

Cyber terrorism/warfare

A packet can't fly a plane...

Typical types of attack:

- -Denial of service
- -Breeching the perimeter

Problems with these attacks

- –Does not hurt enough
- -Not effective

What we really need is...

Attacks that are:

- -Targeted / Closely focused (T)
- -Closely coordinated
- -Wide enough to cripple a country
- -Very effective (E)
- -Too fast for human intervention i.e. automated (A)

Part I: A very nasty worm...

Internal networks are weak
Perimeters are strong
Internal network:

- -Machines are never patched
- -Installed with unpatched software
- -New machines are added
- -Not segmented on network layer

A multi–exploit worm's paradise

Part I: A very nasty worm...

Let's see:

- 1. Microsoft IIS Unicode / 2x decode
- 2. Microsoft IIS MSADC
- 3. Microsoft IIS .printer extensions
- 4. Microsoft IIS WebDAV
- 5. Microsoft SQL with blank SA configured
- 6. Blank local administrator passwords on Microsoft Windows hosts
- 7. ...slammer...
- 8. Apache Chunked Encoding
- 9. OpenSSL < 0.9.6

Part I: A very nasty worm...

Finding more food

Targeting on internal network and Internet very different.

- 1. Find your current network/mask
- 2. SNMP queries all around
- 3. Traceroute to Internet
- 4. Pingsweep one class C higher and lower
- 5. ...brute force...

BlackHat 2008 Vegas

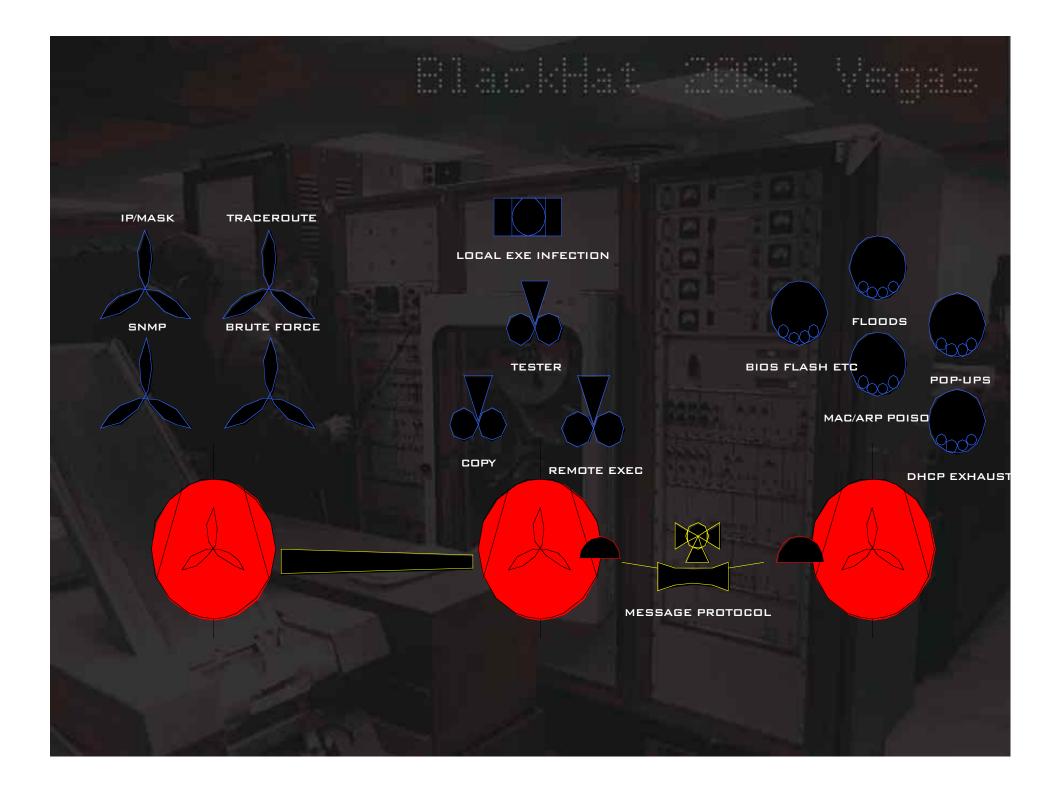
Part I: A very nasty worm...

Denial of service on internal networks is fun:

- -Wire speed flooding
- -ICMP redirection
- -MAC/ARP table trickery
- —DHCP lease exhaustion
- -Hijacking of TCP connections

Since we are here...:

- -DOC/XLS/ZIP/MDB file corruption
- -BIOS flashing
- -Pop-up messages
- -Disable all routers you can find island-ification



Blackhat 2008 Vegas

Part II: Delivery

Who needs 0day silent delivery when you can mail an EXE to someone:

- Using the correct language
- From marketing@companyXX.com
- Subject: "New screensaver for companyXX click here"
- With HTTPS link to intranet.companyXX.com...and then some funny characters...©
- SSL neatly bypass all content level filters

(even PowerPoint thinks its valid)

Blackhat 2008 Yegas

Part II: Delivery

Some stats:

- Target group : IT security team bank
- 13 people in group
- 8 downloaded the EXE
- 5 executed it

One guy executed it 3 times...

Part III: Targeted delivery

How do you find someone on the Internet?

- Google is your friend
- +@companyXX.com -www.companyXX.com
- Scrape it (TOC of Google)
- Example...Hurriyet Newspaper in Turkey

perl emails.pl hurriyet.com.tr

Received 83 Hits:

[bavci@hurriyet.com.tr]

[tturenc@hurriyet.com.tr]

[ecolasan@hurriyet.com.tr]

[yatakan@hurriyet.com.tr]

[dhizlan@hurriyet.com.tr]

[fsever@hurriyet.com.tr]

[rcaglayangil@hurriyet.com.tr]

</snip>

Part III: Footprinting a country

We can extract email addresses from companies

- we need to find companies for each country in the following sectors:
- Telecommunication
- Energy providers (hydro, nuclear, fossil fuel, oil etc.)
- Government departments / Military
- Media providers
- Financial services
- Prominent businesses
- Emergency services
- Transport

Part III: Footprinting a country

Private sector/Public sector

Private:

- Problems with online directories (e.g. Google/DMOZ)
- Solution is specialized directories
- Some online (http://www.world-newspapers.com/), some better to extract (pros/cons)
- Challenge mapping company name to domain name
- Method page 9 of paper.

Part III: Footprinting a country

Private sector/Public sector

Public – government and military

Concept of sub TLD – e.g. gov.za

Not the same for every country – e.g. France (gouv.fr)

Interested in sub domains – maps to departments

- We have Google scraper
- We scrape gov.za (for example)
- Look at all the subdomains
- These becomes targets

Many military domains contained in gov sub TLD.

Recursive scraping...finding *all* the sub domains

Blackhat **2008** Yeg

Part IV: Putting it all together

Years in the industry taught us well-you need a GUI...!



Conclusion

Focused cyber attacks are possible

This method would most likely have negative impact

How does it compare to real life attacks?

Is this YABMT? (yet another bigger mouse trap)

What's the chances of this happening? Should we worry?