Cisco.com

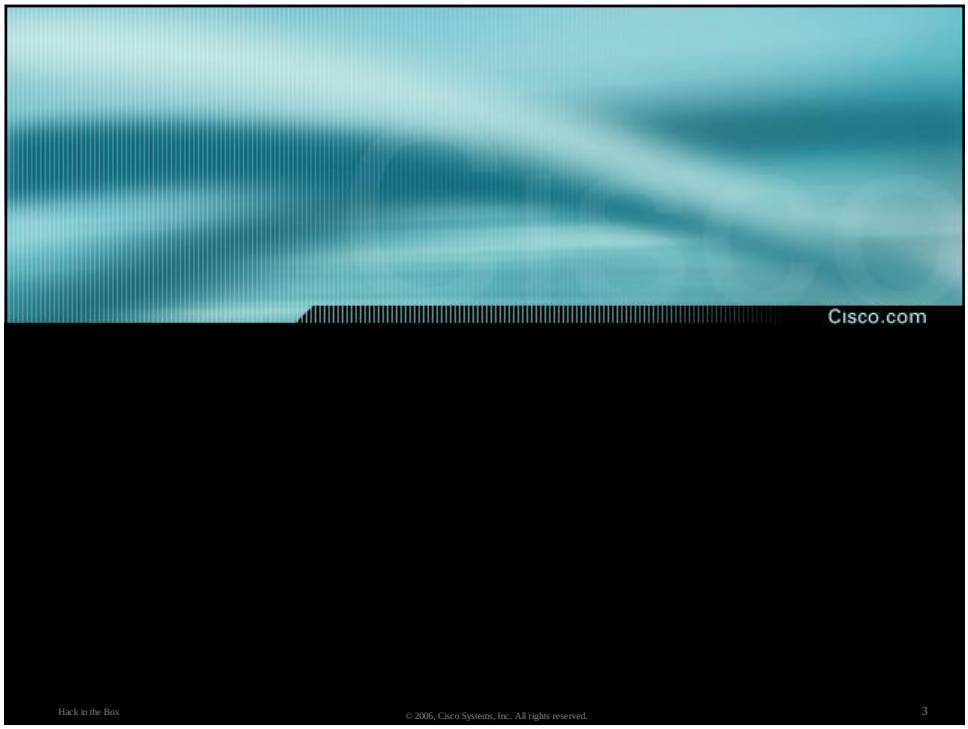
The world through the eyes of a signature developer

Jonathan Limbo <jlimbo@cisco.com>

Security Researcher

Cisco.com

- *The Security Climate*
- *The Evolution of Security Attacks*
- *Exploit Trends and Attack Vectors*
- *Trends in Obfuscation Techniques*
- *Challenges in Network Detection*
- *Next step in Mitigating These Evolving Threats*



Cisco.com

- *Increasing Activity*

  -167 Alerts (108 vulnerabilities, 12 malicious code alerts, 47 Security Issues)

