

Trends in Denial of Service Attack Technology

-or -

*“Oh, please, they aren’t
smart enough to do that...”*

Presentation to CERT-Polska

November 2001

Rob Thomas, robt@cymru.com

Credit Where Credit is Due!

- **Presentation and paper by Kevin Houle, George Weaver, Neil Long, and Rob Thomas – a global-ish study of a global problem!**
- **Portions originally presented by Kevin Houle at NANOG 23, October 2001.**

Paper located at

http://www.cert.org/archive/pdf/DoS_trends.pdf

Agenda – Keeping up with Rob

- Some history.
- Gift giving for all occasions.
- Target selection – ready, FIRE, aim.
- Methods of control.
- Trends in use and methods.
- What we are not seeing.

BP (Before Pain) - Pre-1999

DoS Tools:

- Single-source, single target tools
- IP source address spoofing
- Packet amplification (e.g., smurf)

Deployment:

- Widespread scanning and exploitation via scripted tools
- Hand-installed tools and toolkits on compromised hosts (unix)

Use:

- Hand executed on source host

The danger grows - 1999

DoS Tools:

- Multiple-source, single target tools
- Distributed attack networks (handler/agent)
- DDoS attacks

Deployment:

- Hand-selected, hard-coded handlers
- Scripted agent installation (unix)

Use:

- Custom, obfuscated control channels
 - intruder → handlers
 - handlers → agents

The bubble bursts - 2000

- 02-2000 : Infamous DDoS attacks
- 04-2000 : DNS amplification attacks,
• mstream DDoS tool
- 05-2000 : VBS/Loveletter, t0rnkit
- 07-2000 : Hybris
- 08-2000 : Trinity IRC-based DDoS tool (unix)
- 11-2000 : Multiple IRC-based DDoS tools
(Windows)

