

# Welcome to Blackhat!

Blackhat Security Briefings  
Singapore, October 4, 2002

Timothy M. Mullen  
AnchorIS.Com, Inc.

# Neutralizing Nimda: An Automated Strike-back

## LEGAL DISCLAIMER:

This session describes procedures and processes which may be illegal if deployed against systems which you do not own or have explicit permission to use in the manner we will be illustrating. Code, tools, and procedures are provided for education and research purposes only.

Timothy Mullen is not a lawyer: nothing in this session is meant to be considered legal advise. The accuracy of quoted materials is considered reliable but is not guaranteed.

Thoughts, ideas, and content herein are those of the author, and do not necessarily represent those of the author's employer.

# Session Overview

## Neutralizing Nimda: An Automated Strike-back

### **Technical, Moral, and Legal discussions of strike-back technology**

This session is more about questions than it is about answers. Though almost a year old, Nimda continues to propagate while it consumes bandwidth and resources in the process. Patches have been available since before Nimda struck and clean-up utilities are provided for free; yet we continue to log attacks against our servers on a daily basis. Nothing effective is being done: If you are lucky enough to get a response from an ISP, they will claim their hands are tied, and know-nothing administrators shrug as they delete notification emails.

So, what are your rights when it comes to defending yourself from attack? What are your rights to stop an attacking box from consuming your resources?

We have developed an automated strike-back method where a system can now defend itself against an attacker by neutralizing an attacking box. Currently, deployment of such a system would be considered illegal by many and immoral by others.

This session will discuss several technical methods one can use to stop such an attack (in varying degrees of "finality"), the moral and ethical ramifications of utilizing such a system, and will also attempt to broach legal questions such as "how much is too much," and discuss the application of physical law, i.e. "self defense," to internet events such as worm attacks.

# The Problem

- \_ Nimda continues to spread in spite of publication, patches, removal utilities, and press coverage
- \_ Admins ignore notices/repeat bad installations
- \_ ISP's take no action/responsibility
- \_ Systems advertise their presence to malicious users, allowing for easy acquisition of DDoS hosts.
- \_ Bandwidth utilization/system processing is wasted
- \_ It costs us time and money
- \_ It costs us time and money
- \_ It costs us time and money

IT IS \*MY\* BANDWIDTH!

# Proposed Actions

(from list forums)

- \_ Contact administrators
- \_ Report to ISP
- \_ Blackhole IP's
- \_ Use EarlyBird/DShield
- \_ OS-level solutions (service-shutdown/built-in entropy/auto-magic updates)
- \_ Ignore attacks
- \_ Install the "Big Patch" - Switch to \*nix!
- \_ Publish IP Addresses
- \_ Launch an Anti-worm (Code Green)
- \_ Hack the Offender

# Proposed Actions

(rebuttal)

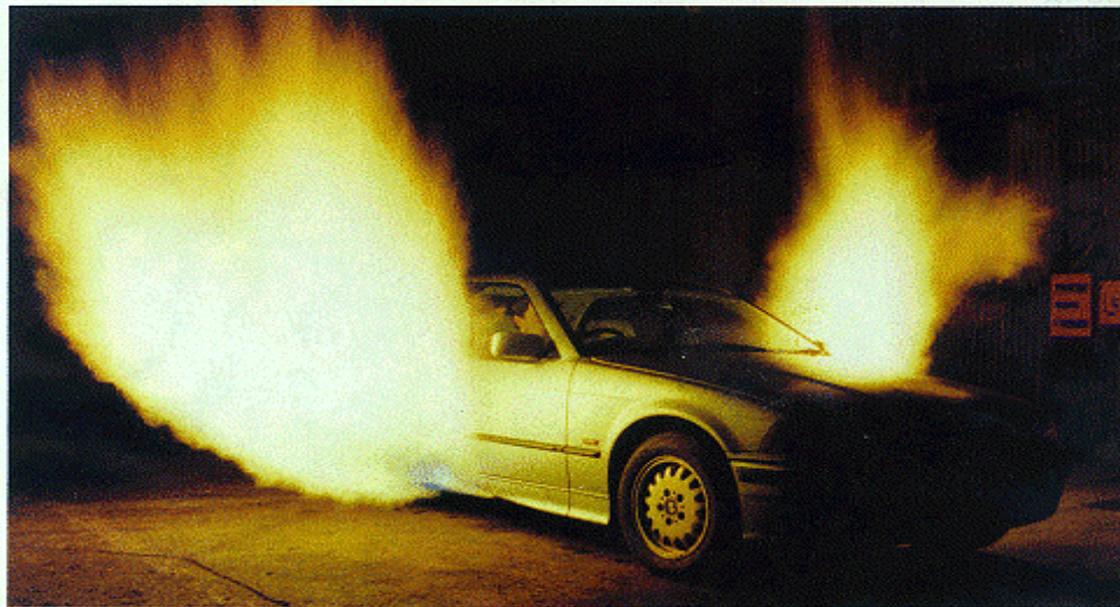
- \_ Contact administrators  
No or hostile response/ no action or responsibility / poor administrative contact records
- \_ Report to ISP  
ditto
- \_ Blackhole IP's  
Bandwidth and processing still utilized/ requires administration
- \_ Use EarlyBird/DShield  
See ditto above / requires even more bandwidth
- \_ OS-level solutions (service-shutdown/built-in entropy/auto-magic updates)  
Would never work! / takes responsibility from the administrator
- \_ Ignore attacks  
Administrative, resource, bandwidth costs continue to build
- \_ Switch to \*nix!  
Total cost high / training / people who couldn't secure an IIS box would be toast in the Unix world
- \_ Publish IP Addresses  
Easy generation of lists for malicious use / would require coordinated effort from publishers to be effective.
- \_ Launch an Anti-worm (Code Green)  
Hard to control / bandwidth use high / attacks "innocent" boxes / illegal
- \_ Hack the Offender  
Illegal / seen as "vigilante" / takes time / Acting out of emotion at this point

