Case Communications August 2009 Newsletter

Case Communications August 2009 Newsletter

In this Issue:

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/Enquiry]**

Welcome,

Welcome to the Case Communications August 2009 Newsletter.

ID card has been hacked and edited

A foreign national's ID card has been cracked and then reprogrammed by a security expert in an investigation by The Daily Mail.

[More]

A plan for a Digital Wales is required

The government and the Welsh Assembly must ensure that the Digital Britain programme fully reflects the needs of Wales, a report has concluded.

Whilst the Welsh Affairs Committee admitted in its report that digital exclusion is not any worse in Wales, it expressed concern that the Digital Britain plan did not consider Wales enough.

[More]

Swine Flu site falls ill on first day

The government's heralded national swine flu website crashed on its first day in operation after demand for access was four times what the government IT officials had predicted.

The website received more than nine million hits per hour after it was activated by the Department of Health.

With the heavy flow of traffic which averaged out to 2,600 hits per second, visitors were directed to a holding page instead.

[More]

Britain opts out of NATO cyber centre

Britain will not take part in a NATO cyber security and warfare scheme due to the conflicting interests that participation would cause with other government departments and allies.

NATO members Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain are all sponsoring a cyber defence and warfare centre that is being setup in Estonia to conduct research on what is expected to be a major part of the future of warfare. The centre is also expected to monitor suspected cyber attacks, study how to firm up NATO cyber defences, and train military officials in offensive and defensive cyber activities.

[More]

The real villain in the Gary McKinnon scandal

He has the backing of politicians across the spectrum, and celebrities flock to his cause. Pink Floyd's Dave Gilmour, Sir Bob Geldof and Chrissie Hynde are even recording a charity record for him. But last Friday, self-avowed "bumbling computer nerd" Gary McKinnon moved one step closer to being extradited to the US. The High Court ruled that he could not be tried in Britain for what America alleges was "the biggest military computer hack of all time". He faces up to 60 years in a maximum-security jail if convicted.
[More]

Technology 'priority for Britons'

Britons are more willing to cut back on holidays and meals out than on spending on communication technology during the recession, an Ofcom review suggests.

Courtesy of BBC - August 2009

[More]

Hackers attack Israeli party site

One of Israel's main political parties has shut down its website following an attack by Palestinian hackers, according to reports.

[More]

Web attack blogger blames Russia

A blogger who was targeted in a co-ordinated attack against websites such as Facebook and Twitter has told the BBC he blames Russia for the assault.

Courtsey BBC News

[More]

The day Twitter stopped

Of course, it wasn't a full day that the world went without the successful microblogging service It was just a few - crippling, to some - hours.

But the distributed denial of service attack(DDoS) that hobbled Twitter and its 45 million worldwide users - and which also sucked in Facebook and LiveJournal - has security experts baffled and concerned.

[More]

Defending virtual borders

The risk to government networks and major financial institutions from cyber warfare is increasing every day but what is being done to defend national borders?

[More]

BT offers free I-Plate BT Broadband Accelerator

BT has announced that it is now offering its Total Broadband customers a dedicated broadband accelerator (previously known as the I-Plate) that promises to increase received broadband speeds by 1.5Mbs.

[More]

Ofcom reports a rise in unbundled broadband lines across the UK

Figures released by communications watchdog Ofcom demonstrate a significant rise in the number of unbundled lines in the UK, passing the six million mark for the first time.

[More]

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

ID card has been hacked and edited

The newspaper borrowed the ID card of a foreign national and subjected it to tests to see how secure it is. The security expert, Adam Laurie, managed to clone the card using a Nokia mobile phone and a laptop.

ID cards have been cloned in the past, but the Home Office was always able to insist that the data held on the card's microchip was secure and could not be modified. But with the help of a second security expert, Jeroen van Beek, the encryption placed on the microchip inside the card was cracked using clues from the codes printed on the card.

