

# **Explaining Distributed Denial of Service Attacks to Campus Leaders**

Internet2 Member Meeting

Arlington, Virginia

3-4 PM May 3rd, 2005

Joe St Sauver, Ph.D. (joe@uoregon.edu)

University of Oregon Computing Center

<http://darkwing.uoregon.edu/~joe/ddos-exec/>

# The Audience For Today's Talk

- Unlike many of my previous I2 or Joint Techs talks which have dealt with technically arcane issues or tactical level concerns, this talk is meant to be more strategic, and is really targeted at the CIOs and Institutional Executive Representatives who are at today's meeting.
- Hopefully it will spur discussions about distributed denial of service attacks with senior administrators back at your campus, as well as with technical staff within your campus computing and networking organizations.
- Because some may refer to this talk after the fact, and because we also have both remote netcast participants and audience members for whom English may not be their primary language, I've tried to write this talk in a way that will make it easy for them to follow along.

# Disclaimer

- I currently am co-chair of the Educause Security Effective Practices Task Force, I sit on the Internet2 Security at Line Speed (SALSA) working group, and I'm one of three senior technical advisors for the carrier Messaging Anti-Abuse Working Group (MAAWG), but my remarks today should not be taken as representing the official position of any of those groups.
- You should recognize that parts of this talk involve projections about what might (or might not) happen in the future. My "crystal ball" horizon is usually fairly short, typically running about 6-18 months, so we'll probably know if I got this one right one way or the other before too long. Maybe, if we're all lucky, I will have gotten this one completely wrong -- if so I couldn't be happier.

# Campus Leaders

- Campus leaders have generally come to understand and appreciate the risks associated with security threats such as viruses, spyware, unpatched hosts, unencrypted network traffic, identity theft and insecure physical facilities.
- But, many chancellor/president/provost-level university executives have had little opportunity to be briefed on the serious risks their campus may face from distributed denial of service (DDoS) attacks.
- This talk is designed to encourage you to brief your campus leadership team on the DDoS issue, and to help lay out some of the issues you may want to be prepared to address.

## **Is The DDoS Issue One Which Meets The Threshold For Executive Attention?**

- Senior campus leaders are busy people. They should not be bothered with trivialities or speculation about improbable events.
- Unfortunately, the DDoS issue is one which is both decidedly non-trivial, and one which has a demonstrated track record of affecting typical campuses, campuses just like yours and mine, as well as some of the Internet's very largest and best run "money-is-no-object"-class enterprises.
- We should probably take a minute to explain why the DDoS issue is potentially such a "big deal..."

# DDoS Attacks Can Impact All of Campus...

- Many common types of DDoS attacks, such as packet flooding attacks, can affect literally everyone on campus by filling external networks pipes to the point where the the campus network is rendered unusable...
- Any attack that can affect everyone on campus is unquestionably a “big deal.”

# DDoS Attacks Can Last for Some Time...

- DDoS attacks may last for hours or days (or longer), or occur repeatedly over a series of occasions.
- Any attack which has the potential to result in sustained disruptions, or reoccurring disruptions, is a “big deal.”

# **DDoS Attacks Can Disrupt Mission Critical University Operations**

- Imagine the impact of a prolonged email outage, or loss of external access to your campus web site, or problems with your teaching and learning system, or having your ERP system be unavailable....
- There are typically a large number of key university operations which require the campus network and/or wide area network connectivity to be present and usable. If you knock out the campus network (or key hosts), this can be as disruptive as causing a campus wide power or water service outage. Business stops.
- Again, unquestionably, this would be a “big deal.”



# **DDoS Attacks Can Be Expensive**

- The out-of-pocket costs associated with avoiding DDOS attacks (and/or the costs associated with mitigating a DDoS attacks, should one occur) may be substantial, and for most sites would represent a sudden large unplanned-for and unbudgeted-for expense.
- That makes DDoS attacks potentially a “big deal.”

# The Press Will Smell Blood in the Water

- Because of all the factors just mentioned, and because DDoS attacks often contain an element of “David and Goliath” (“13 year old takes down million dollar network from his tree house with 2nd hand wireless laptop”), journalists often find DDoS attacks quite newsworthy.
- Anytime there’s potential media interest about a campus incident, it’s a “big deal.”

# DDoS Attacks May Have Legal Implications

- Whether your institution is the victim of a distributed denial of service or “just” has compromised systems that are participating in attacking some other target, there’s a high probability that campus legal counsel will end up becoming involved...
  - Does the university want to investigate the attack and try to have the attacker criminally prosecuted? Would a civil suit be better? Do we want to take any legal action at all?
  - Are there legal issues associated with possible DDoS identification strategies and remediation approaches?
  - Is the university liable for attacks committed via one of its compromised systems?
- Lawyers involved ==> “big deal.”

# OK... So DDoS Attacks May Be a Big Deal

- But what would briefing the executive leadership actually accomplish?
- Well, it may scare the heck out of them, but that's NOT the objective.
- The top brass need to know what they're potentially facing so that they're not blindsided if an incident occurs. Without accurate technical intelligence campus leaders it's also impossible for campus leaders to weigh risks, prioritize issues, and make informed decisions about institutional strategies and exposures.

# DDoS Attacks Are Not Just An IT Problem

- If you come out of an IT background, it is only natural to view a “technical issue” like denial of service attacks as an “IT problem.” However, for all of the reasons we’ve already talked about, denial of service attacks are something that’s really an organization-wide problem.
- Senior campus leaders can work with deans and directors and senior executive staffers to insure that a chosen campus strategy for dealing with DDoS attacks gets translated into an operational plan.
- A strategy that’s articulated from the the top of the institution also carries more weight with campus audiences than one which just comes from within IT.

# Resources

- Once senior management has been briefed, they may be also be able to allocate or reallocate staff and financial resources from outside your traditional organization to help as may be required.

# Timing Your Briefing

- There's also the issue of timing: when should campus leaders be briefed?
  - One approach would be to wait until your campus is actually suffering a distributed denial of service attack, and the administration is in dire need of information about what's going on (obviously at that point you'll have a motivated/interested audience, and there's no risk that you'll end up "crying wolf").
  - An alternative approach is to consider briefing campus leaders now, before your campus is suffering from a distributed denial of service attack. By doing so, you'll have maximum time to pre-plan a coordinated response and to marshall your forces (but you also run the risk that your campus may never actually end up getting hit).
- A short discussion now, to at least introduce the topic, might be best compromise (only you can judge this).

# Are DDoS Attacks Really an "Internet2 Issue?"

- The answer to that question is unequivocally yes. DDoS attacks are an Internet2 issue because:
  - one vector that might be used to attack your campus is your connection to Abilene, the Internet2 backbone
  - turning that around, if hacked hosts on your campus are used to attack other schools, the infrastructure you've built out to support Internet2 means that the bad guys will be potentially wielding a formidable weapon
  - NPPAC (the Internet2 Network Policy and Planning Committee), SALSA (the Internet2 Security at Line Speed initiative), the Educause Security Task Force and myriad federal agencies including the NSF and the Department of Energy have all made it clear that network security is a top priority, and DDoS attacks tend to be among the most costly of all attacks.



# DDoS Attack Costs: The 2nd Most Expensive Type of Information Security Incident in 2004

- According to the 9th Annual CSI/FBI 2004 Computer Crime and Security Survey (see [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf) at page 10):
  - viruses were (in aggregate) the single most expensive type of information security incident (costing 269 organizational respondents a total of \$55,053,900, or an average of \$204,661/organization)
  - **denial of service attacks were the second most expensive type of information security incident**, costing those same respondents \$26,064,050 (an average of \$96,892 each).

# A Meaningful, Tough, Problem

- I would also add that dealing with network denial of service attacks, as an example of a complex, meaningful, tough, real world network problem, is precisely the sort of advanced practical networking challenge that Internet2 member universities should be taking on in the security space.
- If we don't pay attention to the distributed denial of service issue, we run the risk of jeopardizing Abilene's special interconnectivity with federal mission networks.
- Internet2 may be one of the few networks where research on IPv6 and IP multicast DDoS is possible.
- There are also Internet2 corporate partners/corporate sponsors who are active in the DDOS space, providing additional opportunities for collaboration.

# Why Are DDoS Attacks An Issue Now?

- Extensive botnets (literally millions of compromised consumer desktop computers) have been deployed over the last few years for the purpose of delivering spam.
- Internet Service Providers have recently begun to take steps to block those botnet hosts from being easily used for spamming (e.g., by blocking all port 25 traffic except for officially authorized servers). Less spam! Wonderful!
- **If you're a spammer and you've got 100,000's of zombied hosts that are no longer usable for sending spam, what are you going to do with them? Just forget about them? No... You'll look for other ways you can make money with those "assets" -- such as using them to conduct denial of service attacks against uncooperative extortion targets. Ugh.**
- <http://darkwing.uoregon.edu/~joe/zombies.pdf>

# **What Does Your Campus Leadership Need to Know About DDoS Attacks?**

# Every Executive Is Different

- We recognize that every executive or campus administrator is different, and some may have dramatically different levels of interest in particular “technology issues.” For example, some may be technology enthusiasts and passionately interested in knowing all the details of networking security's nuts and bolts, but most will be busy and preoccupied with other concerns and just want the bottom line nutshell message.
- So let's start with that “nutshell message” and then expand from there, recognizing that often simply describing a problem may result in them making collaborative suggestions for potential solutions.