- *Microsoft Office Routing Slip Buffer Overflow Vulnerability*

  - CVE-2006-0009

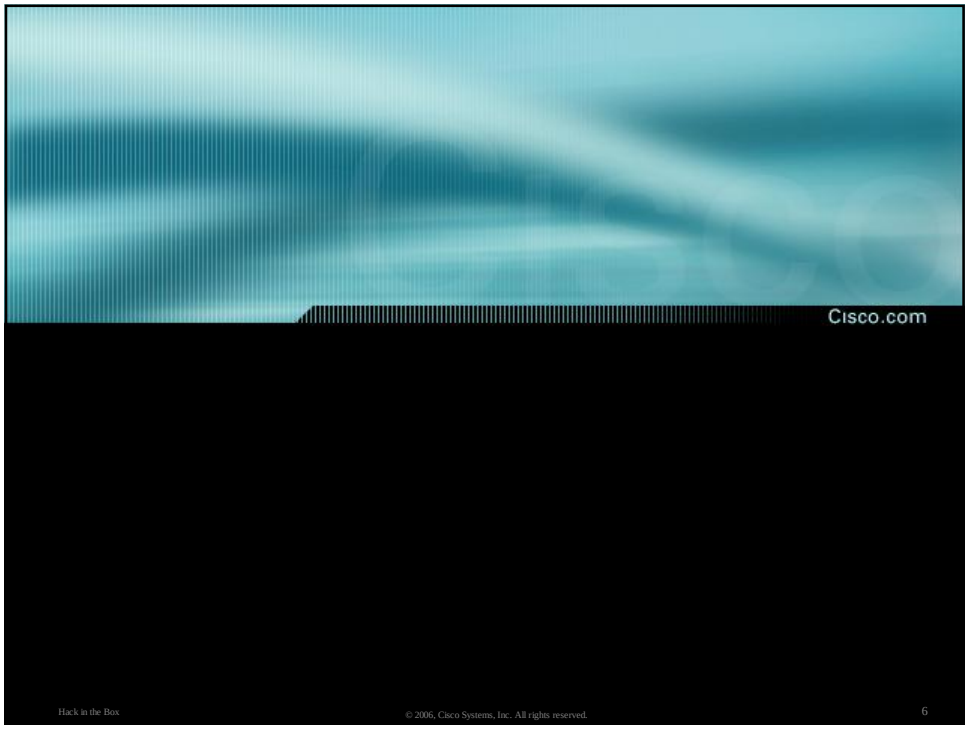
  - Reports indicate that exploit Attempts leveraging the MS06-012 routing slip buffer overflow vulnerability within Microsoft Office are occurring in the wild

(Data from Intellishield)

Cisco.com

- *IRCBot (W32.Wargbot or Mocbot MS06-040)*
  - *- CME-482, CME-762*
  - *- CVE-2006-3439*
  - *- Activity levels with the malicious code and variant remain low*
  - *- Continuing to identify localized outbreaks*
  - *- China reported that ADSL users are experiencing increased attack levels*

(Data from Intellishield)