From this point, they were able to edit details on the ID card including the name, date of birth, that the card holder was entitled to benefits and fingerprints. They were also able to add a note to the ID card that would appear in front of any police or security officer using a card scanner that said: "I am a terrorist - shoot on sight."

When told of the investigation, a Home Office spokesman told the newspaper: "We are satisfied the personal data on the chip cannot be changed or modified and there is no evidence this has happened. The identity card includes a number of design and security features that are extremely difficult to replicate.

"We remain confident that the identity card is one of the most secure of its kind, fully meeting rigorous international standards."

Chris Huhne, the Liberal Democrat shadow home secretary, said: "The Daily Mail's investigation has blown such a huge hole in the government's ill-fated ID card scheme that it is now sinking beneath the waves.

"Surely it can only be a matter of time before Home Secretary Alan Johnson recognises the folly of continuing with this expensive and misguided intrusion into our privacy."

NO2ID condemned the Home Office for knowingly making ID theft easier and ignoring dangerous vulnerabilities in the ID card. Its national coordinator, Phil Booth, said: "This shows up the big con. The Home Office doesn't really care about ID theft, or it wouldn't be pushing technology that any competent crook can subvert."

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

A plan for a Digital Wales is required

"Some of those challenges are particularly acute in Wales, and there is a need for the findings of Digital Britain to be focused into a plan for 'Digital Wales in a Digital Britain'. We call on the Secretary of State for Wales to ensure that the next stage of Digital Britain fully reflects the needs of Wales, that Welsh MPs are fully informed about the stages of implementation and that there is a joined up approach, which involves the Welsh Assembly and the private and third sectors," the committee said.

The committee said it would be particularly challenging to meet the universal broadband commitment of 2 megabits per second (mbps) due to its topography and low population density. But it said solutions must be found so that people in every part of Wales can benefit from the same level of coverage. It added that the "eradication of broadband notspots" in Wales must continue to receive priority attention.

Whilst it was worried about the attention Wales was receiving, the committee was generally pleased with government efforts. In particular, it welcomed the proposal to create an independent Next Generation Fund to subsidise network development in less commercially viable areas. It also urged the Welsh Secretary, the government and the Welsh Assembly Government to work together on the planning for the implementation of these networks at the earliest opportunity.

The only obstacle the committee foresaw was any department taking responsibility for the programme. Originally responsibility for digital inclusion fell with the Wales Office, as former Welsh Secretary Paul Murphy was also digital inclusion minister. But the report urged the government to clarify who will have the lead responsibility for taking forward digital inclusion and Digital Britain work in future.

"Digital inclusion is not an issue which can be delivered by any single government department or agency; progress can only be made if there is effective participation from many different organisations and if these contributions are effectively coordinated. Good coordination between the UK Government and the Welsh Assembly Government is also essential, given that many, but not all, of the most relevant policy areas are devolved," the report concluded.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Swine Flu site falls ill on first day

The NHS attempted to boost capacity but the access problems persisted.

"This is obviously very worrying and raises serious questions about the robustness of the pandemic flu system," said Norman Lamb, the Liberal Democrat shadow Health Secretary.

"It is absolutely vital that the public have access to a reliable source of information on swine flu to provide reassurance and to take the pressure off GPs surgeries."

A spokesman for the Patients Association said: "It's disappointing to hear that the service was not able to meet demand."

NHS officials blamed the surge in traffic on people visiting the site out of curiosity.

It was "rather implausible to think that there might be tens of thousands of people with flu waiting within a one-hour period to all get on and assess their symptoms," said Sir Liam Donaldson, the chief medical officer.

A spokesman for the Department of Health said: "During the early hours of the service, people were very keen to look at the site. We were swamped by the interest. We have been working hard with our IT people to expand the capacity in order to meet demand."

Fortunately the Swine Flu hotline for suspected sufferers was launched without any problems. Callers were able to speak to NHS staff without delay from its 3:00 launch time yesterday.

The staff were estimated to be capable of answering more than 200,000 calls during a 15-hour working day – or more than a million calls a week.

