



Securing an ISP Backbone

Introduction

Michael H. Behringer <mbehring@cisco.com>

Distinguished Engineer

News - January 22,2002

Cloud-Nine Officially Closes ISP!

By:[mark.j](#) @ 10:44:AM - [Comments](#) (35) - SendNews [[HERE](#)] / PrintNews [[HERE](#)]

Today looks set to be a sad and frustrating one for anybody who was ever a customer of the once popular unmetered dialup and broadband ISP Cloud-Nine.

At precisely 10:16am a few minutes ago Emeric Miszti (CEO) and John Parr (Operations Director) of the C9 ISP posted what's likely to be their final announcement on our forums. **C9 is now the latest ISP to close, although it's the first we've ever seen to go from a hack attack!:**

Cloud Nine regret to announce that at 7:45 this morning the decision was taken to shut down our Internet connections with immediate effect.

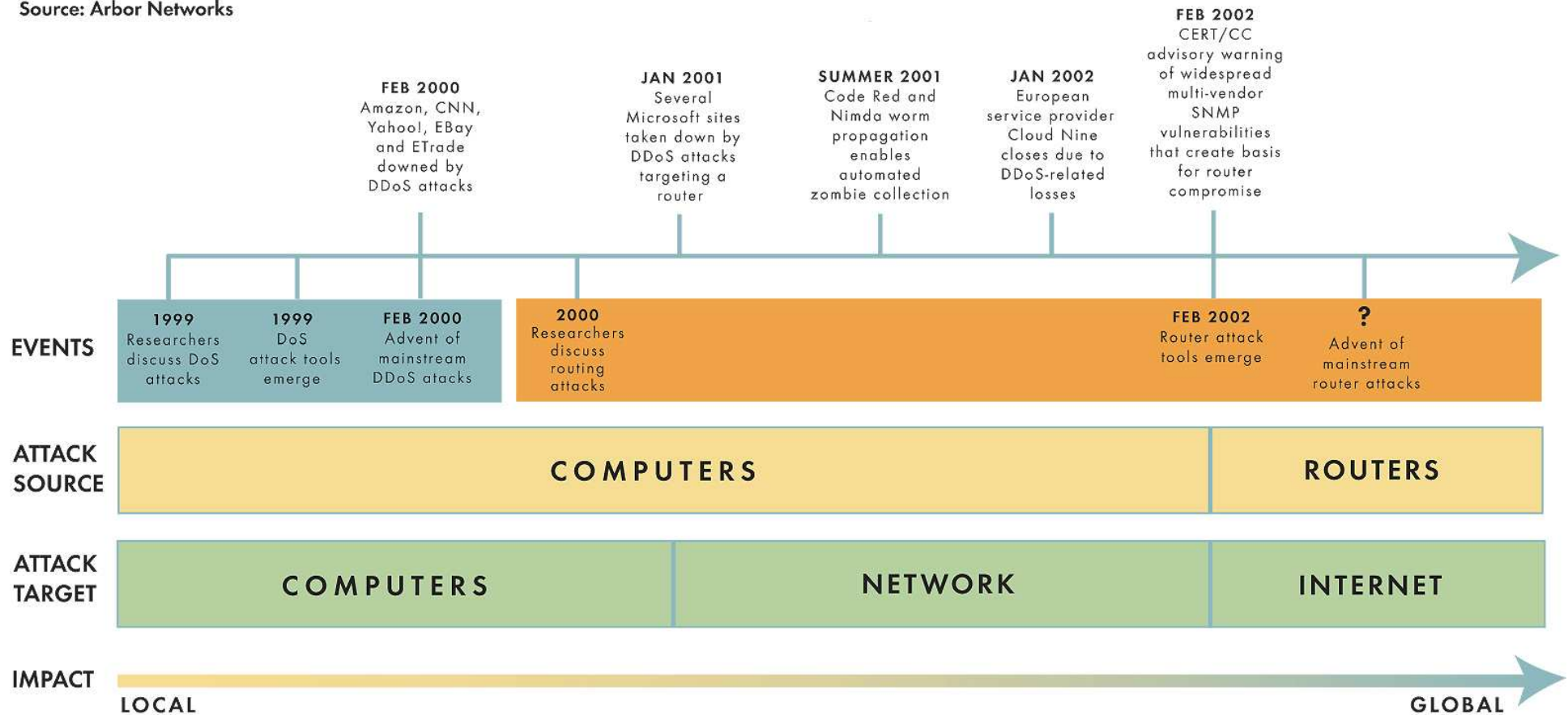
We tried overnight to bring our web servers back online but were seeing denial of service attacks against all our key servers, including email and DNS. These were of an extremely widespread nature.