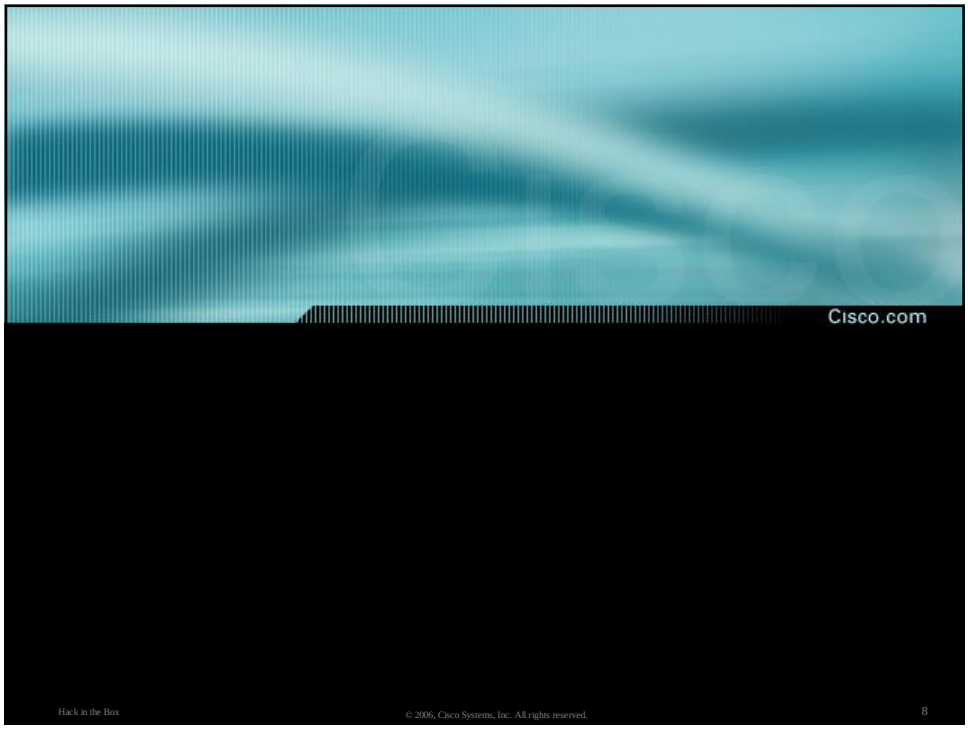


- *Carefully crafted attacks*

  - Complex
- *Growth of public exploits*

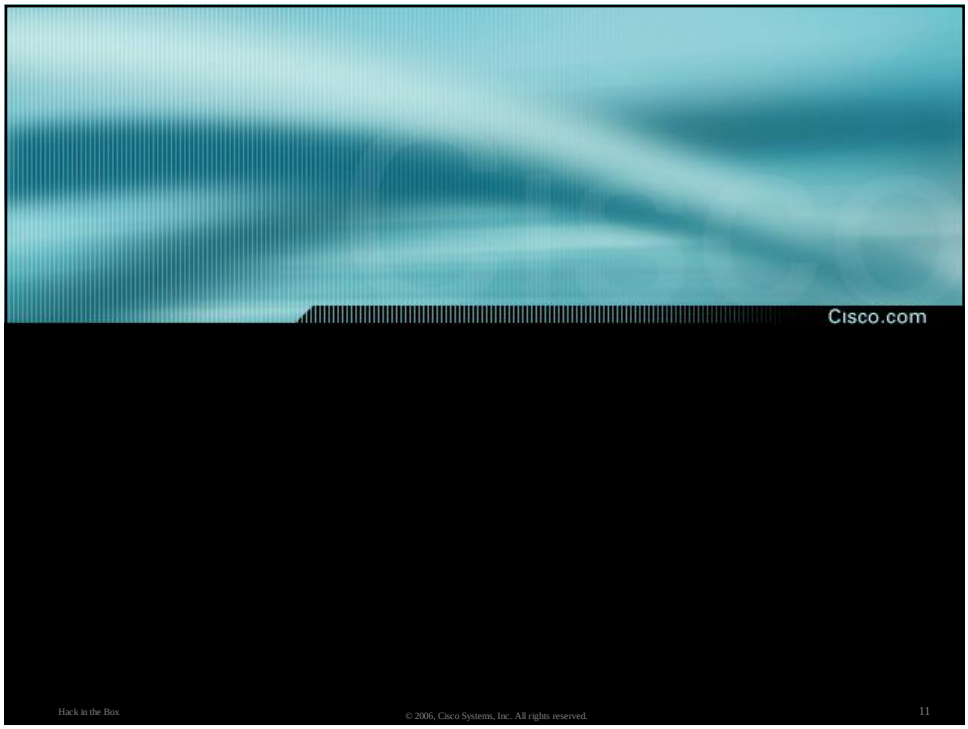
  - PoC to 0-Days
- *Emergence of Security Tools*