The website is www.direct.gov.uk/pandemicflu

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Britain opts out of NATO cyber centre

Britain however will not take part in the initiative nor will it supply any MoD staff to help operate the centre.

According to Defence Secretary Bob Ainsworth, this decision is "due to the need to co-ordinate cyber defence with a number of other government departments and allies."

Britain is taking steps on its own to develop a cyber security strategy. It is expected to involve the intelligence agencies and the MoD. While Britain is open to trading ideas and intelligence with the NATO cyber security centre, there are concerns that deeper involvement would only add another layer of bureaucracy to a cyber defence and warfare strategy.

Russia, China and North Korea have all made inroads into cyber warfare in the last few years. A number of major hacking incidents in Whitehall were allegedly attributed to the People's Liberation Army in China. North Korea has already launched several cyber attacks on South Korea in recent months and any provocation over their nuclear weapons programme could lead to attacks further afield. Estonia, the host of the cyber defence centre was crippled by Russian hackers in 2007 during a dispute over an old Soviet war memorial.

Britain is following the US's lead in setting up a cyber warfare centre that is jointly run by the intelligence agencies and the military.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

The real villain in the Gary McKinnon scandal

But this wasn't the work of a terrorist, says Boris Johnson in The Daily Telegraph. McKinnon, 43, who admits to hacking into 97 US military computers seven years ago, was "simply following up a weird intuition that UFOs exist, with all the compulsiveness that he has exhibited since he was a child". Diagnosed with Asperger's syndrome, the Glasgow-born hacker is just "a classic British nutjob, who passionately believes something that is irrational... he is a prime candidate for the protection of the Government".

That seems even more the case when you consider that he is being tried under the 2003 US-UK extradition treaty, which was meant to tackle the threat posed by al-Qaeda, says Anthony Painter on The Huffington Post. "Now it is being used to extradite a frightened and disabled man."

But "this is not simply an emotional argument", argues David Rawcliffe on the Adam Smith Institute blog. "It is a legal debate." Do McKinnon's supporters really believe the High Court should "have put public pressure and personal pity before the honest interpretation of the law?"

Johnson and other supporters of McKinnon can say all they want, but "if the law is to mean anything, it must remain the preserve of the judiciary, and, paradoxically, it must be followed by the courts even when it seems unjust". This "was not some harmless incident", as one military officer at the US Pentagon tells The Sunday Telegraph. "He did very serious and deliberate damage to military and Nasa computers," causing $700,000 worth of damage.

But there's a bigger issue here: the "lopsided" extradition treaty that makes it "much easier for British citizens to be sent to the US than for Americans to be brought here", says the Daily Mail. As it stands, the UK requires that the US show only "reasonable suspicion" to extradite a British citizen. So no firm evidence need be supplied. But the US asks for "probable cause" from the UK, which carries a greater burden of proof.

There are serious questions about how the process operates, say Sophie Kemp and Jill Lorimer, extradition experts at law firm Kingsley Napley in The Independent. Government figures released by the Liberal Democrats show that suspects in the US are 20% less likely to be extradited than those living in Britain.

You can feel sympathy for McKinnon and the US authorities, who "are doing what they think is right". The real villain in this case is "our own Home Office", says David Hughes on his Daily Telegraph blog. Home Secretary Alan Johnson protested in The Times that he is powerless to intervene. But this hand-washing "would have done justice to Pontius Pilate," says the Daily Mail. The Home Secretary can intervene on humanitarian grounds. As an Asperger's sufferer, McKinnon's "health, sanity and possibly life" are at stake if he is locked up in the US. "What more humanitarian grounds could Mr Johnson need?"

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Technology 'priority for Britons'

The watchdog's annual report says spending on mobiles, the internet and TV is regarded as a higher priority than almost anything except food.

In a poll of 862 people, over 40% said they would save on holidays and eating out and 19% chose spending on mobiles.

Ofcom's Peter Phillips said people were "more canny" about paying for services.

The study also highlights a major rise in the use of social networking websites.