## **The Nutshell Message**

***Using a distributed denial of service (“DDoS”) attack, determined professional miscreants can take you, or virtually any other networked site, “off the Internet” for as long as they want -- or at least make you work very hard in order to stay on.***

*Notes:*

- 1) Feel free to publicly dispute this... Personally, I don't believe in taunting hackers or challenging folks to demonstrate that they can take a site down -- I'm perfectly willing to just stipulate that they probably can do so, instead, saving us both the trouble of a pointless (and really unnecessary) proof-by-demonstration.*
- 2) I'm also willing to stipulate that with substantial effort you might be able to make a given site “DDoS resistant,” but I don't believe that even five percent of Internet2 sites have done so.*

## **“Huh? What's A ‘Distributed Denial of Service Attack?’”**

- In a distributed denial of service attack, network traffic from thousands of hacked computer systems -- often systems located all over the Internet -- gets used in a coordinated way to overwhelm a targeted network or computer, thereby preventing it from doing its normal work. For example:
  - the institution's connection or connections to the Internet may be made to overflow with unsolicited traffic (a so-called "packet flood")
  - web servers may be inundated with hundreds of thousands of malicious repeated requests for web pages
  - campus name servers may become so swamped that university computer users have problems visiting either local web sites or web sites on the Internet

# Resisting the Geek Temptation

- This is the point where you might be tempted to start explaining about IRC command and control channels, and SYN attacks vs. directed broadcast attacks vs. ...
- Resist the temptation. Part of the problem with DDoS is that it really is a family of attacks, rather than a single vulnerability, and it is easy to get tied up in the details.
- For the executive audience, the key thing is not how distributed denial of service attacks work, but rather what distributed denial of service attacks can do.
- Stay “on message.”



## Effects of a DDoS:

- The systems and networks that are the target of the distributed denial of service attacks are still there and haven't been hacked or compromised, BUT they are too overloaded to do useful work.
- An attack that is targeting a single server or desktop can have collateral damage against an entire site, at least to the extent that infrastructure (such as a common Internet connection) is shared.
- When a denial of service attack stops or is abated, the targeted system or systems are usually able to rapidly resume normal operation; lingering direct effects should be minimal or non-existent.
- Regrettably, blocking or abating one DDoS usually will not prevent another one from occurring.

## By Way Of Analogy...

- We're all familiar with "DoS attacks" in real life...
  - Vandals may insert foreign material in a keyhole or coin slot, thereby preventing a door from being opened or a vending machine from being used,
  - Picketers may temporarily block access to a facility,
  - Bomb threats may get called in by a terrorist.
- Unfortunately network DDoS attacks tend to be on a whole different scale, are able to be launched from virtually anywhere, and potentially can disrupt far more people, for a far longer period of time.

# **Now, With A Casual Understanding of the Problems, Solutions Often Get Suggested**

- People, including senior administrators, like to make sure that their staff haven't missed something obvious... as a result, once they've learned about a problem like DDoS attacks, they may suggest some possible solutions...

# "So What's The Big Deal? Why Don't You Guys Just Block The Problematic Traffic?"

- It's trickier to just block the problematic traffic than you might think for a variety of reasons. For example:

-- If your regular Internet (and/or Internet2) connection is being flooded with inbound traffic, you need to block it upstream, BEFORE it can traverse the last network links into your university. If you just try to filter the traffic at your campus border, well, it's too late at that point – your inbound network pipe will still be unusably full.

Filtering traffic upstream requires the cooperation of your upstream network service provider (NSP), and some NSPs may have limited engineering staff devoted to dealing with DDoS attack-related issues.

## **" "What's The Big Deal? Why Don't You Guys Just Block The Problematic Traffic?" (cont.)**

- The miscreant DDoS'ing you may have an army of tens of thousands (or hundreds of thousands of compromised hosts)... and the hosts he's using may constantly change. The sheer mechanics of filtering that many sources can be technically challenging -- for example, some routers and other network hardware may be unable to handle large filter lists and significant network traffic loads
- You need to separate the "baby from the bathwater:" attack traffic may be indistinguishable from legitimate traffic.
- Attempts to limit particular types of traffic (e.g., total UDP traffic) may break fundamental and/or advanced applications (DNS, IP multicast, etc.)
- Attackers may change their attack mechanism over time, adapting their attack to overcome blocks you put into place.

## "How About This: What If We Treat It Like A Blizzard, And Just Plan to 'Ride It Out?'"

- While there is a certain insouciance to the idea of having "denial-of-service days" (sort of like more traditional "snow days"), executives should understand that denial of service attacks can be sustained for days -- or even weeks or more -- at a time. For example, Spamhaus, a major anti-spam activist organization, was subject to an attempted denial of service attack that lasted for **three months**.

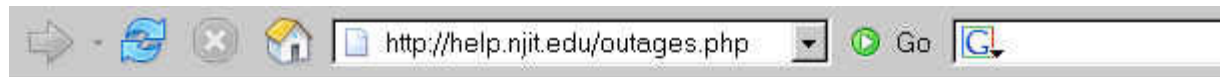
(See <http://www.spamhaus.org/news.lasso?article=13> )

Taking an entire denial-of-service term off would have material impacts on a university's ongoing operations, and probably would simply be unacceptable.

# "Let's Just Disconnect For a While"

- While disconnecting from the Internet would certainly insure that attack traffic coming from the Internet cannot DoS university systems and would allow-intra-campus operations to resume, disconnecting entirely is itself a form of self-imposed “denial of service,” and would likely not be well received by campus constituents.
- In the case of inbound DDoS attacks targeting a particular non-mission critical host, disconnecting that single host may be a pragmatically viable strategy...
- Likewise, in cases where compromised hosts are being used to generate outbound flows, disconnecting those compromised hosts will almost always be the right thing to do (unless you're trying to collect live forensic evidence for prosecution)

# Example of Taking a DDoS Target Offline



1/25

**NJIT was the object of a Distributed Denial of Service (DDoS) attack this morning. This began at approximately 9:40 AM and lasted until approximately 10:30 AM. During this time all Internet connectivity was unavailable or highly intermittent. The destination of this DDoS attack was/is the research IRC server run by the IS department. Connectivity to this server will be unavailable until further notice.**



# University of Chicago: An Outgoing DDoS Host Gets Taken Offline



**December 4, 2005**

Campus Commodity Internet connectivity was degraded beginning at approximately 9:45pm on Friday, December 3 and restored to normal at 10:35am, Saturday December 4.

The problem was reported to network engineering at 9am Saturday. The cause of the problem was a compromised host generating an outgoing denial of service attack. The compromised host was removed from the network.

# "Call the FBI and Let Them Sort It All Out."

- The FBI and other law enforcement (LE) officials will typically be interested in major DDoS attacks resulting in \$50K or more in damages, however their attention will not provide symptomatic relief when a DoS occurs, nor is it a guarantee of a successful investigation and eventual prosecution – DDoS cases are hard to put together.
- You should also understand that many times denial of service attacks are transnational, which raises special investigatory issues, requires LE coordination with foreign counterparts, and can introduce investigative delays.
- Denial of service attacks committed by individuals overseas (and attacks made by minors whether here in the US or abroad), if able to be successfully prosecuted, may yield rather abbreviated sentences. That fact may dampen LE enthusiasm for proceeding with a potentially hard-to-investigate, hard-to-prosecute, “low-payoff” case.

# Netherlands: 5 Day DDoS; 38 Day Sentence...

Original URL: [http://www.theregister.co.uk/2005/03/16/dutch\\_hackers\\_sentenced/](http://www.theregister.co.uk/2005/03/16/dutch_hackers_sentenced/)

---

## Dutch hackers sentenced for attack on government sites

---

By [Jan Libbenga](#) (libbenga at yahoo.com)

Published Wednesday 16th March 2005 08:54 GMT

Five computer hackers in the Netherlands have been handed sentences ranging from work orders to youth detention for disabling a number of websites operated by the Dutch government.

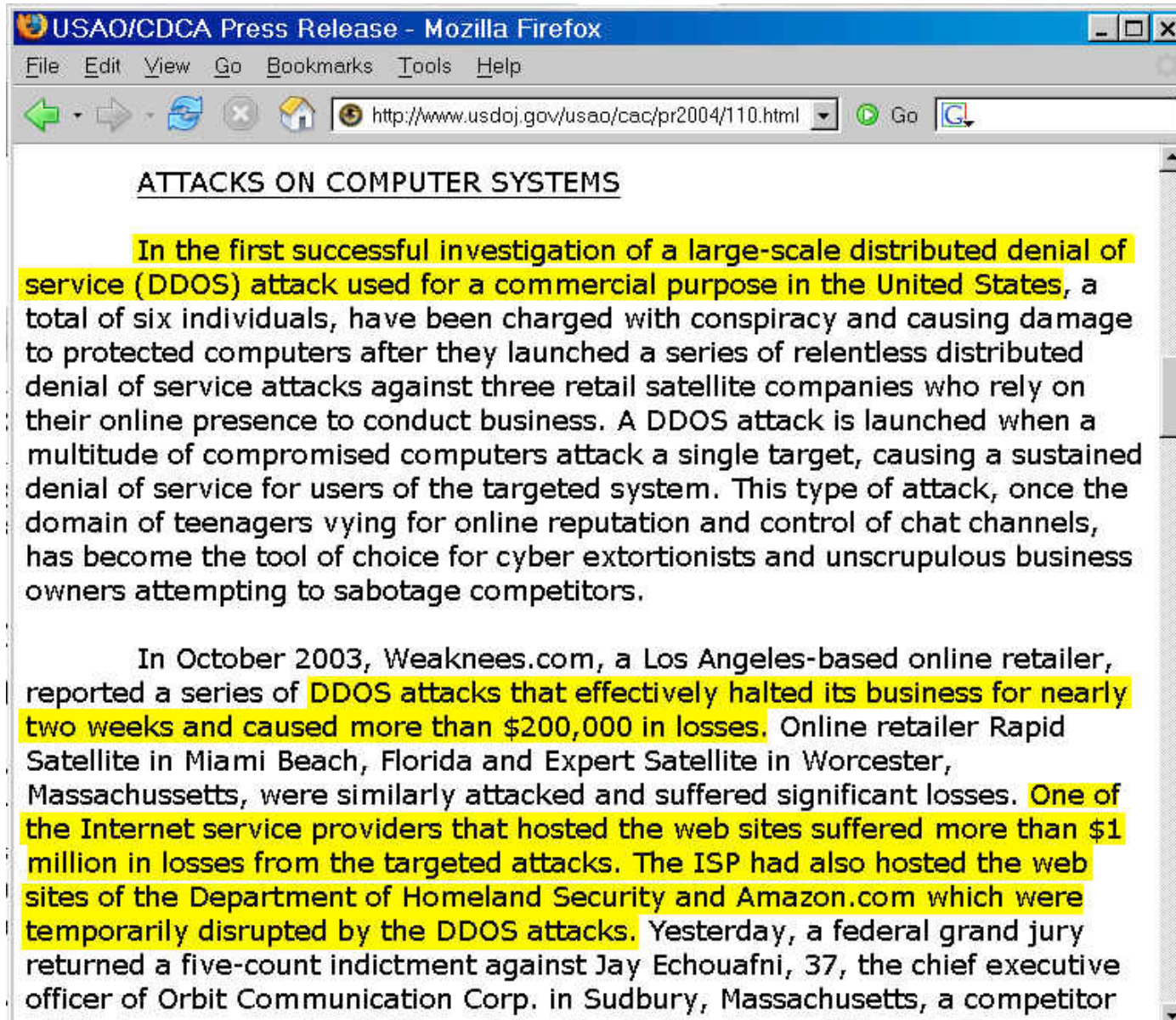
A group of around 15 hackers, who called themselves '0x1fe Crew', carried out a Distributed Denial of Service (DDoS) attack last year on the government websites [overheid.nl](#) and [regering.nl](#) in a protest against recent cabinet proposals. The group claimed cabinet members were its sole targets. The websites, the central gateway to all information on cabinet policy in the Netherlands, couldn't be reached for five days.