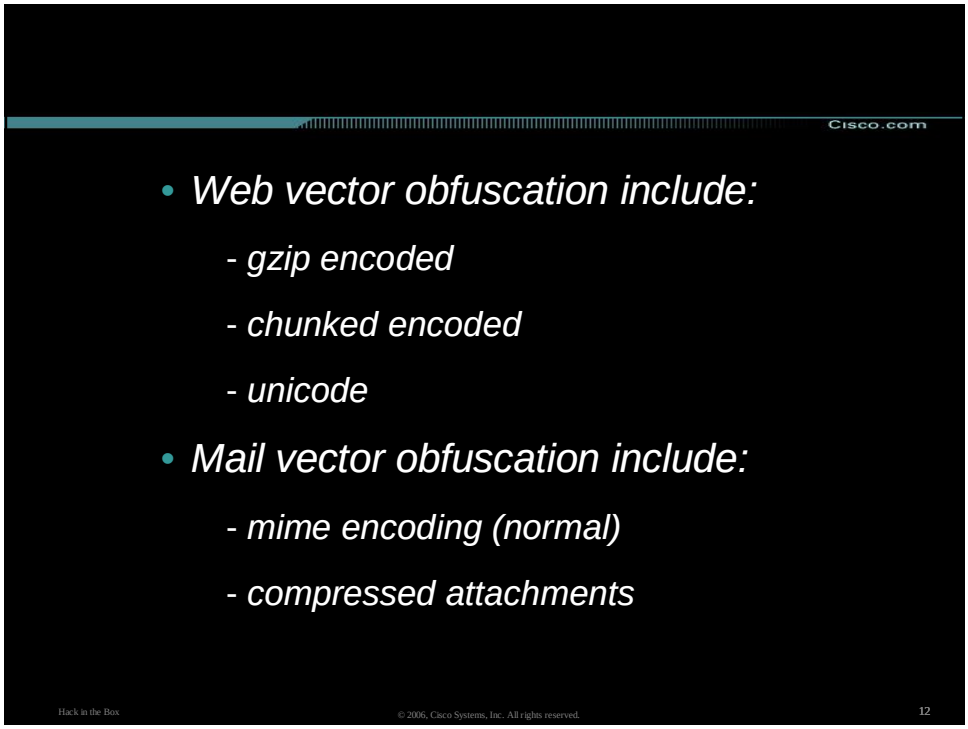
  - Core Impact, Metasploit, Canvas etc…
- *Detection aware security attacks*



- *Weakest point the end-user exploited through mass-mailers*
- *This has evolved to “one-click” exploits.*
  - *spam mails with links to malicious websites*
- *Evolving Attack Vectors makes more dangerous attacks*
- *Trend in exploits through web attack vectors is one of the most dangerous*

- *MSRPC exploits*
  - *Routing and Remote Access Service Code Execution (MS06-025)*
  - *Server Service Code Execution (MS06-040)*
- *File type exploits*
  - *Metafile Code Execution (MS06-001)*
- *Browser Exploits*
  - *Internet Explorer COM Instantiation exploits*
  - *HD Moore’s (creator of Metasploit) Browser bug month*



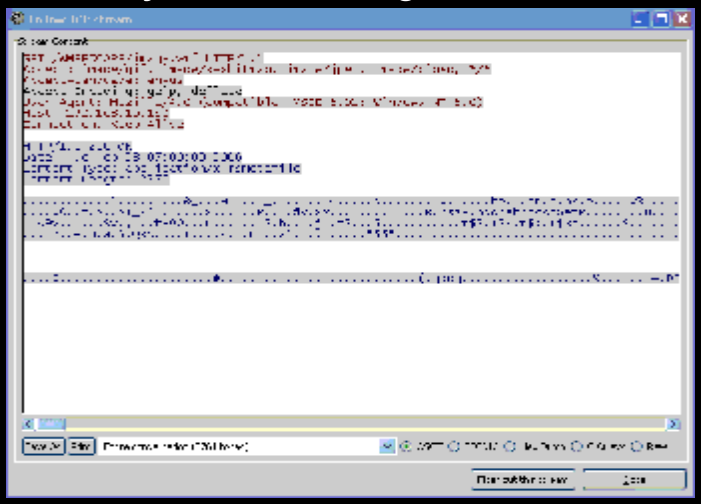


- *Payload Encoding*

GZIP

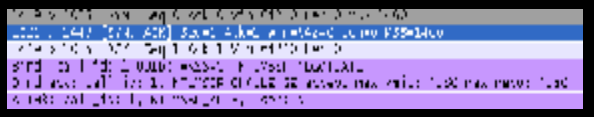
Chunked

Unicode



- *Why is the MSRPC vector such a risk?*
  - *Extremely common in almost all enterprise environments*
- *Services include:*
  - *Server and workstation service*
  - *Computer Browser*
  - *Messenger Service*
  - *Plug and Play*