Some 19m people in the UK, 50% of internet users, visit Facebook, spending an average of six hours a month on the site, it says.

This is an increase from four hours in May 2008.

The report said the proportion of 25 to 34-year-olds who said they had a social networking site profile grew by six percentage points in a year to 46%, while the figure also rose among 35 to 54-year-olds to 35%.

But the proportion of 15 to 24-year-olds with such a profile dropped from 55% in the first quarter of 2008 to 50% in the first quarter of 2009, the study added.

Ofcom researchers asked consumers where they were likely to be cutting back on spending during the recession, as part of its communications market report

Of those asked, 47% said going out for dinner, 41% said DIY and 41% holidays.

This compared with 19% who said they would cut back on mobile phone spending, 16% who said TV subscriptions and 10% who highlighted broadband services.

The report says the trend is supported by the fact communications are costing less, with longer, cheaper mobile phone contracts and the bundling of services such as television and internet at reduced prices.

Ofcom's Peter Phillips said: "Despite the recession, people are spending more time watching TV, using their mobile phone or accessing the internet.

"They would rather do without meals out or holidays than give up their phone, broadband or pay TV package

"Meanwhile, we are becoming more canny about the way we pay for these services.

"Almost half of us economise by taking a bundle of communications services from a single supplier, while one-fifth opt for cheaper mobile contracts which don't include an expensive new phone."

Catch-up TV boost

The report's other findings include:

- In May 2009, consumers spent an average of 25 minutes a day online at home - up from nine minutes in 2004
- Average household spending on internet services fell in real terms between 2007 and 2008
- Nearly a quarter of households, 23%, were watching catch-up TV online in 2008, compared with 17% in 2007
- This was driven by the BBC iPlayer, with 15% of internet users, 5.2 million, watching the service in 2008
- Overall take up of broadband across the UK reached 68% of households by the end of the first quarter of 2009, up from 58% on the previous year
- In May of this year there were more than 250,000 new mobile broadband connections, up from 139,000 new connections in May 2008.

Ofcom also published a report into communications in the nations and regions, which showed take up of services was rising rapidly.

Use of broadband in Scotland was up from 53% to 60%, in Northern Ireland take up rose from 52% to 64%, and in Wales from 45% to 58%.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Hackers attack Israeli party site

Attackers on the official Kadima website posted images of wounded Palestinians and the aftermath of suicide bombings in Israel.

Slogans in both Hebrew and Arabic were also placed on the site, including threats to party leader Tzipi Livni.

The website was back online early Thursday morning.

The Jerusalem Post, quoting an Israel Army Radio report, said the pictures included one of Livni, with the words "We promise you - we're coming".

According to AP news agency, the hacked web page was signed Gaza Hacker Team.

The images were removed shortly after the attack and the site was then shut down. It was brought back online at about 0830 BST.

Kadima, a centrist political party that favours a two-state solution to the Middle East conflict, is the largest party in the Israeli parliament.

It was unable to form a government, and is currently in opposition.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Web attack blogger blames Russia

The pro-Georgian blogger, known as Cyxymu, said he had been targeted for "telling the truth about the Russian-Georgian war" in his writings.

The attack caused a blackout of Twitter for about two hours on Thursday.

Despite the blogger's claims, security researchers say there is "no suggestion the attack was state-endorsed".

Google, Facebook and blogging platform Live Journal - all sites where Cyxymu had accounts - were also affected.

"I write the truth about the Russian-Georgian war and somebody did not like these truths - these people in Russia," the blogger told BBC News.

"I don't know which people," he added.

The blogger, real name Georgy, has posted videos and blogs which criticise Russia over its conduct in the war over the South Ossetia region, which began one year ago.

"It's a big surprise to me that my blog has meant that 250m people have not been able to enter Facebook," he said.

Graham Cluley, of security firm Sophos, told BBC News there was no suggestion the attack against the blogger was state-endorsed.

"It was almost certainly an individual who took objection to his blogs," he said.