http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274_91619

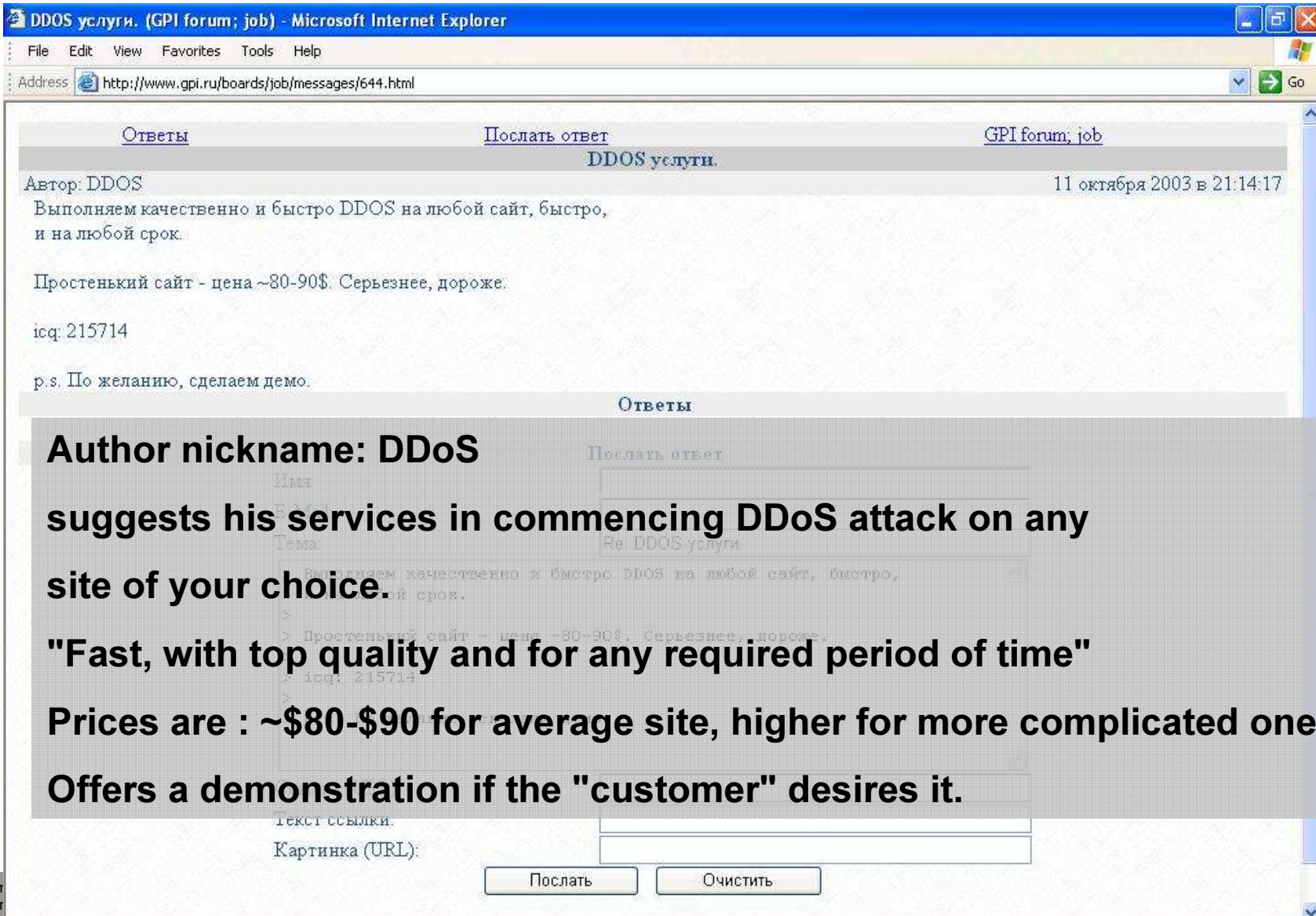
Evolution of Availability Threats

Evolution of Network Availability Threats

Source: Arbor Networks



Recent Trends: DoS-for-Rent



The screenshot shows a forum post in Russian. The browser title is "DDOS услуги. (GPI forum; job) - Microsoft Internet Explorer". The address bar shows "http://www.gpi.ru/boards/job/messages/644.html". The post content includes:

- Author: DDOS
- Date: 11 октября 2003 в 21:14:17
- Text: "Выполняем качественно и быстро DDOS на любой сайт, быстро, и на любой срок."
- Text: "Простенький сайт - цена ~80-90\$. Серьезнее, дороже."
- Text: "icq: 215714"
- Text: "p.s. По желанию, сделаем демо."

