

Fighting Cyber Crime in the Telecommunications Industry

Sachi Chakrabarty



Agenda

- Cyber Crime
- What's all the fuss about CyberCrime ?
- DoS Attacks
- Telco Solutions

Cybercrime ?

Cybercrime



- **Definition**
All criminal offences which are committed with the aid of, or targeted at, communication devices in a network. Eg.: the Internet, the telephone line or the mobile network.
- In information security there are very real threats, and the main threat is crime
- Cybercrime is just like any other type of crime only with different tactics

Types/techniques of Cyber Crimes



- Spam
- Identity Theft
- Cyber fraud
- Phishing
- Extortion
- Bot/Botnets
- Malware
- DoS/DDoS
- Etc.

Emergency Response



- The public have grown used to stories about identity theft, hacking, stolen data and they're no longer shocked into action when they hear about it.
- Familiarity breeds contempt which is good news for criminals because the public stops being on its collective guard.
- But what if there was a way of a network being able to predict the next attack, a network that could detect even the smallest of threats and self-correct to avoid an attack?

How big is the problem, and who are the perpetrators

Sustained Attack Size – Gbps

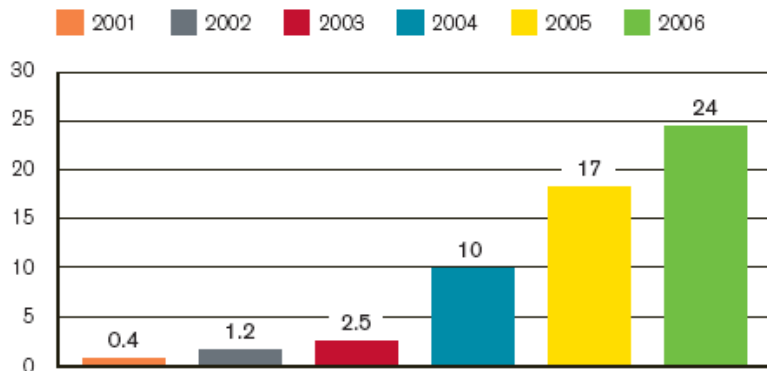


Figure 1: Sustained Attack Size – Gbps

Source: Arbor Networks, Inc.

Attack Targets

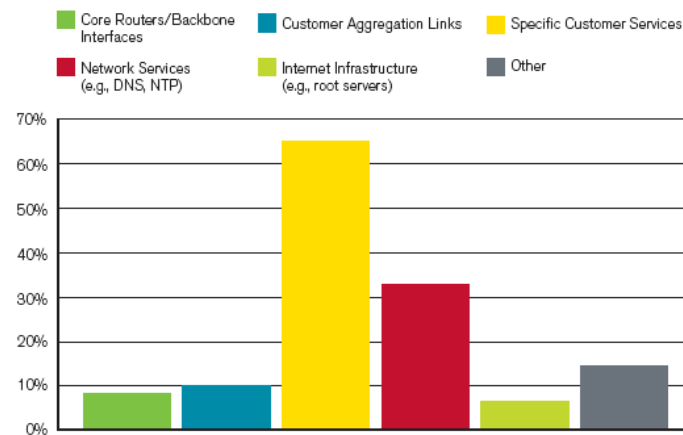


Figure 9: Attack Targets

Source: Arbor Networks, Inc.

■ From notoriety to eCrime

- Originally hackers and 'script kiddies' seeking headlines and notoriety
- Now moved to extortion and organised crime (Russian mafia and highly organised criminal gangs) - Botnets for hire
- Revenue from eCrime greater than narcotics
- eCrime difficult to investigate

Russia

cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Search this site

Go

Go to...

[Special report: Russia](#)[Russia archived articles](#)

In this section

[Putin names long-term ally as new PM](#)[Russia unveils the 'father of all bombs'](#)[Russians given day off work to make babies](#)[Putin dissolves government ahead of elections](#)[Rostropovich art hits high note at auction house](#)[RAF scrambles to confront Russian bombers as Putin](#)**Ian Traynor in Brussels****Thursday May 17, 2007****[The Guardian](#)**

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

While Russia and Estonia are embroiled in their worst dispute since the collapse of the Soviet Union, a row that erupted at the end of last month over the Estonians' removal of the Bronze Soldier Soviet war memorial in central Tallinn, the country has been subjected to a barrage of cyber warfare, disabling the websites of government ministries, political parties, newspapers, banks, and companies.