"They took internet vigilantism into their own hands to try to blast him off the web, but in the process blasted Twitter off instead."

'Fragile service'

Facebook had previously confirmed to BBC News that the attacks were directed at an individual who had "a presence on a number of sites, rather than the sites themselves".

"A botnet was directed to request his pages at such a rate that it impacted service for other users," the spokesperson said.

Botnets are networks of computers under the control of hackers.

The machines were used to mount a so-called denial-of-service (DoS) attack on Thursday.

DOS attacks take various forms but often involve a company's servers being flooded with data in an effort to disable them.

"Attacks such as this are malicious efforts orchestrated to disrupt and make unavailable services such as online banks, credit card

payment gateways and, in this case, Twitter, for intended customers or users," wrote Twitter co-founder Biz Stone on his blog.

Twitter was knocked out by the attack for around two hours, while Facebook said its service had been "degraded". The effect on Live Journal is unclear.

Only Google seems to have escaped unscathed from the attack.

"Google systems prevented substantive impact to our services," the company said in a statement.

Sudden realisation

The company has not confirmed which services were targeted in the attack, but it is thought that its e-mail service Gmail and video site YouTube were under fire.

"We are aware that a handful of non-Google sites were impacted by [an]... attack this morning, and are in contact with some affected companies to help investigate this attack," the company said.

All of the affected services were keen to stress that users' data had not been put at risk in the attacks.

"Please note that no user data was compromised in this attack," wrote Twitter's Biz Stone.

"This activity is about saturating a service with so many requests that it cannot respond to legitimate requests thereby denying service to intended customers or users."

The blogger said he first noticed that things were not right when he realised his Live Journal page was not working.

"After, I entered Facebook to say Live Journal was not working and Facebook was down," he told BBC News.

"So I entered Twitter to say that Live Journal and Facebook were not working, and Twitter was down.

"And so I understood that it was under attack. It is not possible that these three services were all down at one time."

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe/ Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback/ Enquiry]**

The day Twitter stopped

"Up is down, left is right and black is white," I was told chief security researcher Patrick Peterson.

"These attacks do not make sense. In the last few years, we have seen the criminals build systems to make money and not get caught.

"Now we see them making a big splash with this attack which is of no benefit. It does not put a single dollar in their pocket and it exposes them to the risk of being caught," said Mr Peterson.

A denial-of-service attack generally works by using hijacked computers or botnets to deluge a site or service with thousands and thousands of requests, overwhelming it and rendering it obsolete.

In the case of Twitter, the New York Times' said those responsible unleashed a wave of spam e-mail messages which infiltrated the service and other sites.

"It's a vast increase in traffic that creates the denial-of-service," said Bill Woodcock, a research director of Packet Clearing House, a non-profit organisation that tracks internet traffic.

The first DoS attacked dates back to ver a decade ago.

Wikipedia cites a major hit on domain name servers involving AOL and Register.com in January 2001. The following month, it was the turn of the Irish department of finance, targeted by students.

More recently, the Iranian government was the focus of foreign activists seeking to help the opposition following June's contested presidential elections.

The US government was affected just two months ago, as was Korea.

"So ten years ago, we saw the biggest names on the internet like Microsoft, Yahoo and Amazon get attacked because they were the marquee brands of the day. Today, they are going after Twitter and Facebook for the same reason."

But despite these high-profile trophies, Mr Peterson describes denial-of-service as, to all intents and purposes, an outmoded tool in the criminal fraternity.

"You have to be brave or stupid to have attacks this brazen with law enforcement being more active in the realm of cybercrime. There is a serious risk of being caught."

Other industry experts agree.

"Organised crime and other groups have gone off to other things. It's more lucrative for them to use the internet, not to take the internet away," John Harrison of security firm Symantec told

CNEtc.com

In the blogosphere, some claim that Twitter and Facebook are working together to track down who is behind the attack. Some security experts are also pouring through the data. The theories range from a teenager to a Georgian blogger.

For the future, Mr Peterson says the best way to stop a denial-of-service is to employ techniques that alert sites to differences in the way requests are coming in from computers.