The Dutch government immediately launched legal proceedings against the group and this week five hackers were convicted. The main suspect, who was given a 38-day detention sentence, says he will appeal. The 18-year-old claims there is no technical proof of his participation in the attacks. "They sentenced me because I was the spokesman for the group," he told news site *Webwereld*.

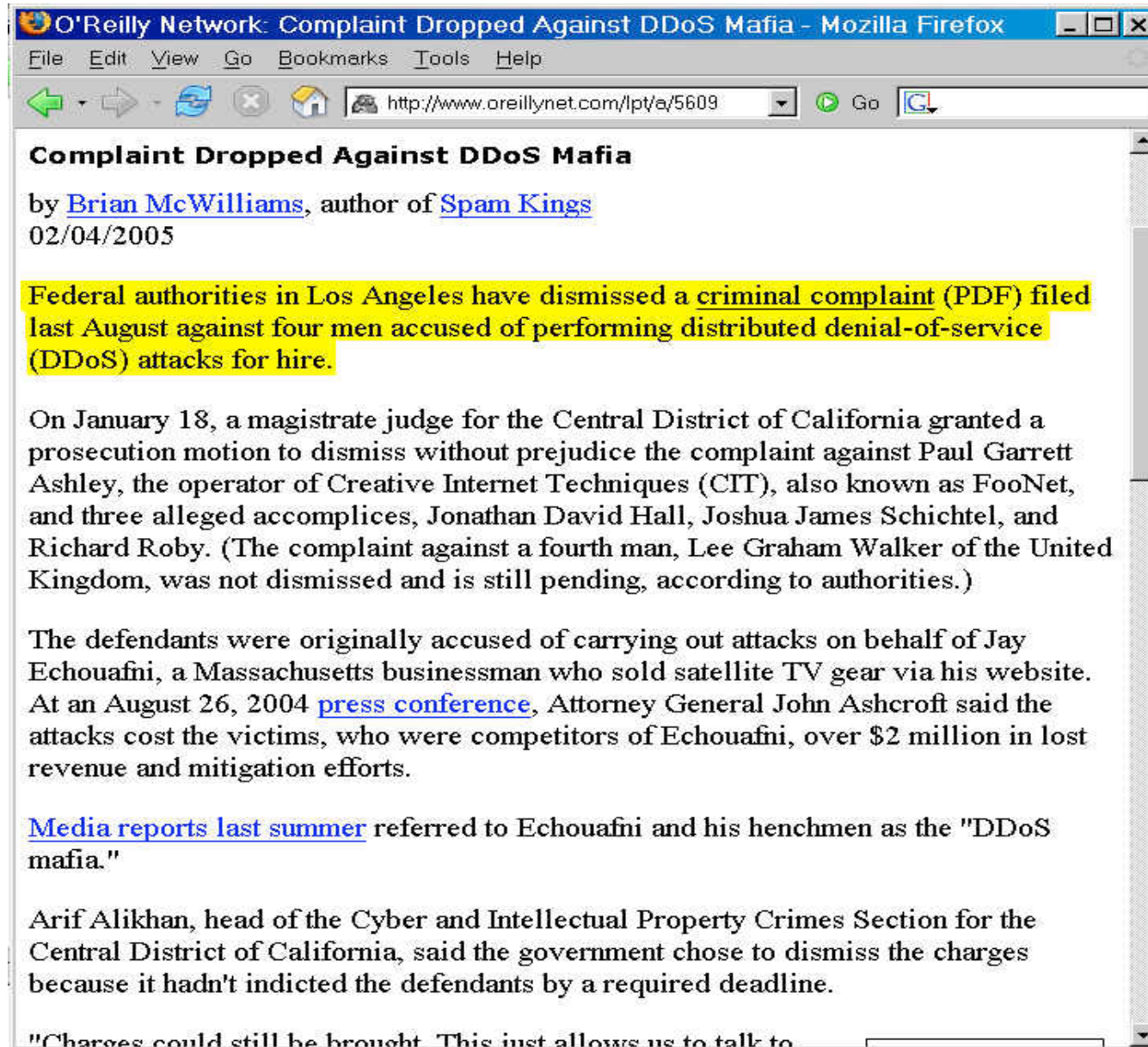
It is first time in the Netherlands that anyone has been convicted for such an attack.



# First Successful US Investigation of a DDoS



# ... Dismissed (for now)



O'Reilly Network: Complaint Dropped Against DDoS Mafia - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.oreillynet.com/lpt/a/5609

## Complaint Dropped Against DDoS Mafia

by [Brian McWilliams](#), author of [Spam Kings](#)  
02/04/2005

Federal authorities in Los Angeles have dismissed a criminal complaint (PDF) filed last August against four men accused of performing distributed denial-of-service (DDoS) attacks for hire.

On January 18, a magistrate judge for the Central District of California granted a prosecution motion to dismiss without prejudice the complaint against Paul Garrett Ashley, the operator of Creative Internet Techniques (CIT), also known as FooNet, and three alleged accomplices, Jonathan David Hall, Joshua James Schichtel, and Richard Roby. (The complaint against a fourth man, Lee Graham Walker of the United Kingdom, was not dismissed and is still pending, according to authorities.)

The defendants were originally accused of carrying out attacks on behalf of Jay Echouafni, a Massachusetts businessman who sold satellite TV gear via his website. At an August 26, 2004 [press conference](#), Attorney General John Ashcroft said the attacks cost the victims, who were competitors of Echouafni, over \$2 million in lost revenue and mitigation efforts.

[Media reports last summer](#) referred to Echouafni and his henchmen as the "DDoS mafia."

Arif Alikhan, head of the Cyber and Intellectual Property Crimes Section for the Central District of California, said the government chose to dismiss the charges because it hadn't indicted the defendants by a required deadline.

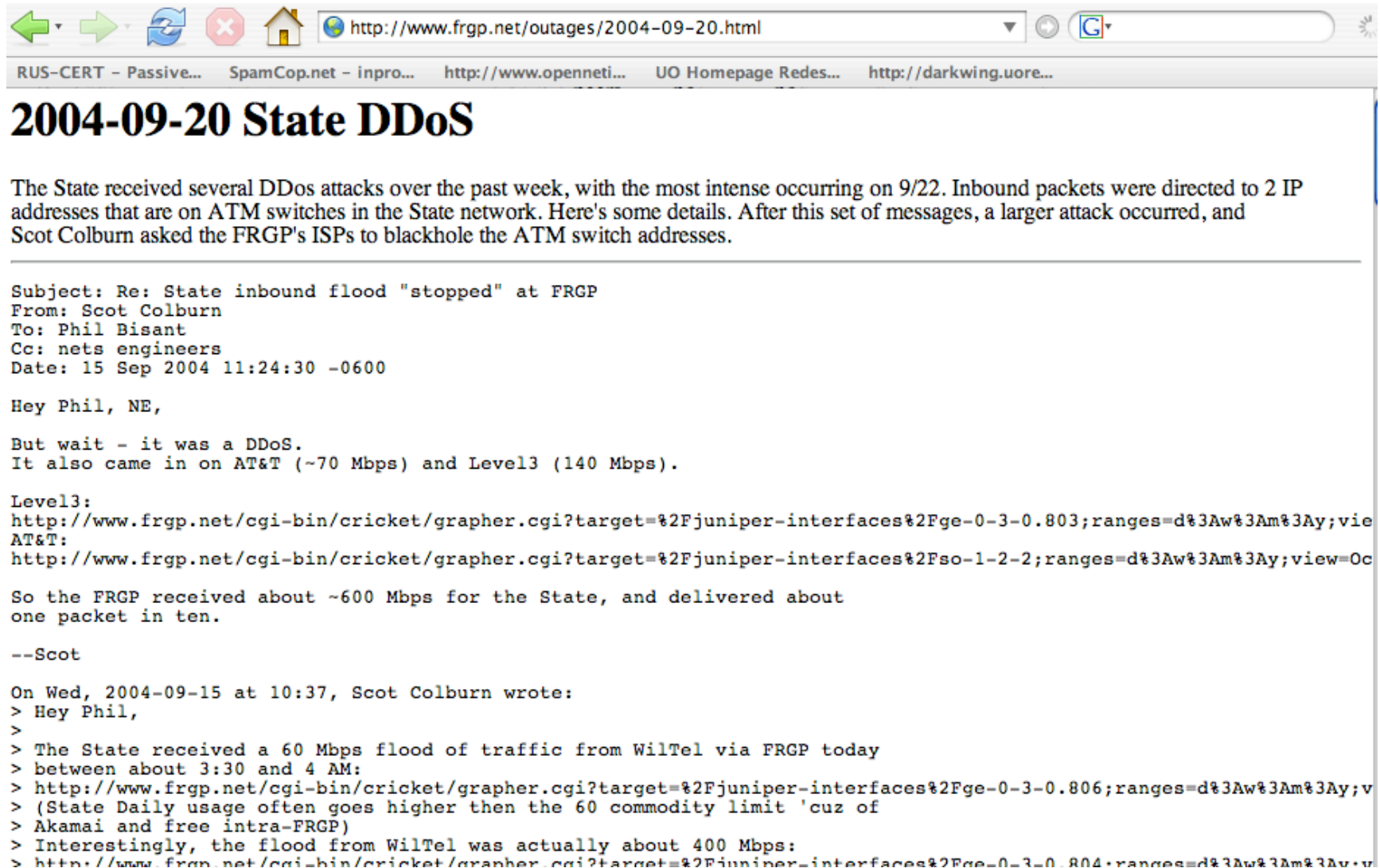
"Charges could still be brought. This just allows us to talk to

## **"Are Internet2 Universities Really at Risk?"**

- Everyone on the Internet is vulnerable to denial of service attacks, which obviously includes Internet2 universities and gigapops.
- As "proof by example," if you Google around a little, it isn't hard to find examples of Internet2 universities or gigapops that have been hit with denial of service attacks...