Bronze Soldier, the Soviet war memorial removed from Tallinn. Photograph: Timur Nisametdinov/AP

Article continues ▾

Guardian Unlimited

LISTEN TO OUR RUGBY

- Home
- News**
- News By Industry
 - Auto
 - Cons. Products
 - Energy
 - Healthcare / Biotech
 - Finance / Insurance
 - Ind'l Goods / Svs
 - Infotech**
 - Hardware
 - Software
 - Internet & Telecom
 - TeS
 - Media / Entertainment / Art
 - Services
 - Telecom
 - Transportation
- Companies A-Z
- Politics/Nation
- International Business
- Economy
- Most Read Articles
- Multimedia
- Money Matters**
- Mutual Funds
- Insurance
- Savings Centre
- Loan Centre
- Credit Cards
- Tax Centre
- Markets**
- Real Estate
- Stocks
- Forex
- Debt / Money
- Commodities

Cyber crime mafia plays hell with cos

RITVIK DONDE & THANUJA BM
 TIMES NEWS NETWORK [MONDAY, JUNE 25, 2007 12:01:14 AM]
 [Blocked Ads]
 MUMBAI/BANGLORE: The US-based retailer and owner of TJ Maxx stores TJX saw nearly 40 million customer records being hacked into, and by the time the company came to know of this, most of the details were already up on sale on a few e-commerce websites. TJX is not alone. In early 2003, a Russian-hackers' extortion network shut down Grafix Softech which hosted 120 gambling sites around the world, by planting botnets in its systems.

Multibet.com in Australia received similar digital threats just two years ago. When its CEO refused, the company was attacked four times and his business was interrupted for 20 days until he wired the protection money to a Latvian bank account. Another band of new age hackers demanded \$40,000 from BetCris, another gambling portal in 2003.

"The cyber crime industry is the new-age mafia, it is even bigger than the illegal drug industry" says David Spenhoff, vice-president at anti-virus maker Trend Micro. What used to be attempts to earn five minutes of fame in the cyber world has undergone tremendous transformation. Over the past two to three years, the attack pattern has changed completely.

Earlier, an attacker used to be a prying programmer who wanted to make a name for himself in the cyber world. Today hackers like Gary McKinnon are passé. McKinnon

Reach out to millions of buyers
 Get instant response.
 List your property NOW!

I want to: Sell Rent
 Property Type: ---Select Type---
 Bathrooms: ---Select---
 City: ---Select City---
 Bedrooms/ BHK: ---Select---

List Now
 More Details

magicbricks.com
 — India's No.1 Property Site —

[Blocked Ads]

Cyber Crime is the new-age mafia, it is even bigger than the illegal drugs industry.

Reach out to

Feel the pain – Do you want to be in the news ?

TIMES ONLINE

NEWS COMMENT BUSINESS SPORT LIFE & STYLE ARTS & ENTERTAINMENT DRIVING

UK | WORLD | POLITICS | WEATHER | TECH & WEB | RELATED REPORTS |

Where am I? > Home > NEWS > Tech & Web

From Times Online

May 22, 2007

Telegraph website targeted in mystery attack by hackers

Jonathan Richards

The Daily Telegraph website has been the victim of a mystery and destructive attack by hackers that has blocked access to the site over the last 24 hours.

The paper confirmed that its site had been the victim of a 'distributed denial of service attack' (DDoS), and that many readers had not been able to log on since yesterday morning.

A third party team of experts was still working to return systems to normal, following what the paper described as "an act of vandalism".

"With these things it's always difficult to know what might be behind it," a Telegraph spokeswoman said.

RELATED LINKS

> Putin accused of launching cyber war

The paper had not received any threats demanding that particular stories be removed, the spokeswoman said, but a "revenge attack" was one of the possible

EXPLORE TECH & WEB

- > PERSONAL TECH
- > GADGETS & GAMING
- > THE WEB

TIMES RECOMMENDS

- > Google Street View privacy row
- > How many tech writers does it take to set up a wi-fi network?
- > Jobs and Gates bury the hatchet

MOUSETRAP WEBLOG



bbc.co.uk home

TIMES ONLINE

WSJ.com THE WALL STREET JOURNAL ONLINE



Ryan Naraine

Tracking the hackers

February 16th, 2007

Massive DDoS attack KO's CastleCops

Posted by Ryan Naraine @ 7:34 pm

Categories: Browsers, Rootkits, Spam and Phishing, Spyware and Adware, Botnets, Exploit code,

Viruses and Worms

Tags: Phishing, Distributed Denial Of Service, Ryan Naraine



Worthwhile? +22
24 VOTES

The anti-phishing community at CastleCops.com has been knocked out by a massive DDoS (distributed denial-of-service attack).