Below the post is a reply form with fields for "Имя", "Тема", "Текст ссылки", and "Картинка (URL)", and buttons for "Послать" and "Очистить".

Author nickname: DDoS

suggests his services in commencing DDoS attack on any site of your choice.

"Fast, with top quality and for any required period of time"

Prices are : ~\$80-\$90 for average site, higher for more complicated ones.

Offers a demonstration if the "customer" desires it.

Recent Trends: Extorsion

- “You pay me 20,000\$ or your web site goes down.”

Headlines

Super Bowl fuels gambling sites' extortion fears

By Paul Roberts

IDG News Service, Boston Bureau

30-01-2004

In recent years, online sports betting parlors or "sports books" have fast supplanted the shadowy world of "bookies," or professional bet takers in the U.S., Canada and Europe, growing into a multibillion dollar industry, despite official disapproval from Washington, D.C. lawmakers and U.S. religious conservatives.

BBC NEWS UK EDITION

Last Updated: Friday, 19 March, 2004, 12:35 GMT

[E-mail this to a friend](#)

[Printable version](#)

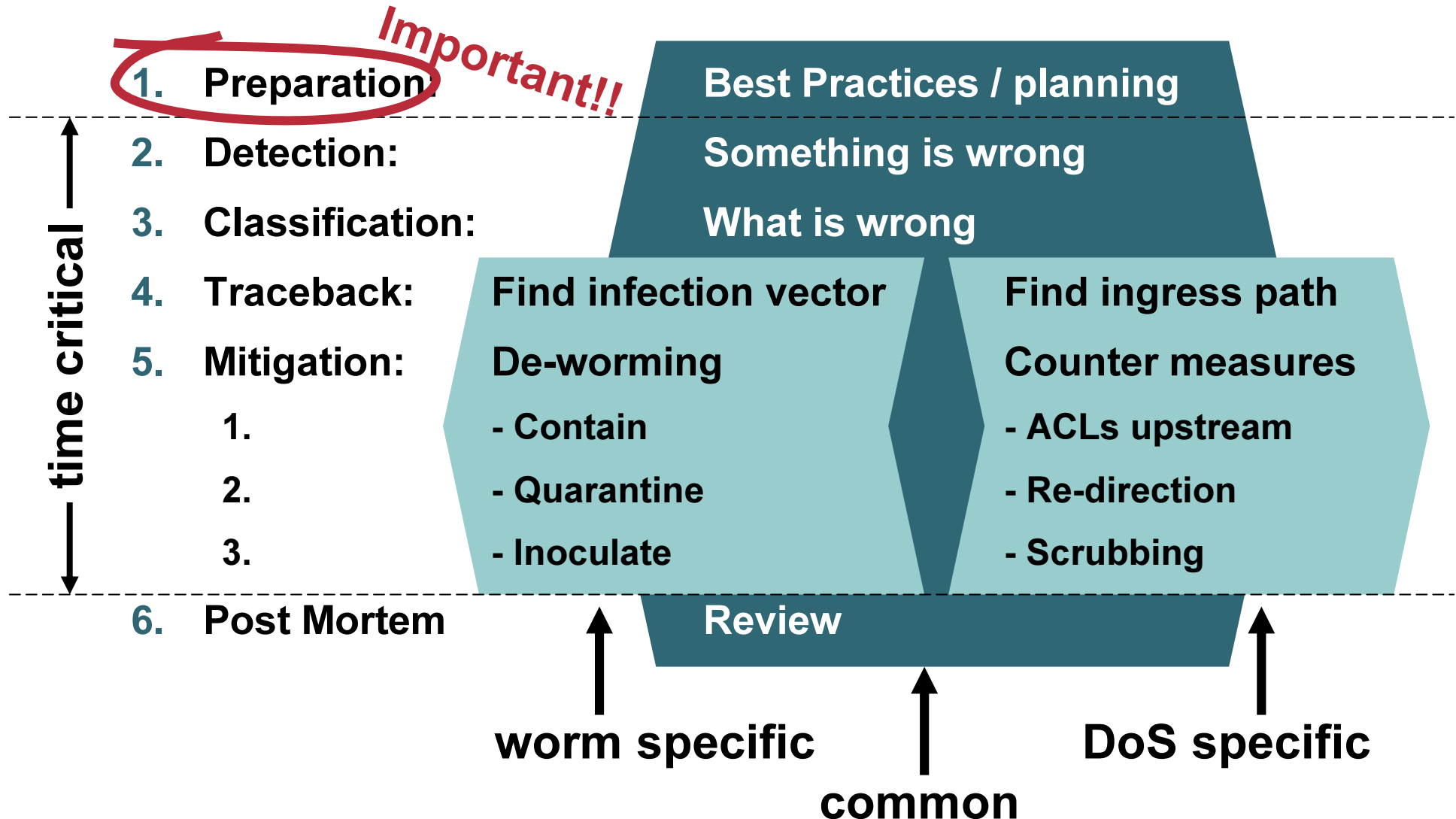
Bookies suffer online onslaught

By Mark Ward

BBC News Online technology correspondent

The extent to which British betting websites are being attacked by criminals using the net to bring down a site unless a ransom is paid has been revealed by a BBC News Online investigation.

6 Phase Incident Response Methodology for Worms and DoS



Call for Action

- **The Internet is becoming the target**

- **Must secure:**

Your routers

Your DNS / other critical services

The infrastructure

- **Must protect:**

Your customers from the Internet

The Internet from your customers



**You are part of the
Internet!**

**Goal of this Wokshop:
Work together to secure the global Internet**

You are not alone!

more involvement



- **CERT-CC (www.cert.org)**
Current security issues and solutions
- **NANOG (www.nanog.org)**
North American Network Operators Group
- **PSIRT (www.cisco.com/go/psirt)**
Cisco's Product security team (with HOT page)
- **NSP-security (puck.nether.net/mailman/listinfo/nsp-security)**
Closed list with SP security experts
- **INOC-DBA (www.pch.net/inoc-dba/)**
Set up an Inter-NOC SIP telephone network