# Front Range



The screenshot shows a web browser window with the address bar displaying <http://www.frgp.net/outages/2004-09-20.html>. The browser's tab bar shows several open tabs, including "RUS-CERT - Passive...", "SpamCop.net - inpro...", "http://www.openneti...", "UO Homepage Redes...", and "http://darkwing.uore...". The main content area of the browser displays a news article titled "2004-09-20 State DDoS". The article text describes a DDoS attack on the State network, mentioning that inbound packets were directed to two IP addresses on ATM switches. It also mentions that Scot Colburn asked the FRGP's ISPs to blackhole the ATM switch addresses. The article includes a quoted email from Scot Colburn to Phil Bisant, dated September 15, 2004, at 11:24:30 -0600. The email discusses the DDoS attack, mentions Level3, and provides two URLs for the FRGP's cricket/grapher.cgi script. The email also mentions that the FRGP received about 600 Mbps for the State and delivered about one packet in ten. The email ends with a signature from Scot Colburn. The article also includes a quote from Scot Colburn dated Wednesday, September 15, 2004, at 10:37, where he discusses the DDoS attack on the State network, mentioning that it was a 60 Mbps flood of traffic from WilTel via FRGP today, between about 3:30 and 4 AM. He also mentions that the FRGP's commodity limit is 60 Mbps, and that the flood from WilTel was actually about 400 Mbps.

**2004-09-20 State DDoS**

The State received several DDos attacks over the past week, with the most intense occurring on 9/22. Inbound packets were directed to 2 IP addresses that are on ATM switches in the State network. Here's some details. After this set of messages, a larger attack occurred, and Scot Colburn asked the FRGP's ISPs to blackhole the ATM switch addresses.

---

Subject: Re: State inbound flood "stopped" at FRGP  
From: Scot Colburn  
To: Phil Bisant  
Cc: nets engineers  
Date: 15 Sep 2004 11:24:30 -0600

Hey Phil, NE,

But wait - it was a DDoS.  
It also came in on AT&T (~70 Mbps) and Level3 (140 Mbps).

Level3:  
<http://www.frgp.net/cgi-bin/cricket/grapher.cgi?target=%2Fjuniper-interfaces%2Fge-0-3-0.803;ranges=d%3Aw%3Am%3Ay;vie>  
AT&T:  
<http://www.frgp.net/cgi-bin/cricket/grapher.cgi?target=%2Fjuniper-interfaces%2Fso-1-2-2;ranges=d%3Aw%3Am%3Ay;view=Oc>

So the FRGP received about ~600 Mbps for the State, and delivered about one packet in ten.

--Scot

On Wed, 2004-09-15 at 10:37, Scot Colburn wrote:  
> Hey Phil,  
>  
> The State received a 60 Mbps flood of traffic from WilTel via FRGP today  
> between about 3:30 and 4 AM:  
> <http://www.frgp.net/cgi-bin/cricket/grapher.cgi?target=%2Fjuniper-interfaces%2Fge-0-3-0.806;ranges=d%3Aw%3Am%3Ay;v>  
> (State Daily usage often goes higher then the 60 commodity limit 'cuz of  
> Akamai and free intra-FRGP)  
> Interestingly, the flood from WilTel was actually about 400 Mbps:  
> <http://www.frgp.net/cgi-bin/cricket/grapher.cgi?target=%2Fjuniper-interfaces%2Fge-0-3-0.804;ranges=d%3Aw%3Am%3Ay;v>

# University of Alaska-Anchorage

http://technology.uaa.alaska.edu/kb/Incident\_Reports/04\_20\_05\_Network\_Outage.cfm    Go

---

## 04\_20\_05\_Network\_Outage

Article Number: 5772

**Start Date and Time:** 4/20/2005 12:00pm  
**End Date and Time:** 4/20/2005 5:30pm  
**Duration:** 5 Hours 30 Minutes

**Current Status:** Open, All systems available

**Severity:** Major

**Systems Affected:** UAA/Statewide Network Access

**Customer Impact:** UAA Internal/External Network Customers

**Description:**  
A few minutes prior to noon yesterday, the Anchorage campus network was severely impacted by a denial of service, or DOS attack. This happens when a heavy, uninterrupted stream of network traffic is directed at a specific network device which connects our (or any other organization's) network to the global Internet. The sustained stream of traffic causes core switching equipment to become so busy handling this traffic that it cannot transport legitimate network traffic thus creating the denial of service.

UAA engineers isolated the problem at approximately 3pm yesterday and returned on-campus network operations by 4pm. Final engineering changes to our core switching equipment permitted re-connection of the Anchorage campus network to the UA wide-area network by approximately 6pm. Engineers have monitored traffic levels overnight and are working with Statewide network operations to investigate the source of the attack which appears to be located on the Fairbanks campus.

The outage created immediate loss of all enterprise campus services – including email, directory services, Blackboard and Internet access. As mentioned above, on-campus service was restored around 4pm but many off-campus users were left without service until early evening. Internet Service Providers (ISPs) are frequently the targets of DOS attacks as are major corporations and organizations.

At the moment, every effort is being taken to identify the source of the attack, neutralize it and make adjustments to our core switching equipment to minimize the effects of future attacks of this type. Thanks for your patience in this matter. I will keep you all



# University of Houston



<http://www.stp.uh.edu/vol69/76/news/news4.html>

## **Denial-of-service attack disrupted Web access Friday**

**Cougar News Staff**

The UH System experienced a computer network outage Friday during which Internet users at all System universities had difficulty connecting to UH servers.

The problem affecting numerous outbound ports, which began around 10 a.m., was caused by a denial-of-service attack that originated from an on-campus high performance computing lab, Information Technology reported Friday.

"Denial of service is an Internet thing where some entity or person tries to flood traffic into the network connection, which denies users' connections," Dennis Fouty, associate vice president for Central Computing & Telecommunication Services, said.

Normal Internet access was restored by 8:15 p.m. Friday, IT reported.

# University of Tennessee-Chattanooga

← → ↻ × 🏠 <http://raven.utc.edu/cgi-bin/WA.EXE?A2=ind0402&L=utinfo&F=&S=&P=4152> Go

**Date:** Tue, 10 Feb 2004 08:21:14 -0500  
**Reply-To:** Monty Wilson <monty-wilson@utc.edu>  
**Sender:** UTC Campus Information <UTCINFO@RAVEN.UTC.EDU>  
**From:** [Monty Wilson <monty-wilson@utc.edu>](mailto:monty-wilson@utc.edu)  
**Organization:** UTC  
**Subject:** Denial of Service Attack on UTC Network  
**Content-Type:** text/plain; charset="us-ascii"

Currently the UTC access to the Internet is under a massive denial of service attack. This attack has made access to the Internet extremely limited. The Network Staff is working with the Internet Service Provider to resolve this attack as quickly as possible. Since this is an external attack, on campus email should continue to work. We will update the list as new developments occur.

Monty Wilson  
University of Tennessee at Chattanooga  
Assistant Vice Chancellor Information Technology

# Those Sites Are In Pretty Good Company

- I don't want you to think that being the victim of a denial of service is some sort of evidence of gigapop or campus level issues, because it's not.
- In fact, those three example universities are in excellent company when it comes to being targeted for denial of service attacks...