"The criminals may have a botnet of around 50,000 to 100,000 infected computers in their control. But there are also 10 to 20 million legitimate users out there and their traffic looks nothing like DoS traffic," explained Mr Peterson.

"If you can get a smart system to detect anomalies, then you can block the DoS bots making 1,000 requests a minute versus one that makes three requests per minute and keep your site online."

However, just blocking access from the IP addresses of offending computers can cause the knock-on problem of blocking legitimate users who do not know that their computer has been compromised.

For Twitter, the implications of the attack are serious.

It wants to be more than a social media brand. It wants to be a communications standard.

And while this has not been seen as a good day for Twitter, it has to ensure such an attack does not overwhelm it next time. Because there will certainly be a next time, says Mr Peterson.

"A few months ago, I would never had predicted anything like this. Denials-of-service were a thing of the past.

"But this is a trend. And I think a lot of people who view DoS attacks as fun will look at all the media attention and it will invite more criminals to try their hand at it," warned Mr Peterson.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Defending virtual borders

Estonia is an online savvy state and champion of so called 'e-government,' a paperless system with many government services online. The population can even vote via the web.

In 2007 a large number of Estonian government and financial websites were brought to a standstill as they came under sustained online attack.

On 4 July 2009, US and South Korean government websites and those of certain banks and businesses ground to a halt as they came under denial of service assaults. In the United States, the Pentagon and the White House were also targeted.

These cyber attacks were all initially thought to be orchestrated by countries unfriendly to Estonia, South Korea and the US and to date have been the highest profile examples of so-called cyber warfare.

Digital battlefield

Conventional warfare relies on tanks, troops, artillery, aircraft and a whole gamut of weapons systems. Cyber warfare requires a computer and an internet connection.

Rather than sending in the marines, the act of typing a command on a keyboard can have a devastating effect on computer systems and networks.

According to Clive Room of Portcullis Computer Security: "It is possible to bring an entire state to a standstill theoretically and we've seen it done on a small scale practically, so the threat ahead of us is very big indeed."

From criminal gangs trying to steal cash, to foreign intelligence services trying to steal secrets, the threat of cyber warfare is now very real.

Nato suspects that along with the tanks and troops involved in the conflict in Georgia in 2008, Russian forces also engaged in cyber attacks against Georgian government computer systems.

Professor Peter Sommer of the London School of Economics explained that cyber warfare should just be seen as a part of modern warfare in general:

"[Carl Von] Clausewitz said war is diplomacy conducted by other means. What cyber warfare gives you is a whole range of new types of technologies which you can apply."

Zombie machines

These international attacks are not isolated instances. Everyday government and corporate websites fend off thousands of attempts to infiltrate hack and cause disruption.

Twitter, Facebook and other high-profile sites have recently been brought to their knees by similar attacks.

The popular weapon of choice in cyber warfare is the distributed denial of service attack or DDoS. Unknown to their owners, infected computers become zombie machines digitally press-ganged to do the bidding of hackers, this is known as a botnet.

In their thousands these zombie machines attempt to log on to a particular website, forcing it to fail or collapse under the sheer weight of data it is receiving.

The threat of cyber warfare is being taken seriously by Western governments and Nato. Online assets are being deployed to bolster national and international digital defences.

NATO has set up a cyber defence facility in Estonia codenamed K5. The American government has launched a national cyber security strategy and the UK has responded by creating two organisations, the Office of Cyber Security and the Cyber Security Operations Centre based at GCHQ in Cheltenham.

However the amount of people involved is still small, said Clive Room.

"The government's own reckoning is about 40. About 20 people within each of those two offices."

In comparison he estimates that there are about 40,000 people "listening in to us in China" and "working round the clock."

For Professor Sommer, the UK has had a response to cyber warfare in place for 10 years, but "it's been pretty hidden so far."

"You tended to get to know about it if you were an academic or you moved in certain sort of technical circles," he said.