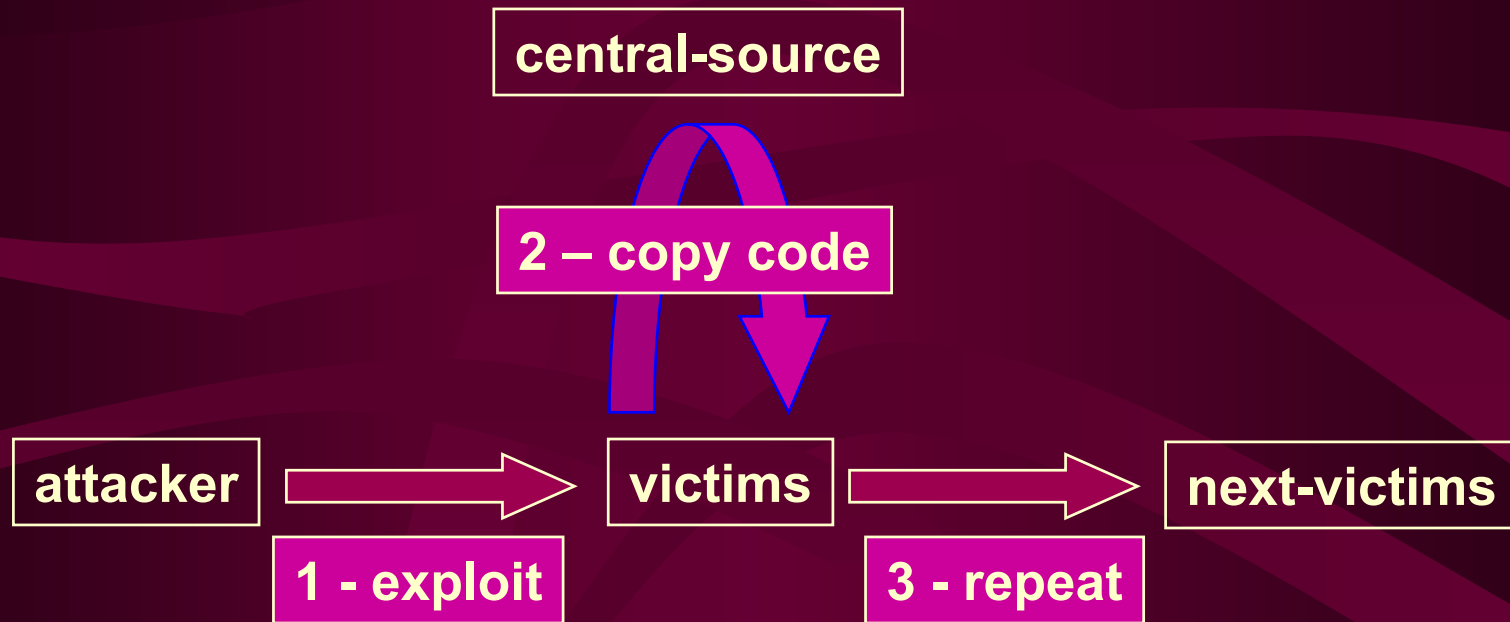
The “fun” continues - 2001

- 01-2001 : Ramen worm
- 02-2001 : VBS/OnTheFly (Anna Kournikova), erkms worm, li0n worm
- 04-2001 : Adore/Red worm, carko DDoS tool
- 05-2001 : cheese worm, w0rmkit worm,
 - sadmind/IIS worm
- 06-2001 : Maniac worm
- 07-2001 : W32/Sircam, Leaves, Code Red worm, various telnetd worms, various
 - IRC-based DDoS tools (knight, kaiten)
- 09-2001 : Nimda worm

Methods of gift giving - The deployment of malware

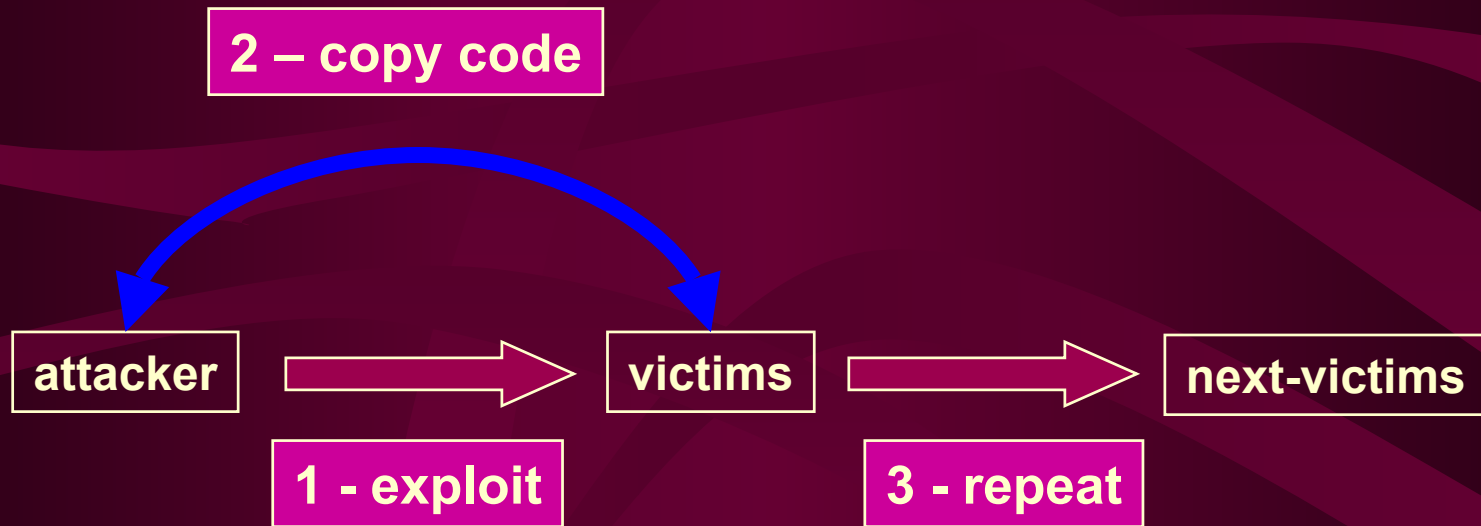
- Greater degree of automation
 - Self-propagating worms
 - Central source propagation
 - Back channel propagation
 - Autonomous propagation