# The Law vs. Strike-back

- \_ A strike-back is currently illegal
- \_ I believe provisions should be made to allow for strike-back against worms
- \_ Physical continuum law now being applied to Internet events (Ebay vs. Bidder's Edge)
- \_ Is "Self-Defense" a viable legal position?
- \_ **If not, it should be...**

# Self-Defense?

I M A G E S



## Anti-Theft Device with a Vengeance

Car hijackers in South Africa are in for a roasting. Alarmed by levels of crime—there were over 13,000 forcible car thefts last year—former Johannesburg lawyer Charles Fourie has invented the Blaster. The device shoots liquefied gas, ignited by electric sparks, from nozzles fitted under the front doors. The resulting 2.5-m tongues of flame are designed to deter would-be thieves. Fourie concedes that the plumes of fire could “definitely blind a person,” but feels the risk is justified by the threat

of violence from thieves, who sometimes shoot and kill drivers. South African law permits the use of lethal action where a person’s life or property is threatened. Despite the chances of maiming potential thieves, hundreds have signed up for the \$655 Blaster. Police Superintendent David Walkley of Johannesburg’s crime intelligence unit was Fourie’s first customer and is satisfied that “there are certainly risks using it, but there are also risks in not having anything at all.”

# Self-Defense?

## (Definitions)

### SELF-DEFENSE:

"The protection of one's person or property<sup>1</sup> against some injury attempted by another. The person is justified in the use of force against an aggressor when, and to the extent it appears to him, and he reasonably believes that such conduct is necessary to defend himself or another against such aggressor's imminent use of unlawful force. One who is **not the aggressor in an encounter** is justified in using a *reasonable amount of force* against his adversary when he reasonably believes: (a) that he is in immediate danger of unlawful bodily<sup>2</sup> harm from his adversary, **and** (b) that the use of such force is necessary to avoid the attack, (i.e., one threatening only bodily harm), and to use deadly force against his non-deadly attack."

<sup>1</sup> Inclusion of property is an important provision-

<sup>2</sup> Room for interpretation? Is "property" implied from initial inclusion?

Source: Black's Law Dictionary

# Self-Defense?

(Definitions)

## REASONABLE FORCE:

"That degree of force which is not excessive and is appropriate in protecting oneself or one's property. When such force is used, a person is justified and is not criminally liable, nor liable in a tort."

Source: Black's Law Dictionary

# Self-Defense?

(Definitions)

## California Jury Instruction Code Section 5.30

The following is read to CA jurors sitting on criminal cases involving defendants claiming self-defense:

"It is lawful for a person who is being assaulted to defend himself/herself from attack, if, as a **reasonable person** s/he has grounds for believing and does believe that bodily injury<sup>2</sup> is about to be inflicted upon him/her. In doing so, that person must use all force and means which s/he believes to be **reasonably necessary** and which would appear to a **reasonable person**, in the same or similar circumstances, to be necessary to prevent the injury which appears to be imminent."

<sup>2</sup> See previous note regarding inclusion of "property."

Source: Shuyokan Budo Genjitsu Ryu Website

# The Facts

- \_ The worm "intends" to compromise our systems
- \_ It will continue to attack until stopped or patched
- \_ Nimda attacks near-subnets 75% of the time
- \_ The attack is definitive
- \_ The costs (harm/injury) are identifiable and measurable
- \_ The costs \*will\* continue to rise
- \_ Effect is Internet-wide (one researcher quantified the attacks at 5 \*billion\* a day)
- \_ No redeeming value- everyone agrees this is problem that needs to be dealt with.
- \_ This \*will\* happen again- if a consensus is reached, strike-back technology could save millions, if not billions, of dollars in hard and soft costs associated with worm propagation (depending on who you believe).