The volunteer-driven site, which is run by the husband and wife team of Paul and Robin Laudanski, had been coping with on-and-off attacks since February 13 but an intense wave that began around 3:45 PM EST today completely crippled the server capacity.



At 10:15 PM, despite industry-wide efforts at mitigation, CastleCops.com was still displaying a "Site Temporarily Unavailable" message.

"They got whacked real hard today. It was so strong that it knocked their ISP over," said a source involved in the scramble to mitigate the attack.

Law enforcement authorities are involved in the ongoing investigations.

CastleCops.com just celebrated its [fifth anniversary](#) as a high-profile anti-malware community. In partnership with Sunbelt Software, CastleCops.com runs the Phishing Incident Reporting and Termination (PIRT) Squad.

SKY NEWS

Firms hit rivals with web attacks

May 4, 2007

Legitimate businesses are turning to cyber criminals to help them cripple rival websites, say security experts.

The rise in industrial sabotage comes as some suggest cyber criminals are turning away from using web-based attacks.

Experts suspect this is because of the risks involved in mounting such an attack on a web shop or retailer.

Instead the tools, usually hijacked home computers, are being used to pump out junk e-mail.

Cash call

Often these hijacked PCs, known as bots, are used for "Distributed Denial of Service" (DDoS) attacks that attempt to knock

Online gambling sites were among the first to be threatened with DDoS attacks if they did not hand over significant sums

In a recent entry on the Symantec Security Response blog, Yazan Gable said the company had seen a "pretty sharp decline

Mr Gable said this was because extortion attacks were no longer profitable because knocking a website offline via DDoS

Many of those controlling the networks of bot computers have now started using them to send out spam which was just

But Paul Sop, chief technology officer at Prolexic which helps victims cope with DDoS attacks, said they were proving as

"We've seen more DDoS attacks in the last few months than we have ever seen," he said.

The decline could just be part of the arms race between criminals and security firms.

"When the gangs feel the pincers coming in they change their strategy," he said.

There was no reason to think the decline was because such attacks were no longer profitable. Not least, he said, because

"Once they have you hooked they'll keep going," he said, "it can get up to some pretty serious numbers."

Mr Sop said the number of extortion-based attacks had declined a little but this had been more than made up for by cor

"We are seeing a lot of anti-competitive behaviour," he said.

Mr Sop added that many more Asian targets were being hit by DDoS attacks - a region in which Symantec did not histor

In Asia, he said, DDoS attacks were proving very popular with unscrupulous firms keen to get ahead of their rivals.

What's all the fuss about DOS Attacks?

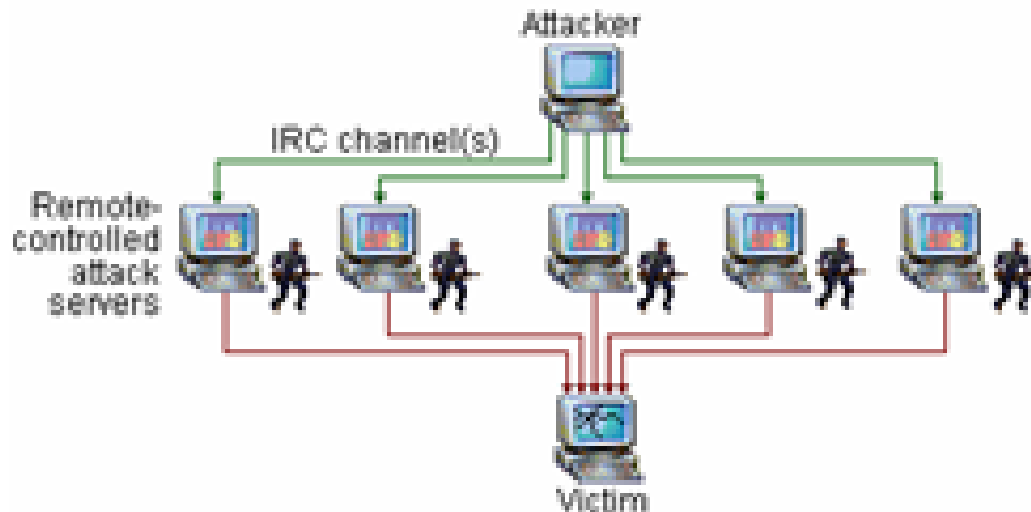
Distributed Denial of Service Attacks – What and How?