- **many more...**

Securing a Core Network — Overview

1. Basic Security

AAA, SSH, SNMPv3, rACL, CoPP, etc...



**Individual
router security**

2. Don't let packets into (!) the core

→ No way to attack core, except through routing, thus:



**Still "open":
routing
protocol**

3. Secure the routing protocol

Neighbor authentication, maximum routes, dampening, GTSM, ...



**Only attack
vector: Transit
traffic**

4. Design for transit traffic

Correct Core Design

Capacity / QoS

Choose correct router for bandwidth



**Now only
insider attacks
possible**

5. Operate Securely



**Avoid insider
attacks**

Agenda: ISP Security

0900-0915	Introduction: Current Threats for SP Networks
0915-1030	Securing Routers and the Management Plane
	Break
1100-1145	Securing the Control Plane
1145-1230	Securing the Data Plane
	Lunch

References

- **Team Cymru**
ISP security guidelines, templates, bogon tracking, etc:
<http://www.cymru.com>
- **NANOG (North American Network Operators Group)**
Presentations on ISP security techniques, discussions, etc
<http://www.nanog.org>
- **Packet Clearing House**
Relevant techniques, white papers, config examples, etc.
<http://www.pch.net/>
- **Internet Storm Center and Distributed Intrusion Detecion**
Global Internet monitoring system
<http://isc.sans.org/> and <http://dshield.org/>

References (Cisco - public)

Product Security:

- Cisco's Product Vulnerabilities; A must-know for every Cisco user!!!
[<http://www.cisco.com/go/psirt>]
- Security Reference Information: Various white papers on DoS attacks and how to defeat them [<http://www.cisco.com/warp/public/707/ref.html>]

ISP Essentials:

- Technical tips for ISPs every ISP should know
[<ftp://ftp-eng.cisco.com/cons/isp/>]

Technical tips:

- Troubleshooting High CPU Utilization on Cisco Routers
[<http://www.cisco.com/warp/public/63/highcpu.html>]
- The “show processes” command
[http://www.cisco.com/warp/public/63/showproc_cpu.html]
- NetFlow Performance White Paper
[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/ntfo_wp.htm]

Mailing lists: (see PSIRT pages for subscription)

- cust-security-announce: All customers should be on this list.
- cust-security-discuss: For informal discussions.

Q and A