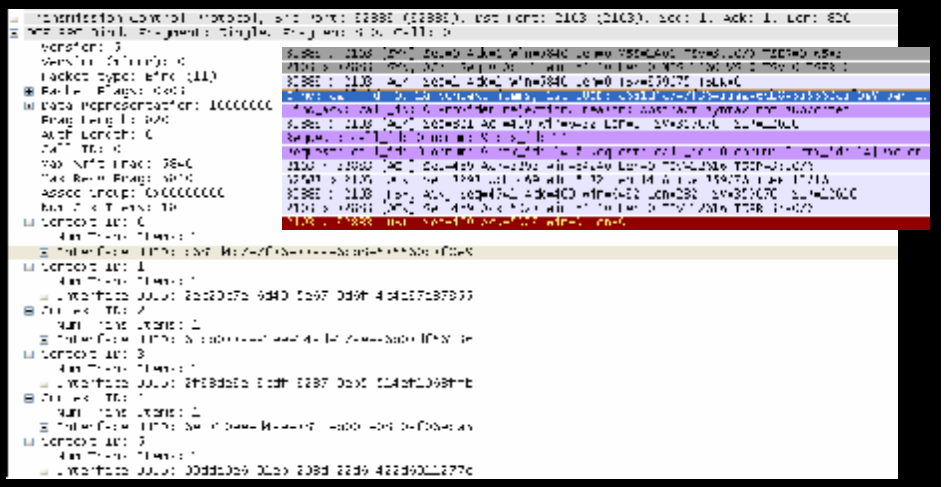
- *Modified version of DCE/RPC*
  - *Universally Unique Identifier (UUID)*
- *Used by Microsoft to create a client/server model*
  - *Connection Oriented*
  - *Bind Request*
  - *Bind ACK*



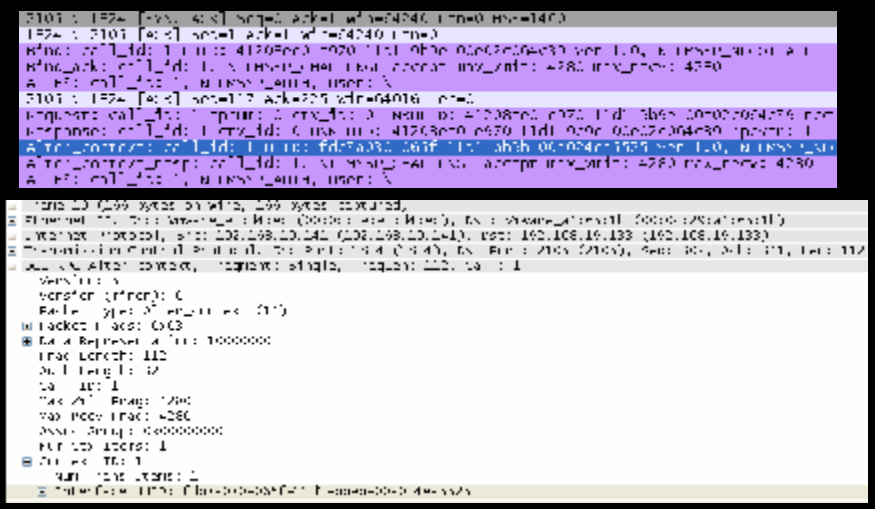
- *Transported over TCP or UDP and SMB*

- *MSRPC Obfuscation*
  - *Multiple UUID's*
  - *Dynamically switching UUID*
  - *MSRPC Fragmentation*
  - *SMB wrapped fragmentation*
  - *Anonymous MSRPC Encryption Wrapping*