Central Source Propagation



Example: 1i0n worm

Back Channel Propagation



Example: Ramen worm

Autonomous Propagation



Examples: Code Red, Code Red II

Trends Matrix

Targeting Systems: Blind vs. Selective Targeting

Degree of	Blind Targeting	Selective Targeting
Automation	Very high	Low \leftrightarrow high
Vulnerability-specificity	Very high	Low \leftrightarrow high
Other criteria	Low	Very high

Blind Targeting

- Social Engineering

- W32/Sircam
- “Anti-virus” software

- Specific vulnerabilities

- sadmind/IIS worm - UNIX/IIS
- Code Red, Code Red II - IIS
- Nimda - Windows/IIS
- Various telnetd worms – UNIX

- Activity tends to follow vulnerability lifecycles

Selective Targeting – Malware Makes House Calls

– Windows end-users increasingly targeted

- less technically sophisticated
- less protected
- difficult to contact en mass
- slow response to security alerts/events
- well-known netblocks
- widespread broadband connectivity
- increase in home networking
- exploit technology base is maturing

- CERT® Tech Tip - Home Network Security
http://www.cert.org/tech_tips/home_networks.html

Selective Targeting – Routers Aren't Unknown Anymore

– Routers increasingly targeted

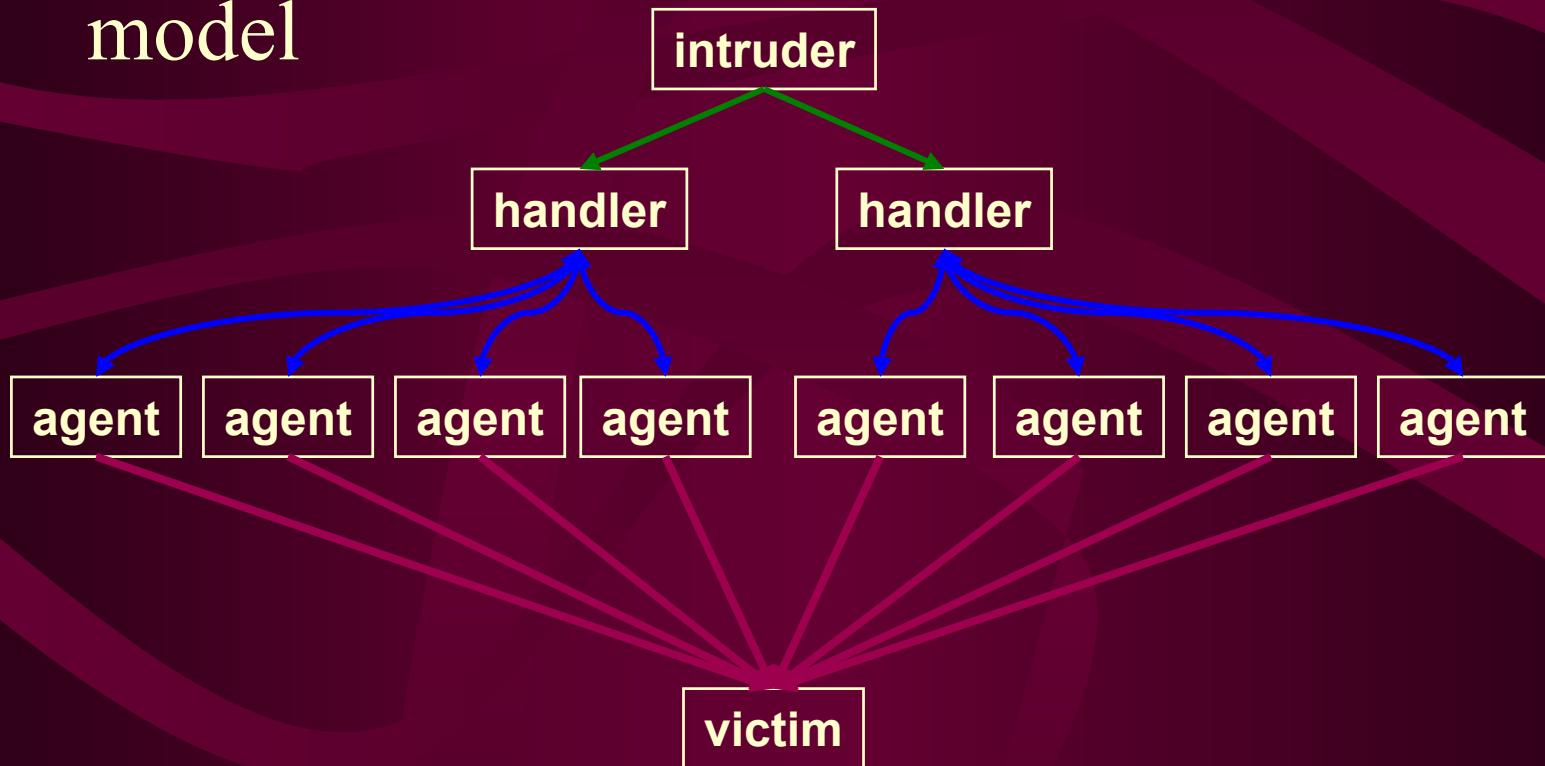
- Source for recon/scanning
- Proxy to IRC networks
- Source for packet flooding attacks