# Yahoo, Google, MSN Have Been Hit...

## Blackout hits major Web sites

By Jim Hu

[http://news.com.com/Blackout+hits+major+Web+sites/2100-1038\\_3-5234500.html](http://news.com.com/Blackout+hits+major+Web+sites/2100-1038_3-5234500.html)

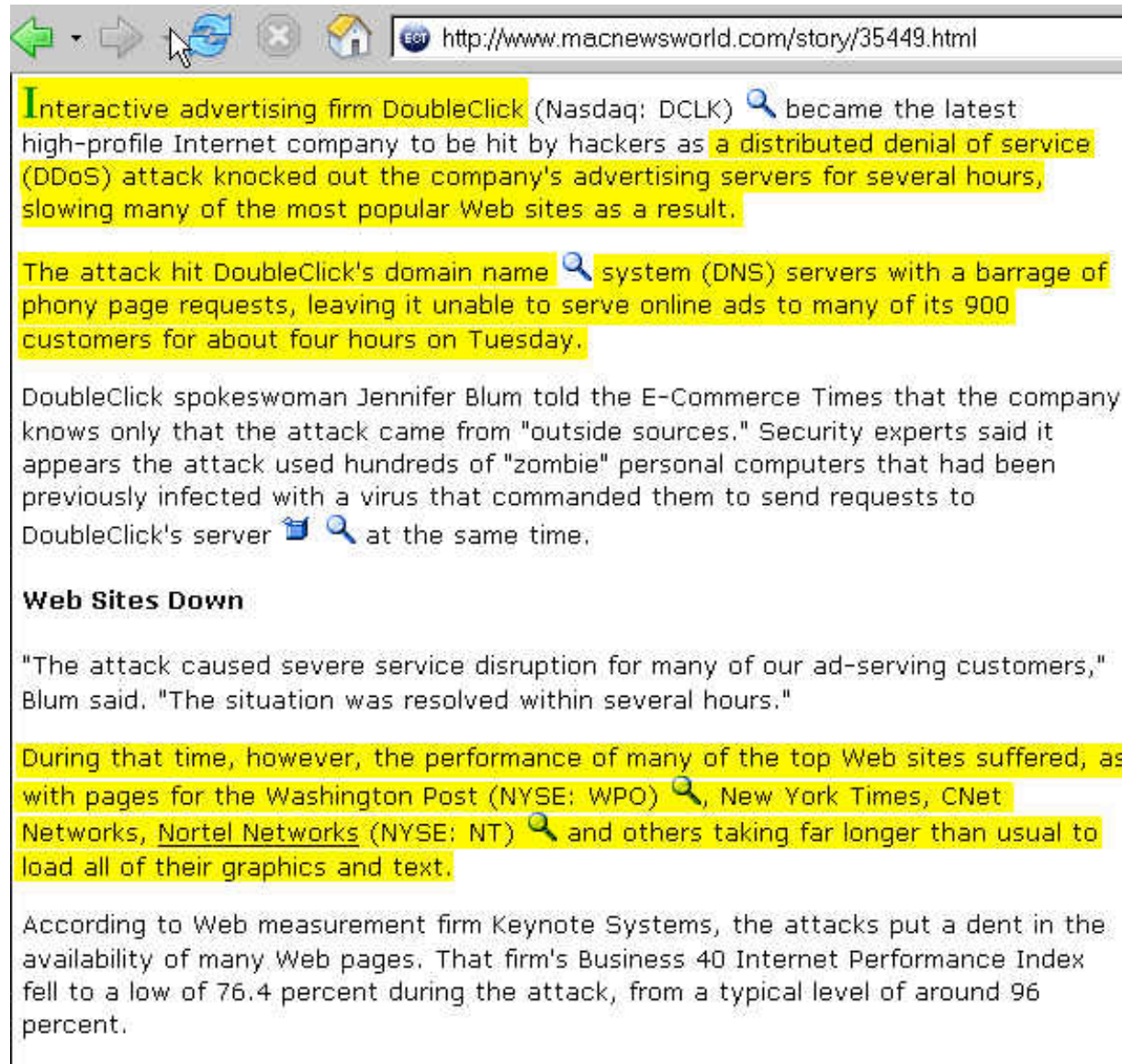
Story last modified Tue Jun 15 15:01:00 PDT 2004

**A domain name outage Tuesday morning that left many popular Web sites, including those of Yahoo, Google, Microsoft and Apple, temporarily inaccessible was the result of an Internet attack, according to Web infrastructure company Akamai.**

The attack caused problems for more than two hours--from 5:30 a.m. to 7:45 a.m. PDT. Many of the world's most popular sites suffered from widespread outages, according to [Keynote Systems](#), which compiles statistics related to Web surfing. On a typical day, the top 40 sites measured by Keynote rarely dip below 99 percent availability. On Tuesday, however, Keynote saw availability drop to 81 percent.



# Internet Advertising Companies Have Been Hit...



The screenshot shows a web browser window with the address bar displaying <http://www.macnewsworld.com/story/35449.html>. The main content area features a news article with several paragraphs. The first paragraph is highlighted in yellow and reads: "Interactive advertising firm DoubleClick (Nasdaq: DCLK) became the latest high-profile Internet company to be hit by hackers as a distributed denial of service (DDoS) attack knocked out the company's advertising servers for several hours, slowing many of the most popular Web sites as a result." The second paragraph is also highlighted in yellow and reads: "The attack hit DoubleClick's domain name system (DNS) servers with a barrage of phony page requests, leaving it unable to serve online ads to many of its 900 customers for about four hours on Tuesday." The third paragraph is not highlighted and reads: "DoubleClick spokeswoman Jennifer Blum told the E-Commerce Times that the company knows only that the attack came from 'outside sources.' Security experts said it appears the attack used hundreds of 'zombie' personal computers that had been previously infected with a virus that commanded them to send requests to DoubleClick's server at the same time." Below this is a section header "Web Sites Down" followed by a quote from Blum: "The attack caused severe service disruption for many of our ad-serving customers," Blum said. "The situation was resolved within several hours." The next paragraph is highlighted in yellow and reads: "During that time, however, the performance of many of the top Web sites suffered, as with pages for the Washington Post (NYSE: WPO), New York Times, CNet Networks, Nortel Networks (NYSE: NT) and others taking far longer than usual to load all of their graphics and text." The final paragraph is not highlighted and reads: "According to Web measurement firm Keynote Systems, the attacks put a dent in the availability of many Web pages. That firm's Business 40 Internet Performance Index fell to a low of 76.4 percent during the attack, from a typical level of around 96 percent."

Interactive advertising firm DoubleClick (Nasdaq: DCLK) became the latest high-profile Internet company to be hit by hackers as a distributed denial of service (DDoS) attack knocked out the company's advertising servers for several hours, slowing many of the most popular Web sites as a result.

The attack hit DoubleClick's domain name system (DNS) servers with a barrage of phony page requests, leaving it unable to serve online ads to many of its 900 customers for about four hours on Tuesday.

DoubleClick spokeswoman Jennifer Blum told the E-Commerce Times that the company knows only that the attack came from "outside sources." Security experts said it appears the attack used hundreds of "zombie" personal computers that had been previously infected with a virus that commanded them to send requests to DoubleClick's server at the same time.

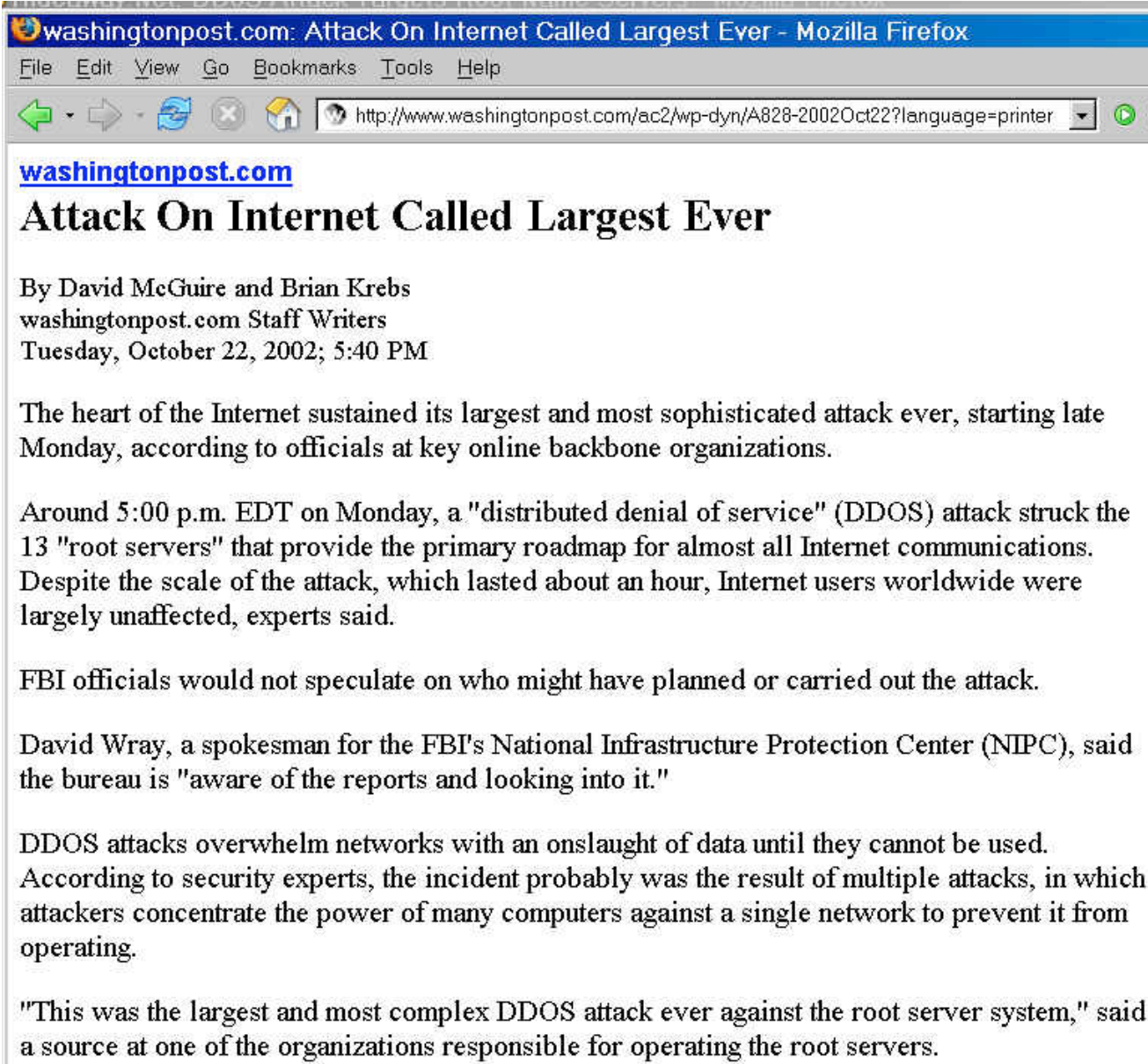
### Web Sites Down

"The attack caused severe service disruption for many of our ad-serving customers," Blum said. "The situation was resolved within several hours."

During that time, however, the performance of many of the top Web sites suffered, as with pages for the Washington Post (NYSE: WPO), New York Times, CNet Networks, Nortel Networks (NYSE: NT) and others taking far longer than usual to load all of their graphics and text.