DOS is the deliberate denial of a service or services.

- DOS is not an attempt to penetrate systems, to steal or alter data.
- The attacker seeks to render a system inoperative, while keeping his identity secret.

DDOS is a DOS attack launched from multiple sources.

- Launching an attack from multiple sources increases the potency of the attack and makes the task of tracing the source more difficult.



Who is the target?

Question: Who is a DOS target ?.

Answer: Any connected addressable device. Some targets are more likely, Governments, organisations, prominent companies, controversial companies or researchers, sporting bodies etc. But in essence anybody can fall victim.

Question: Are there any specific sectors at risk?

Answer: Online businesses – retail, gambling, government, ISP's Banking, Utilities and Business to business

Question: Are there any Compelling Events?

Answer: Organisations might be targeted on particular events Big events e.g. gambling site when it's the Grand National. "Rebellions" against Government web sites

Question: What happens?

Answer: Ultimately bring the web site down which results in lost revenue, loss of goodwill i.e. customers can't get on the site. Impact third party organisations e.g. B2B sites

Frequently Attacked Targets

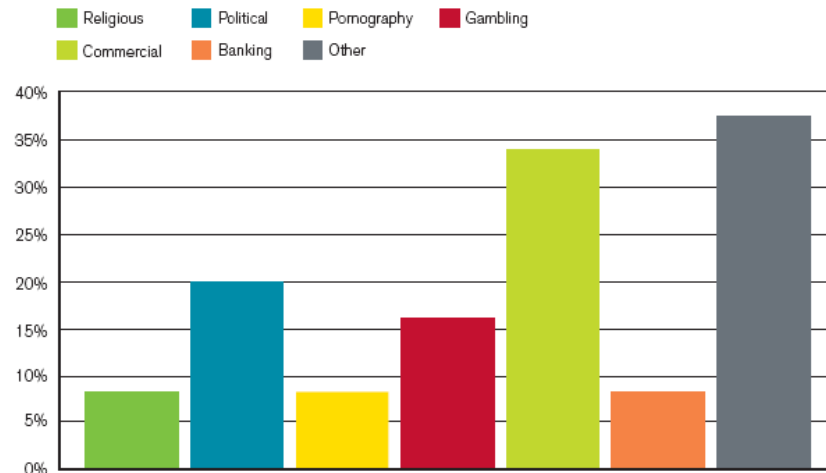


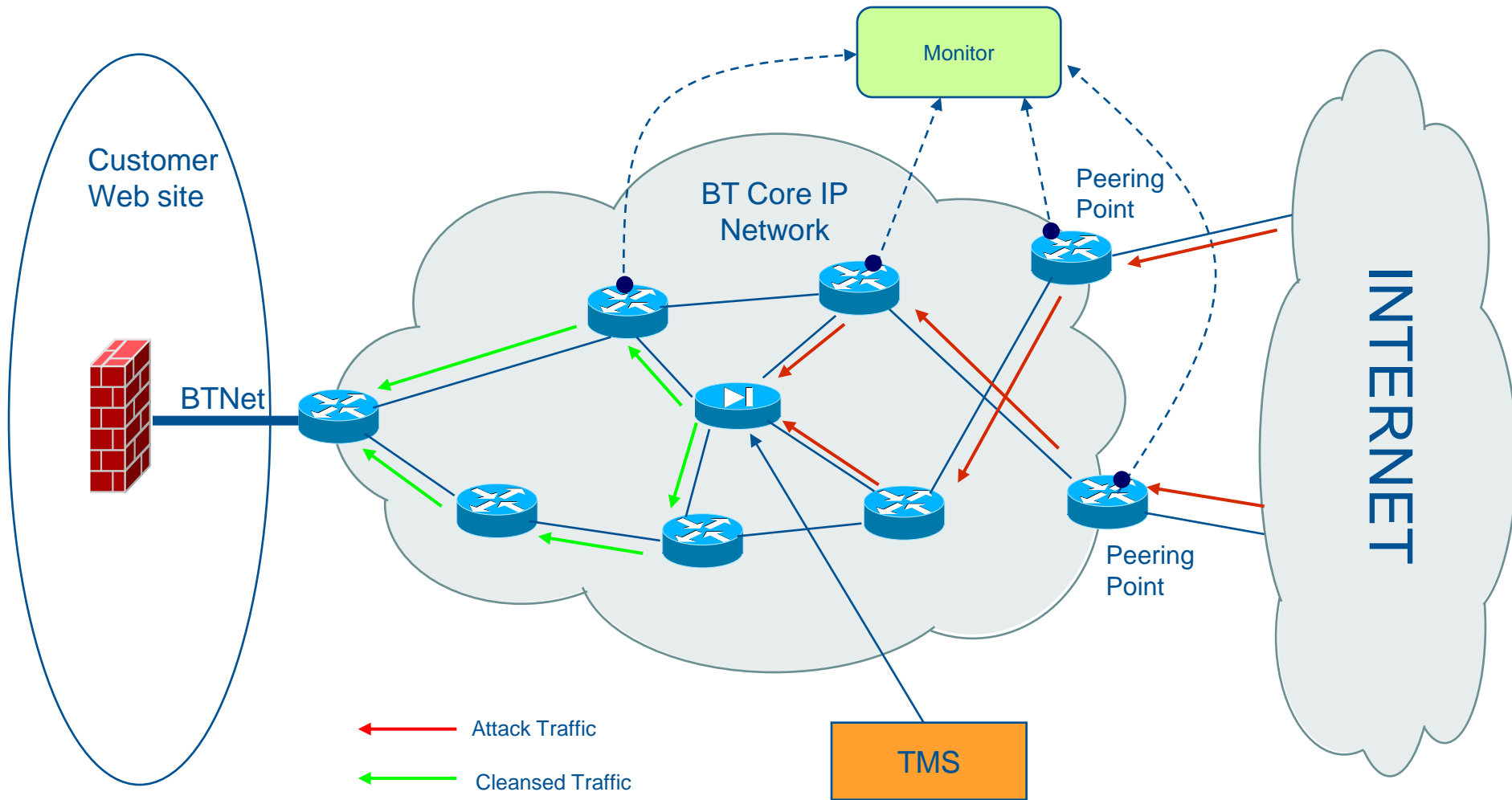
Figure 10: Frequently Attacked Targets
Source: Arbor Networks, Inc.

What is the solution?

BT DDOS Solution

- Its an integrated offer with BTnet:
 - The service is delivered via BTnet, with integration traffic inspection
- Detection & Mitigation Solution
 - A system of detectors across BTNet monitors the internet traffic directed at a website to identify traffic surges and unusual patterns of activity which could signify a DDoS attack.
 - When an attack is identified, the traffic is diverted through a mitigation device which filters out attack traffic and allows genuine traffic to continue on to your site.