- *Multiple UUID's*

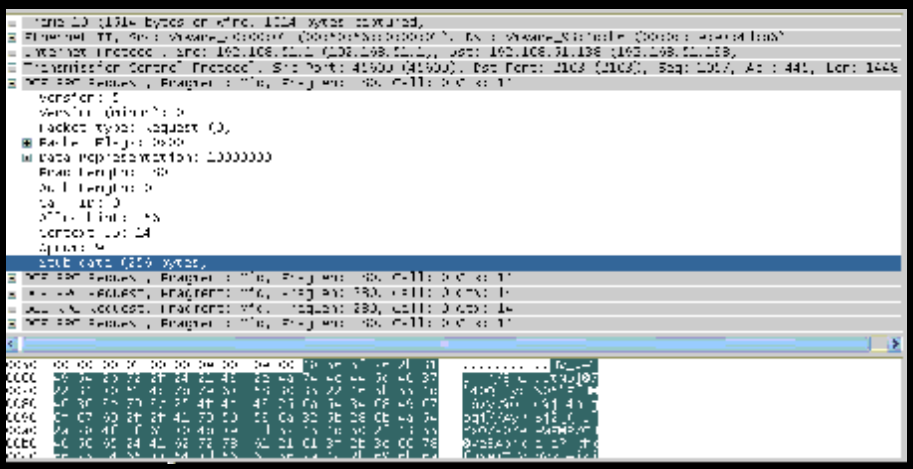


- Dynamically switching UUID



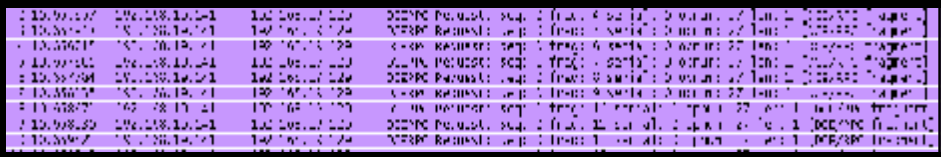
Cisco.com

- MSRPC Fragmentation (Over TCP)



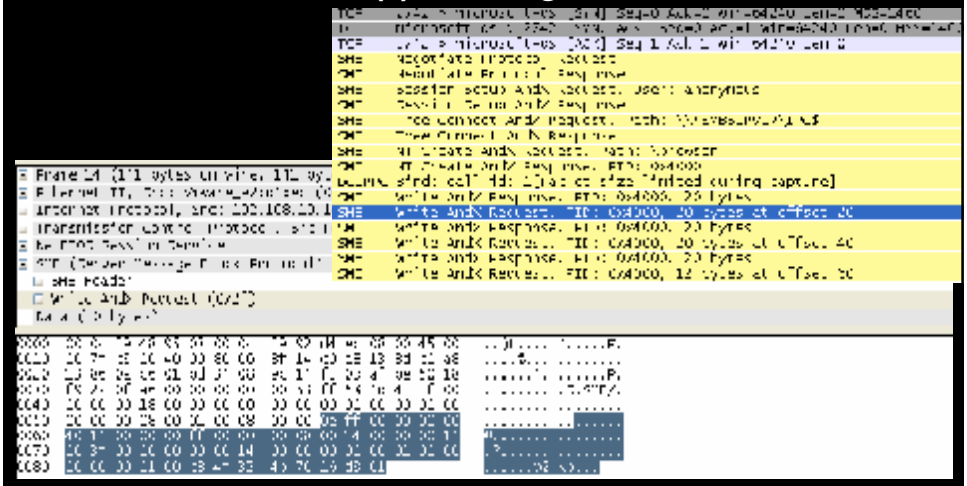
Cisco.com

- MSRPC Fragmentation (Over UDP)