According to Web measurement firm Keynote Systems, the attacks put a dent in the availability of many Web pages. That firm's Business 40 Internet Performance Index fell to a low of 76.4 percent during the attack, from a typical level of around 96 percent.

# Internet DNS Root Servers Have Been Hit...



The screenshot shows a Mozilla Firefox browser window with the title bar "washingtonpost.com: Attack On Internet Called Largest Ever - Mozilla Firefox". The address bar displays the URL "http://www.washingtonpost.com/ac2/wp-dyn/A828-2002Oct22?language=printer". The page content includes the Washington Post logo, the article title "Attack On Internet Called Largest Ever", the authors "By David McGuire and Brian Krebs", their affiliation "washingtonpost.com Staff Writers", and the date "Tuesday, October 22, 2002; 5:40 PM". The article text describes a "distributed denial of service" (DDOS) attack on 13 "root servers" that provide the primary roadmap for almost all Internet communications. It mentions that the attack lasted about an hour and that Internet users worldwide were largely unaffected. The article also notes that FBI officials would not speculate on who might have planned or carried out the attack. David Wray, a spokesman for the FBI's National Infrastructure Protection Center (NIPC), said the bureau is "aware of the reports and looking into it." The article further explains that DDOS attacks overwhelm networks with an onslaught of data until they cannot be used, and that the incident was the result of multiple attacks, in which attackers concentrate the power of many computers against a single network to prevent it from operating. Finally, a source at one of the organizations responsible for operating the root servers is quoted as saying, "This was the largest and most complex DDOS attack ever against the root server system."

washingtonpost.com

## Attack On Internet Called Largest Ever

By David McGuire and Brian Krebs  
washingtonpost.com Staff Writers  
Tuesday, October 22, 2002; 5:40 PM

The heart of the Internet sustained its largest and most sophisticated attack ever, starting late Monday, according to officials at key online backbone organizations.

Around 5:00 p.m. EDT on Monday, a "distributed denial of service" (DDOS) attack struck the 13 "root servers" that provide the primary roadmap for almost all Internet communications. Despite the scale of the attack, which lasted about an hour, Internet users worldwide were largely unaffected, experts said.

FBI officials would not speculate on who might have planned or carried out the attack.

David Wray, a spokesman for the FBI's National Infrastructure Protection Center (NIPC), said the bureau is "aware of the reports and looking into it."

DDOS attacks overwhelm networks with an onslaught of data until they cannot be used. According to security experts, the incident probably was the result of multiple attacks, in which attackers concentrate the power of many computers against a single network to prevent it from operating.

"This was the largest and most complex DDOS attack ever against the root server system," said a source at one of the organizations responsible for operating the root servers.

# Amazon, CNN, eBay, eTrade, etc. Have Been Hit...



It's small comfort to the high-tech industry that the 16-year-old perpetrator of last February's incidents, a Canadian hacker nicknamed Mafiaboy, last month pled guilty to single-handedly attacking Amazon. com Inc., eBay, Yahoo, Charles Schwab & Co., CNN and eTrade, among others.

Mafiaboy carried out his distributed denial-of-service spree using attack tools available on the Internet that let him launch a remotely coordinated blitz of IP packets from servers compromised by agent attack "zombies." Mafiaboy awaits sentencing, but it's expected he won't get much more than two years in a juvenile detention center.

Those attacks forced most of the victimized e-commerce sites offline for about three hours. In the heat of battle to block the blitz of IP packets, ISPs did what they could through filtering bad traffic and claimed victory when it ended. But security experts familiar with what occurred agree that this filtering accomplished little and that relief came because Mafiaboy simply stopped his attacks after three-hour intervals.

# DDoS Attacks Can Hit Anyone

- No one is immune from DDoS attacks. That's why it is important to spend some time thinking about this issue now, before you get hit by a denial of service attack.



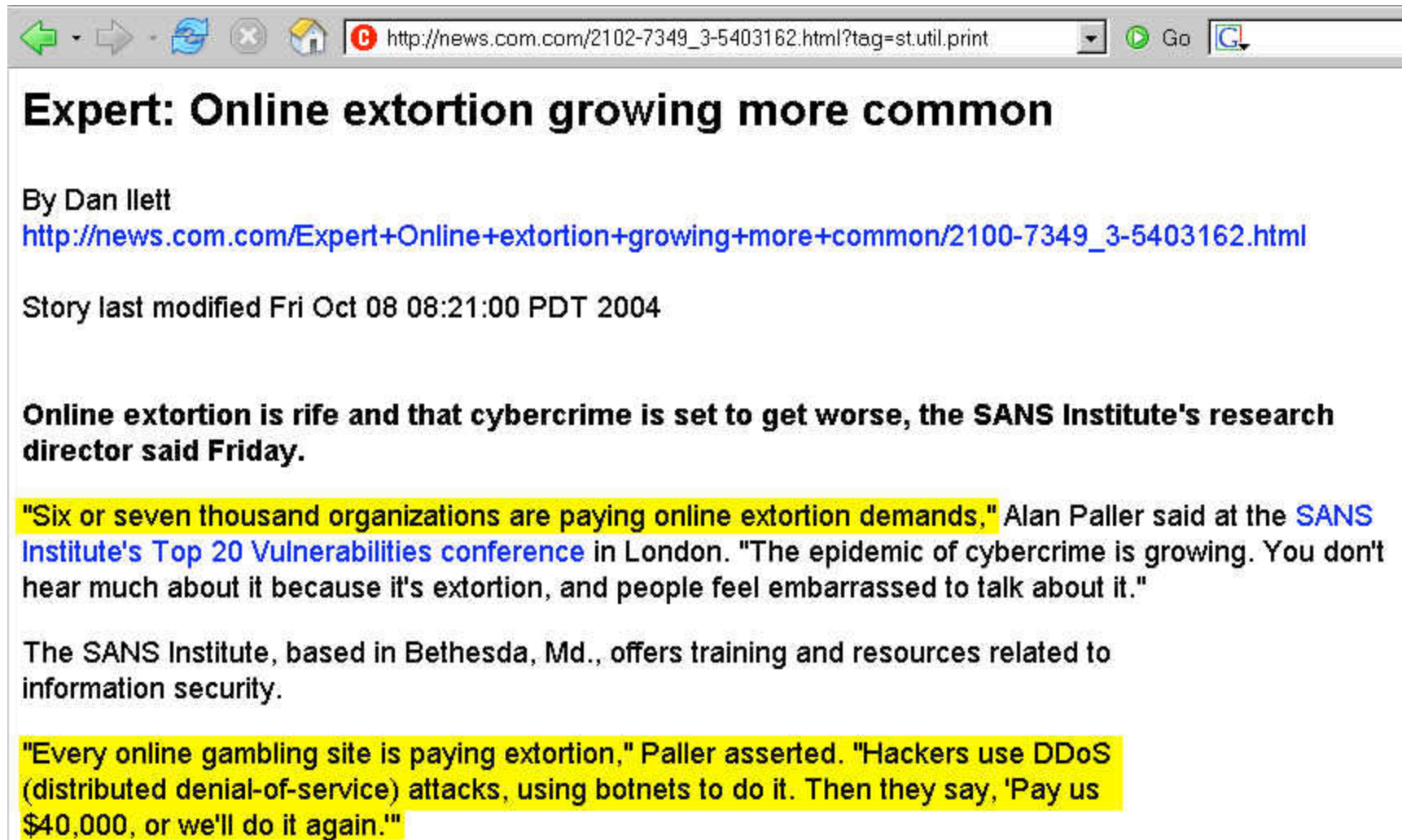
# What Motivates DDoS Attacks?

- ***Extortion:*** *some sites are hit with DDoS attacks if they refuse to pay "protection money"*
- **Direct Action:** in other cases, a DDoS may be designed to directly accomplish a particular task, such as rendering a particular internet service unusable (example: a DDoS targeting an anti-spam DNSBL site)
- **Revenge:** other sites may DDoS'd as an act of revenge for an actual or perceived slight or act of disrespect
- **Ideology:** a site may be targeted for a denial of service because it is associated with particular political, religious, cultural or philosophical beliefs
- **Notoriety:** because DDoS's are often very newsworthy, engaging in a DDoS attack can be one way of attempting to garner publicity or call attention to an cause

# What Motivates DDoS Attacks? (cont.)

- **Peer Recognition/Social Status** – some attackers may not care about general publicity, but may be highly motivated by approval and recognition from smaller “in” groups such as miscreant clans.
- **Design Errors:** Some denial-of-service-like attacks are simply the result of design errors in legitimate consumer hardware; this can result in what amounts to a real denial of service attack, albeit an unintentional one.
- **Simple Problems of Scaling to Internet Size Audiences:** Similarly, mere mention of a sufficiently interesting web site on a popular news site such as slashdot.org can be sufficient to “DDoS” some sites...
- Let's briefly consider a couple of those motives...

# DDoS Extortion Rackets



The screenshot shows a web browser window with a grey title bar and a standard toolbar. The address bar contains the URL [http://news.com.com/2102-7349\\_3-5403162.html?tag=st.util.print](http://news.com.com/2102-7349_3-5403162.html?tag=st.util.print). The main content area displays a news article titled "Expert: Online extortion growing more common" by Dan Ilett. The article text discusses the prevalence of online extortion, citing a SANS Institute conference and mentioning DDoS attacks on gambling sites.

**Expert: Online extortion growing more common**

By Dan Ilett  
[http://news.com.com/Expert+Online+extortion+growing+more+common/2100-7349\\_3-5403162.html](http://news.com.com/Expert+Online+extortion+growing+more+common/2100-7349_3-5403162.html)

Story last modified Fri Oct 08 08:21:00 PDT 2004

**Online extortion is rife and that cybercrime is set to get worse, the SANS Institute's research director said Friday.**

"Six or seven thousand organizations are paying online extortion demands," Alan Paller said at the [SANS Institute's Top 20 Vulnerabilities conference](#) in London. "The epidemic of cybercrime is growing. You don't hear much about it because it's extortion, and people feel embarrassed to talk about it."

The SANS Institute, based in Bethesda, Md., offers training and resources related to information security.