- Key factors in BT's detection and scrubbing solution include:
 - monitoring of all traffic destined for your whole network, regardless of where it has come from.
 - a unique profile of expected traffic for each client.
 - automated responses.
 - cleansing and removal of bad traffic.
 - Customer portal showing intelligence reports.
- Quick Time to React – 10 minutes V 30 minutes
 - The BT Management Portal ensures that your entire internet accessible infrastructure is safe, 24/365. Our time window between spotting and reacting to suspicious activity is 10 minutes -considerably faster than the normal 30 minutes.

BT DDoS Solution in Action



Superior Solution:

- Quicker Response Time – 10 minutes V 30 minutes industry norm
- Minimal Network Latency
- BT already has extensive experience, in protecting our clients from all forms of security attacks:
- BT denies 14 million unauthorized connection attempts each day, prevents two million viruses per month and blocks five million spam messages each day.
- BT hosts and protects over 1,000 websites and over 1,500 firewalls for customers, many of which are 'mission critical' to our client organizations.

What's in it for the customers?

- More cost-effective alternative to DIY measures
- This enables you to protect your organisation's brand and revenue while maximising investment in your online infrastructure.
- Network based services. No equipment is sited at your premises, for easier maintenance.
- A fast reaction time, with minimal false positives.
- Mitigation of high-volume traffic and application layer attacks, for a strong, multi-layered defence.
- Expertise and resources which adapt your security to match ever-evolving threats.
- Dedicated 24/365 monitoring
- Individual customer log-ins to the portal, for secure and confidential use.
- Single or multiple IP address ranges monitored, for equal protection across all your network zones.
- Online customer reports to monitor and assess your transactions.
- Alert thresholds defined by you to meet your needs.