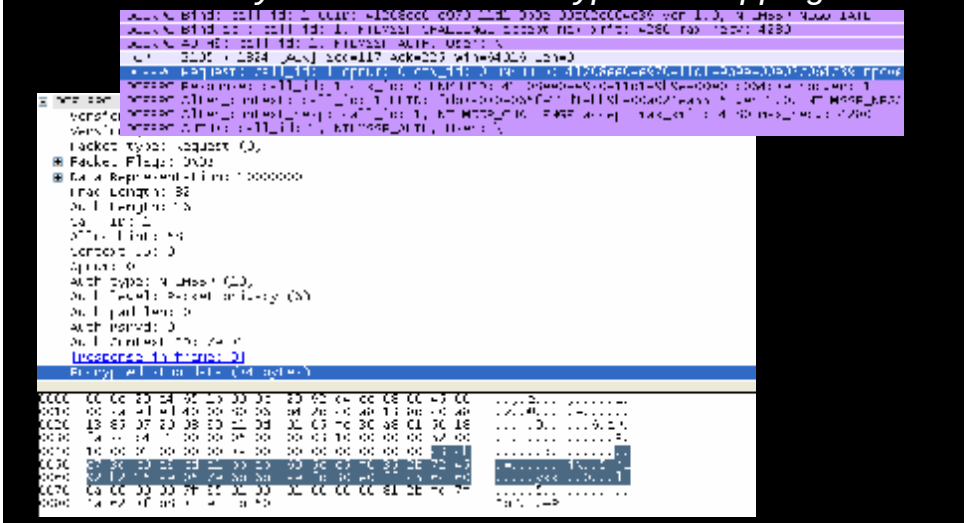


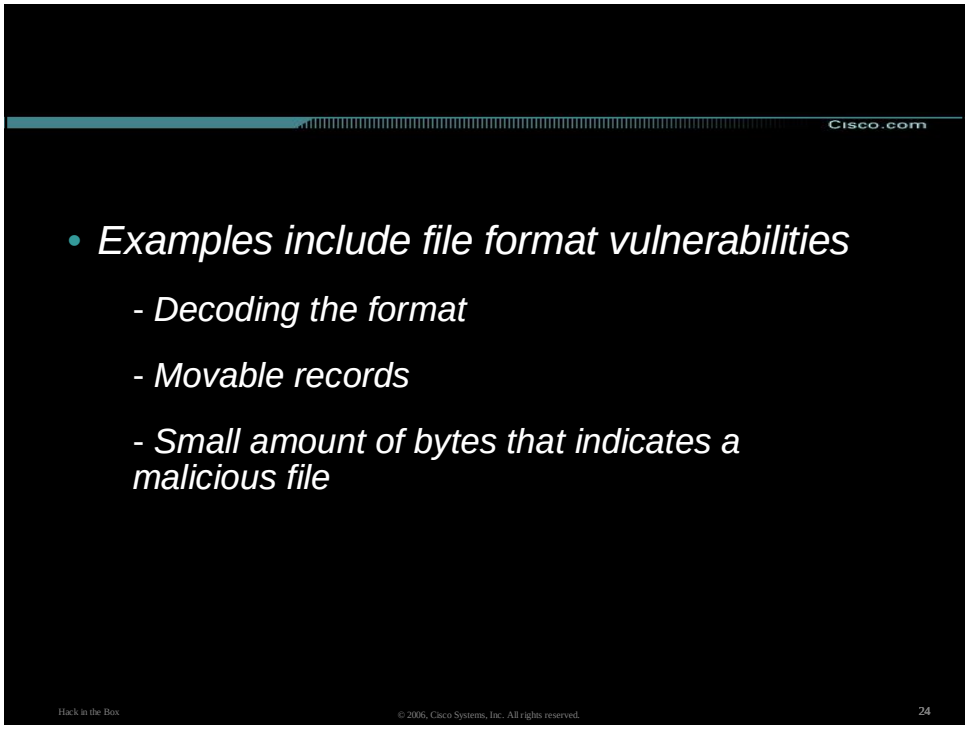
- Data is only 1 byte per packet

- *SMB Wrapped Fragmentation*



- Anonymous MSRPC Encryption Wrapping





- *File format type attacks are best handled through end point mitigation systems*
- *Detection at the kernel level can overcome attacks through encryption*

- *Mitigate threats at the security perimeter*
- *The best tool for network reconnaissance*

  - Prevent the attack before it happens

Cisco.com

- *How intelligent is your network?*
- *Integrated detection from the endpoint and the network makes a more complete picture*

  - multiple sources of intelligence