"Every online gambling site is paying extortion," Paller asserted. "Hackers use DDoS (distributed denial-of-service) attacks, using botnets to do it. Then they say, 'Pay us \$40,000, or we'll do it again.'"

# **“Why Would Anyone Pay An Extortionist?”**

- Extortionists may preface their discussions by providing a brief convincing demonstration of their capabilities.
- Complaining to law enforcement authorities may result in limited immediate symptomatic relief.
- Inhouse staff and/or upstream providers may demonstrate a limited ability to technically help.
- The cost of paying the extortionist may be less than the cost of hardening the network and systems to resist the attack, or less than the cost of business lost if the DDoS does occur; they may simply be “running the numbers.”
- Obviously, paying up is a really bad idea (if only because extortion is illegal under the Hobbs Act, 18 USC 1951), extortionate demands may continually escalate, and by paying you may be encouraging/inspiring others to try it)

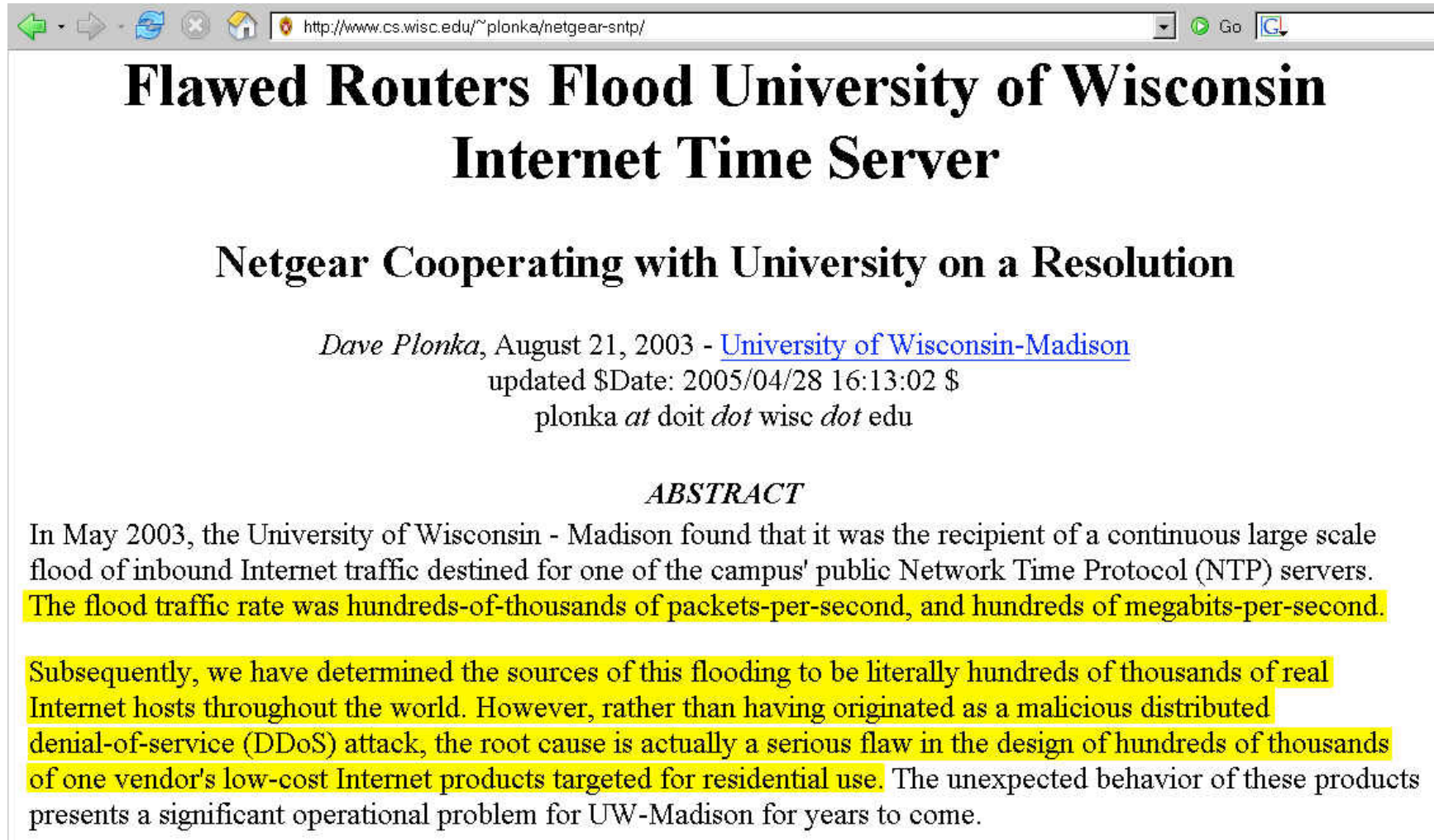
# Is Higher Education An Attractive Target For DDoS-Enforced Extortion Attempts?

- Imagine a threatened DDoS attack during a crucial time, such as during a prime window for students to submit applications for admission – how many of us now rely on online applications for a significant proportion of our matriculating class? How tight is that window? Do you routinely send out printed backup application materials?
- Or maybe you have closely defined windows for students to enroll in classes via an online portal -- what would the impact be if your enrollment system was offline for half a day or a day during peak registration times? Or how long could you continue to function without access to your institutional teaching and learning system? Or your administrative ERP system?
- I think higher education IS vulnerable to DDoS extortion.

# **“I’m Skeptical About The Extortion Thing”**

- Okay, take the extortion scenario off the table. Are there other reasons why people might want to DDoS you?
- For example, have you had to deal with student P2P file sharing issues, perhaps as a result of RIAA or MPAA DMCA complaints? Were those students feeling happy? Or maybe you had to discharge an employee recently -- was he or she disgruntled at being terminated?
- Does your university do scientific testing using animals, or undertake defense-related research work, or do anything else that might serve as a “lightning rod” for an online act of protest?
- Heck, sometimes a site may get DoS’d accidentally, when something as obscure as a networked university time server ends up getting used in unexpected ways...

# Example of an Unintentional Design Error "DDoS"



The screenshot shows a web browser window with the address bar displaying `http://www.cs.wisc.edu/~plonka/netgear-sntp/`. The main content of the page is a document titled "Flawed Routers Flood University of Wisconsin Internet Time Server" with a subtitle "Netgear Cooperating with University on a Resolution". The author is listed as "Dave Plonka, August 21, 2003 - [University of Wisconsin-Madison](http://www.cs.wisc.edu/~plonka/netgear-sntp/)" and the date is "updated \$Date: 2005/04/28 16:13:02 \$". The document includes an "ABSTRACT" section that describes a DDoS attack on the University of Wisconsin-Madison's NTP servers in May 2003, caused by a design flaw in Netgear routers.

**Flawed Routers Flood University of Wisconsin Internet Time Server**

**Netgear Cooperating with University on a Resolution**

*Dave Plonka, August 21, 2003 - [University of Wisconsin-Madison](http://www.cs.wisc.edu/~plonka/netgear-sntp/)*  
updated \$Date: 2005/04/28 16:13:02 \$  
plonka at doit dot wisc dot edu

**ABSTRACT**

In May 2003, the University of Wisconsin - Madison found that it was the recipient of a continuous large scale flood of inbound Internet traffic destined for one of the campus' public Network Time Protocol (NTP) servers. The flood traffic rate was hundreds-of-thousands of packets-per-second, and hundreds of megabits-per-second.

Subsequently, we have determined the sources of this flooding to be literally hundreds of thousands of real Internet hosts throughout the world. However, rather than having originated as a malicious distributed denial-of-service (DDoS) attack, the root cause is actually a serious flaw in the design of hundreds of thousands of one vendor's low-cost Internet products targeted for residential use. The unexpected behavior of these products presents a significant operational problem for UW-Madison for years to come.

# Reasons Aside, The Outcome's The Same

- Regardless of the reason for a flood of traffic that's acting as a denial of service -- extortion, revenge, unintentional design error or something else, the outcome's the same: as the target of what is (or what amounts to) a denial of service attack, a university system or network may be rendered unusable.
- Stay on message, focus on the outcome of a DDoS.



# That May Be Enough for An Initial Meeting

- You will have functionally defined the DDoS problem, explaining how a DDoS can affect university operations
- You will have continued to discuss some of the unique characteristics that make dealing with online denial of service attacks difficult
- You will have overcome the audience's temptation to go into denial by showing them that real universities are getting hit (as are best-of-breed Internet properties)
- You will have explored at least a few possible reasons for DDoS attacks (extortion, revenge and simple inadvertent design errors).
- **At the end of that meeting, you might be charged with an action item: “Figure out what we should do about this DDoS thing, and then let’s meet again.”**

# **Figuring Out What Your Campus Should Do**

# Starting With Your Own Staff

- The agenda for your meeting with your staff probably needs to cover at least four areas:
  - 1) review what was shared with campus senior leaders,
  - 2) talk about how your campus will identify DDoS attacks,
  - 3) talk about campus strategies for DDoS mitigation, and
  - 4) conclude by talking about opportunities for collaborative action against DDoS attacks – including making sure that your own hosts don't participate in DDoS attacks.

## **==> DDoS Identification**

- Ironically, one of the hardest problems you may initially face is simply identifying and confirming that an attack is going on....
- Some institutions may have limited formal network monitoring in place, and as a result the first indication that "something's wrong" may be user complaints.
- In other cases, you may have monitoring in place, but some outbound attacks may fall below the “threshold of materiality” for I2 schools with large pipes. You may not notice a couple of Mbps attack, but a business living at the end of a skinny pipe (like a frame relay T1) sure will!
- In other cases, hopefully in MOST cases, you WILL have formal networking monitoring in place, including an intrusion detection system monitoring network traffic for attack attempts.
- One clear challenge is avoiding “false positives.”

# A Spike In Traffic Isn't Always a DoS Attack

- Once your staff begins to suspect that something is wrong, differential diagnosis of a DoS attack will require them to first rule out some other possibilities.