"More recently because the problems got bigger and because of greater public alarm and interest they have decided to make it more public."

Misdiagnosis

If defending against cyber warfare is tough, trying to pin point, track back and identify the origin of an online attack can be a near impossible task.

In the case of the Estonian attacks, initial reports suggested that Russia was to blame. These allegations have been strongly denied by Russian authorities, and to date only one individual, an ethnic Russian student living in Estonia, has been fined as a result of the attacks.

For Professor Sommer, misdiagnosis is easy: "All too quickly people say they know where the attack is coming from."

"My experience of doing investigations of all sizes is that very often the initial diagnosis is wrong."

"If you look at the recent Korean attacks it seems, at a political level, a reasonable supposition that it originated in North Korea because they're the people that are most active at the moment.

"On the other hand, some of the reports say at a technical level they seem to have originated here in the United Kingdom, which makes no sense. So diagnosis is quite difficult."

However, one thing is certain: cyber warfare is here to stay.

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

BT offers free I-Plate BT Broadband Accelerator

BT claims that the BT Broadband Accelerator filters out interference from home phone wiring to help broadband connections run faster. Although speed improvements are likely, they can't be guaranteed, says BT. The improvements in speed will take up to 2 weeks to come through so that line stability is not affected. BT claims that even if it doesn't improve the speed the I-Plate can help stabilise your broadband line making it more reliable.

Customers are expected to pay £1.20 for the postage costs. Previously the I-Plate retailed for just under £10.
When placing the order (the £1.20 is added to the user's phone bill) the site states "Available to BT Total Broadband customers only. Non BT Total Broadband customers will be contacted to place an order for BT Total Broadband."
Non BT Total Broadband customers can order the device for £7.07 (inc VAT)

Customers need to fill in a short questionnaire in order to determine whether or not the device will help to filter out interference from their home phone wiring.
The BT Broadband Accelerator is designed to block interference from televisions, lighting and home wiring, which BT says can slow down home broadband speeds.
The company said the seven out of ten UK homes with a BT NTE 5 master socket are eligible for the product, and claimed that in its study of 36,000 lines, the technology typically showed a speed increase of up to 1.5Mbps. Some lines showed speed improvements of as much as 4Mbps.
As well as boosting overall speeds, BT said the technology could prove a bonus for ADSL customers who live some distance from their local telephone exchange, while the minority of people who were previously just beyond the reach of a broadband service, may now be able access the high-speed web.

"The BT NTE 5 master socket can be easily identified by the horizontal split in the face plate and BT logo," said BT. "All consumers need do is simply unscrew the face plate, clip the BT Broadband Accelerator in place in the socket and replace the face plate over the I-Plate."

Lexton Snol PCADVISOR
August 5, 2009

Case Communications August 2009 Newsletter

Archives

Read the back issues

Missed anything interesting? Then click on the link below to read all the back issues of this magazine. **[Full archive list]**

Subscribe FREE

Sign-up for the newsletter

If you would like to subscibe or un-subscribe to this magazine then click on the link below. **[Subscribe / Unsubscribe]**

Feedback

Tell us your thoughts

If you have something interesting to say or comments about the ezine, please feel free to email them to us: **[Email feedback / Enquiry]**

Ofcom reports a rise in unbundled broadband lines across the UK

Using data collected by the Office of the Telecoms Adjudicator, Ofcom found by the end of July 2009 6,009,593 unbundled lines had been established in the UK. Looking at local loop unbundling figures (LLU), the Telecoms Adjudicator was interested in tallying up lines where the internet service provider offered their own services over BT's copper wire telephone network.

Ofcom started compiling unbundled figures back in September 2005. At that time there were just 123,000 unbundled lines in the UK and the majority of people could only get their broadband and landline telephone service from BT.

Speaking on the findings, Ofcom chief executive Ed Richards said: "in just four years unbundling has gone from a flicker on the dial to a major competitive force in telecoms. This has delivered the dual benefits of driving up broadband take-up and driving down prices."

Broadband Genie
11.08.09