- Compromise via weak/default passwords
- Routers sometimes reconfigured
 - public guides are available

- Increased threat of routing protocol attacks
 - discussions at DefCon and Black Hat Briefings

Control Infrastructure – The “Old Way”

- Control Infrastructure – The classic DDoS model



Control Infrastructure – The “Older Way” is the “New Way”

- Increased use of IRC networks and protocols
 - IRC server replaces the handler
 - common, ‘legit’ service ports (e.g., 6667/tcp)
 - commands are buried in ‘legit’ traffic
 - no agent listeners; outbound connections only
 - More ‘survivable’ infrastructure
 - reduction in address lists maintained
 - disposable, easy to obtain agents
 - makes use of public IRC networks
 - private servers are also used

Why IRC?

- Agent redirection / update is easier
 - everyone change to a new channel
 - everyone change to a new IRC server
 - everyone download this updated module
- “floating” domains used to direct agents
 - bogus WHOIS data, stolen credit cards
 - ‘A’ record modification redirects hard-wired agents

Trends in Use –

Keep it simple, keep it legit

- Less emphasis on forged packet characteristics
 - size and distribution of DDoS makes response difficult
 - overwhelming number of sources in DDoS attack
 - sources often cross multiple AS boundaries
 - high bandwidth consumption is easy; no need for fancy packets
 - increase in attacks using legitimate traffic
 - mixes with other traffic
 - harder to filter/limit

Trends in Impact – The blast radius grows

- Increase in collateral damage
 - backup systems impacted by sharp increases in log volumes
 - financial impact on sites with measured usage circuits
 - multiple sites impacted in shared data centers
 - arp storms impacting locally infected networks
- Highly automated deployments are themselves causing denial of service conditions

What We Are Not Seeing

- Changes in fundamental conditions that enable denial of service attacks
 - Over-consumption of finite resources
 - Processing cycles
 - Memory resources
 - Network bandwidth
 - Interdependency of security on the Internet
 - The exposure to DoS attack of SiteA depends on the security of SiteB
 - ***There are huge numbers of SiteB's***

What We Are Not Seeing (2)

- Advances in DoS attack payload
 - Seeing the same common packet stream types
 - Known attacks work, there is little incentive to improve
 - TCP (SYN|ACK|FIN|RST) flood
 - UDP flood
 - ICMP echo request/reply flood
 - Amplification attacks
 - Source IP address spoofing

What We Are Not Seeing (3)

- Reductions in launch-point availability
 - Vendors are still producing insecure products
 - Administrators and users are still deploying and operating systems insecurely
 - Vulnerability life cycle is still lengthy (2-3 years)

What We Are Not Seeing (4)

- A decrease in pages for Rob.
- An increase in sleep for Rob.
- ***Hey, wait, this describes us ALL!***

Questions?

- Feedback is always welcome!
 - Questions are always welcome!
 - Suggestions are always welcome!
-
- <http://www.cert.org>
 - <http://www.cymru.com/~robt>
 - robt@cymru.com

Thank you for your time!

- Thanks to CERT-Polska for the invitation!