For example, could it be that systems or networks are simply experiencing higher-than-normal real loads?

Particularly in the Internet2 community, remember that substantial effort has been expended on developing high performance networked applications that may “fairly-but-fully” utilize available network capacity. Real apps may \*look like\* a DOS attack, but you should not reward successful end-to-end performance experiments, appropriately done by legitimate users, with summary disconnection from the network!

# **“Normal” Failures**

- You also need to carefully exclude the possibility that systems are unavailable simply because a “normal” failure has occurred. Systems and interfaces will die from time to time, fiber will accidentally get backhoe’d, and unprotected power may be interrupted. Obviously none of those failures are DDoS attacks.

“When you hear hoofbeats, look for horses, not elk, first.”

Be vigilant, but don’t be paranoid. Not everything is a DDoS attack.

# Where Was Degraded Performance Seen?

- -- Was degraded performance seen on a single server?
  - A set of servers all running a single particular app?
  - One particular subnet?
  - Across all of campus?
  - Across the entire Internet (or at least across all of Internet2)? See <http://isc.sans.org/> or, for Internet2, see <http://ren-isac.net/monitoring.cgi>
- -- On smaller networks, you may be able to informally localize the affected areas.
  - On larger networks, help desk ticketing summaries or real time systematic performance monitoring with tools like Nagios may help you do troubleshooting and problem extent isolation.

# **When Was Traffic Seen? DDoS Timing**

- Can we tell when the DDoS started? Is the DDoS still going on?
- Is it continuous, or intermittent?
- Graphical SNMP-based traffic representations produced by tools such as MRTG or RRDtool may help you tease out attack timing issues.



# Digging In

- Now that you've localized where and when the attack occurred, [maybe] your staff can begin to dig in.
- Is flow-level ("Netflow") data available for the relevant part of campus for the intervals of interest?
- Are current or retrospective packet-level traffic samples (or at least SYNs) available for review?
- Are staff members seeing IDS event reports?
- Of course, if you don't have solid network monitoring infrastructure deployed, it may be hard for you to do some or all of those things.
- **Suggested action item for your staff: review your campus system and network monitoring and IDS infrastructure now, before you need access to this data for DDoS-related purposes.**

# What About Commercial DDoS ID Tools?

- There are excellent commercial DDoS identification tools that will help to automate the process of identifying and characterizing DDoS attack traffic, however those tools may be prohibitively expensive for ubiquitous deployment, although obviously prices may change over time, particularly as market demand ramps up and competitive pressures increase.

## **==> DDoS Mitigation**

- ***“DDOS DEFENSE CHALLENGE :The seriousness of the DDoS problem and the increased frequency, sophistication and strength of attacks have led to the proposal of numerous defense mechanisms. Yet, although many solutions have been developed, the problem is hardly tackled, let alone solved.”***

“A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” Jelena Mirkovic and Peter Reiher,  
<http://www.cis.udel.edu/~sunshine/publications/ccr.pdf>

# All DDoS Attacks Aren't 'One Single Animal'

- It is important to recognize that there are many different types of DDoS attacks, and mitigating one type of DDoS attack may require completely different steps than would be required for another type.
- For example, a denial of service attack that targets a vulnerability in a particular operating system or application may be best handled by insuring that that O/S or application gets suitably patched.
- Similarly, if you have a host that is participating in an outbound attack on another site, “mitigation” may be a synonym for “disconnecting that host from the network.”
- What, however, can we do about distributed denial of service attacks that are manifested as massive traffic floods?

# Mitigating Traffic-Flooding DDoS Attacks

- Mitigating a traffic-flooding distributed denial of service attack is usually a collaborative process of filtering or diverting that traffic, and will usually involve your institution's networking staff working with your Gigapop or Abilene engineers, your commodity ISP's engineers and security staff, etc.

# Directly Sinking Attack Traffic Via Blackhole Communities

- In some cases, provision may be made for downstream customers to self-tag routes with blackhole community values following the process outlined at <http://www.secsup.org/CustomerBlackHole/> or as discussed in more detail at <http://www.nanog.org/mtg-0410/pdf/soricelli.pdf>  
This approach allows attack traffic to be blackholed by a targeted site in an efficient fashion, as close to the attack source as possible.
- If your provider does not support this sort of direct approach, you're looking at spending time on the phone with them to arrange for manual creation of blackhole routes when you're under attack. That's not so hot.
- **Suggested Action Item For Your Staff: Do our providers support blackhole communities? If so, do you know what values to use if you need them?**

# I2 and Some Gigapops Are Already Doing This, As Are Some Carriers

- BGP Communities in Abilene  
<http://www.abilene.iu.edu/bgpcommun.html>
- Calren BGP Blackhole Communities  
<http://www.cenic.net/operations/documentation/CalREN%20BGP%20Blackhole%20Comm.pdf>
- SprintLink's BGP Policy  
<http://www.sprint.net/policy/bgp.html>
- UUNet  
<http://www.merit.edu/mail.archives/nanog/2004-03/msg00078.html>
- XO  
<http://www.xo.com/products/smallgrowing/internet/dia/features/BGPpolicy.pdf>

# Ingress Filtering

- Another example of a concrete step that you can take which can help ameliorate at least one class of denial of service attack is ingress filtering, as documented in BCP 38. See: <http://www.faqs.org/ftp/bcp/bcp38.txt>
- **Action item: have your staff verify that your site is following the best common practices documented in BCP 38.**



# Remember QoS?

- I don't want to leave you with the impression that blackholing or ingress filtering are the only approach people have suggested for dealing with DDoS attacks. For example, those of you who were really sad when QoS fell off the collective consciousness of Internet2 may take heart -- QoS has come up yet again, this time in the context of mitigating DoS attack traffic. See for example:

“Mitigating Network DoS Attacks,”

Packet, Vol 16 #1, Q1 2004

( [http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/about\\_cisco\\_packet\\_issue\\_home.html](http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/about_cisco_packet_issue_home.html) )

- And there are others (but we won't go into them now).

## **==> Collaborating With Others**

- There are tremendous opportunities for collaborative effort with respect to distributed denial of service attacks.
- Obviously the process of a carrier blackholing traffic upstream from a target customer is one concrete example of how collaboration can make a difference, but there are other opportunities where collaboration can help your institution prepare to deal with the DDoS threat.

# Networking (People, Not Wire, Style)

- Do your network engineers and security staff know the Abilene engineers (and your commodity ISP's engineers and security staff?) If not, this might be something to work on rectifying BEFORE a DoS attack occurs.
- Internet2 Joint Tech Meetings tend to provide a natural forum for meeting and interacting with Internet2 technical staff, and NANOG may be a suitable forum for your engineers to learn who's-who when it comes to operational network security at major commodity network service provider. NANOG presentations often include network security-related topics. Do your technical staff members attend these meetings?
- **Action item: Make sure technical staff gets involved with the operational network security community.**

# If Staff Travel To Meetings Is Impossible...

- If technical staff can't go to Joint Techs or NANOG, you should at least encourage them to take advantage of mailing lists and talks available free of charge on the Internet. Some excellent DDoS/Bot related talks include:
  - Hank Nusbacher's "DDoS: Undeniably a Global Internet Problem Looking for a Global Solution,"  
<http://www.interall.co.il/presentations/ripe41.pdf>
  - Honeynet's "Know Your Enemy: Tracking Botnets"  
<http://www.honeynet.org/papers/bots/>
  - John Kristoff's botnets talk from NANOG 32  
<http://aharp.ittns.northwestern.edu/slides/botnets.pdf>
  - Peter Moody's botnets talk from the SLC Joint Techs  
<http://www.internet2.edu/presentations/jtsaltlake/20050214-Botnets-Moody.pdf>
  - Additional resources:  
<http://www.honeypots.net/incidents/ddos-mitigation>

# Other Opportunities to Collaborate

- Arbor's DDoS Fingerprint Sharing Alliance  
( <http://www.arbor.net/fingerprint-sharing-alliance.php> )
- Bleeding Snort ( <http://www.bleedingsnort.com/> )
- Drone Armies / Botnet Research and Mitigation Mailing List (contact [gadi@tehila.gov.il](mailto:gadi@tehila.gov.il) or [gadi@CERT.gov.il](mailto:gadi@CERT.gov.il))
- Educause Security Task Force  
[http://www.educause.edu/content.asp?SECTION\\_ID=30](http://www.educause.edu/content.asp?SECTION_ID=30)
- FIRST (<http://www.first.org/> )
- InfraGard ( <http://www.infragard.net/> )
- Internet2 Security Initiatives  
(<http://security.internet2.edu/>)
- NSP-SEC (see: <http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-nspbof-nsp-sec.pdf> )

# Looking at Anti-DDoS Vendors

- Sometimes you'd just like to work with a vendor, buying a commercial solution to help deal with a problem like DDoS attacks.
- There are many different vendors who will be happy to collaborate with you in the anti-DDoS space. A couple of them include:
  - Arbor Networks (an Internet2 Corporate Sponsor, and long time collaborator with Internet2 on traffic anomaly detection and mitigation)
  - Cisco (an Internet2 Corporate Partner, and a company which has recently signaled increased interest in the anti-DDoS space by buying Riverhead for \$39M)

# Making Sure Your Own Hosts Don't Participate in DDoS Attacks

- A few basic steps include:
  - watch outbound (as well as inbound) traffic for issues
  - insure that your hosts are patched up to date, and are running antivirus/antispymware software, and are using a software (or personal hardware) firewall
  - consider scanning campus hosts with Nessus, etc.
  - install anti-spoofing filters on each subnet and your border router (Cisco has a nice anti-DDoS suggestion page: [www.cisco.com/warp/public/707/newsflash.html](http://www.cisco.com/warp/public/707/newsflash.html) )
  - make sure your contact information is current for your domain, your IP address block, and your ASN whois information; you should also have both RFC2142-required [abuse@<domain>](mailto:abuse@<domain>) and [security@<domain>](mailto:security@<domain>) contact addresses, and those addresses should be read

# **Thanks For The Chance to Talk Today!**

- Are there any questions?