtering products
  - Create a set of requirements for evaluating each product
  - Choose a product that evolves as ways to escape content filtering increase over time

Questions?

EMAGINED SECURITY

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: blog.emagined.com
Dashboard:
dashboard.emagined.com

For a PDF copy of these slides send email to:

seminar@emagined.com