# The Goals

## Immediate:

- \_ Stop the attack against us
- \_ Stop the attack against others
- \_ Notify the administrator
- \_ Stop future attacks from the same machine (re-infection, etc.)
- \_ Patch the box? Dangerous--

## Long Term:

- \_ Implement framework for future threats
- \_ Identify "acceptable" strike-back methods
- \_ Gain legal support

# The Strike-back

## SOME PROPOSED METHODS:

### \_ System shut-down

Drastic. It stops the attack, but is the most expensive to the host company. Writing to the boot.ini would alert the admin and keep the box from loading. However, upon load, it would start attacking again.

Is that "excessive" force?

### \_ Remote Patch

Complex. Possibly introduces other issues- what level do you patch them to? Requires reboot- what if the system did not come back up? This too could cause problems for the admin.

### \_ Stop www publishing service

Stops the attack, but restarting the service would resume attack. Requires another method of alerting the admin. Disables all web services, which could cause undue hardship for the host.

# The Strike-back

## THE PREFERRED METHODS:

- 1) Instantiate Nimda's named "Mutual Exclusive" object (MUTEX)**
- 2) Block outbound-only traffic at the port level**

- \_ Option 1 is Nimda specific- Option 2 provides for future worm defense**
- \_ Least invasive of all methods- provides for "reasonable force" required to stop the attack**
- \_ Persistent across reboots**
- \_ Little impact if any on server operations**
- \_ Leaves all other host services running**
- \_ Actually restores server host availability in that bandwidth is not being consumed by outbound attacks**
- \_ Requires no patching or cleaning software to be run**
- \_ Leaves the host vulnerable, but does not allow for propagation of any service-based worm.**
- \_ Easily removed by the host administrator after notification**
- \_ Leaves all other system files intact/unaltered to preserve forensics**

# The Strike-back

TECHNICAL PROCESS (Option 1):

## Named Mutex:

- \_ **Strike-back host listens for attacks**
- \_ **Strike-back host accepts connection and verifies attack signature**
- \_ **Strike-back host logs attack**
- \_ **Strike-back host verifies vector availability- only uses vector if available; Bail-on-Fail**
- \_ **Strike-back host logs status**
- \_ **Using worm attack vector (dir trav here) toolkit is loaded to box**
- \_ **First tool "esc.dll"- escalates process privileges, and adds IWAM and IUSR to "Administrators" group.**
- \_ **Second tool "mutex.exe" – creates named mutex on load, preventing Nimda from executing. [fsdhqherwqi2001 = CreateMutex(NULL,TRUE,"fsdhqherwqi2001");]**
- \_ **Script removes IWAM and IUSR from "Administrators" group**
- \_ **Script removes "esc.dll" to clean up**
- \_ **Script leaves "readme.txt" explaining what happened**
- \_ **Strike-back host logs status**
- \_ **Strike-back host returns to listen state**

# The Strike-back

TECHNICAL PROCESS (Option 2):

## Create IPSEC outbound filter (Win2k)

- \_ **Strike-back host listens for attacks**
- \_ **Strike-back host accepts connection and verifies attack signature**
- \_ **Strike-back host logs attack**
- \_ **Strike-back host verifies vector availability- only uses vector if available; Bail-on-Fail**
- \_ **Strike-back host logs status**
- \_ **Using worm attack vector (dir trav here) toolkit is loaded to box**
- \_ **First tool "esc.dll"- escalates process privileges, and adds IWAM and IUSR to "Administrators" group.**
- \_ **Second tool "ipsecpol.exe" – creates and assigns IPSEC policy to block outbound port (80 in this case)**
- \_ **Script removes IWAM and IUSR from "Administrators" group**
- \_ **Script removes "esc.dll" to clean up**
- \_ **Script leaves "readme.txt" and small script to remove the IPsec filter**
- \_ **Strike-back host logs status**
- \_ **Strike-back host returns to listen state**

# The Strike-back

TECHNICAL PROCESS:

## DEMO

**(Note to The Fed: These are my boxes so don't try to pinch me.)**



# Considerations

- \_ Proxied attacks
- \_ Defining an attack
- \_ Defining an acceptable defense
- \_ Future worms may start to be written to patch the vector to increase the difficulty of remote strike-backs or auto-patches
- \_ Are we tampering with evidence?
- \_ International Law

# Discussion

- \_ Should strike backs be legal?
- \_ Are they ethical?
- \_ What other technical hurdles?
- \_ Questions/Concerns

# Acknowledgements

\_ I would like to thank the following people for their contributions (whether they know they contributed or not) to this project:

**Blue Boar** – coding, technical guidance, research

**JD Glaser** – technical guidance, coding, opinions and feedback

**Jeremiah Grossman** – outbound port blocking idea, opinions and feedback

**Jennifer Granick** – legal opinions and consultation

**Blain Kubesh** – originally reported to Security Focus list Nimda's use of a named mutex

**Scott Culp** – opinions and feedback

[www.HammerofGod.com](http://www.HammerofGod.com)  
[thor@hammerofgod.com](mailto:thor@hammerofgod.com)

# Thank You!

\_ Additional information available on the  
Hammer of God website:

[www.HammerofGod.com](http://www.HammerofGod.com)  
[thor@hammerofgod.com](mailto:thor@hammerofgod.com)