Anonymous: serious threat or mere annoyance?

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, Network Security

For a couple of weeks in December 2010, the Wikileaks 'Cablegate' controversy was in danger of being overshadowed by another, related phenomenon – Distributed Denial of Service (DDoS) attacks launched by the so-called Anonymous movement against organisations they deemed to be contrary to Wikileaks' interests. The attacks provoked a press frenzy that frequently exaggerated their effectiveness and missed at least one intriguing aspect – that they effectively relied on people infecting their own PCs. So how did these attacks work, how effective were they, and what are the implications?

Who are Anonymous?

Anonymous originates from the 4chan.org message board, an 'anything goes' website that allows users to post images and comments without registering. They can use names (any names) or they can post without identifying themselves, in which case the posting is labelled 'Anonymous'.

The site became a rallying point for a series of (mostly juvenile) pranks and campaigns. Before the Wikileaks-related activities, Anonymous was best known for Operation Payback in which it attacked the Recording Industry Association of America (RIAA) and other organisations connected with copyright protection and music and software anti-piracy efforts. The anti-copyright activities of Operation Payback continue to this day, in a somewhat spasmodic manner.

The group then gained considerable notoriety for its attacks on the Church of Scientology with 'Project Chanology'.[1] Critics (and even some supporters) of Anonymous considered this campaign a mistake, as it enabled the Church of Scientology to claim religious persecution, while the damage caused was minimal. The 'church' moved quickly to protect itself from the Anonymous activities by switching hosts and employing the services of Prolexic – a specialist in mitigating DDoS attacks.[2] Two members of Anonymous were subsequently jailed for taking part in the attacks.[3]

Wikileaks campaign

The campaign in support of Wikileaks came as something of a surprise to many. Anonymous wasn't known for engaging in sophisticated debates about freedom of information or transparency of government. The campaign was presented as 'Operation Avenge Assange' (in reference to Wikileaks leader Julian Assange), but most people continued to refer to it as Operation Payback. Via its websites, Anonymous issued the statement (though with rather more spelling mistakes):

"While we don't have much of an affiliation with WikiLeaks, we fight for the same: we want transparency (in our case in copyright) and we counter censorship. The attempts to silence WikiLeaks are long strides closer to a world where we cannot say what we think and not

Figure 1: Anonymous indulged in some limited website defacement.

express how we feel. We cannot let this happen: that is why we will find out who is attacking WikiLeaks and with that find out who tries to control our world. What are we going to do when we find them? Except for the usual DDoSing, word will be spread that whoever tries to silence or discourage WikiLeaks, favours world domination rather than freedom and democracy."

The main targets of the Anonymous attacks over the first couple of weeks of December 2010 were:

- Financial organisations – such as MasterCard, Visa and PayPal – which blocked payments to Wikileaks.
- EveryDNS.com, which removed Wikileaks' DNS record.
- The website of Joe Lieberman (lieberman.senate.gov), the US senator who wants Assange to be tried under espionage laws.
- US politician Sarah Palin, who called for Assange to be treated like a terrorist, also found her website (sarahpac.com) under attack from some Anons, but only a minority.
- The Swedish law firm (www.advbyra.se) representing the two women who have made allegations of sexual misconduct against Assange.
- The Swedish prosecutor's office responsible for the case (aklagare.se).
- Swiss bank PostFinance (postfinance.ch), which suspended Assange's defence fund account.

Other targets would emerge – among them online retailer Amazon which, in spite of it kicking Wikileaks out of its S3 cloud storage service, initially remained immune from retaliation. Anonymous also indulged in some website defacement, although the number of sites affected was very small and they were mostly easy targets.

Anonymous claims to be an amorphous entity. This is not entirely true, but it is true that anyone can join in. The group's activities are organised primarily via IRC chatrooms and, to a lesser extent, Twitter and Facebook. Because there is no formal structure and no overt or admitted leadership, it's difficult to pin down exactly how the group's activities come about. Ideas are seeded in the IRC channels and members – or 'Anons' – join in or not as they see fit. This apparently anarchic nature is both a strength and a weakness, as we'll see.

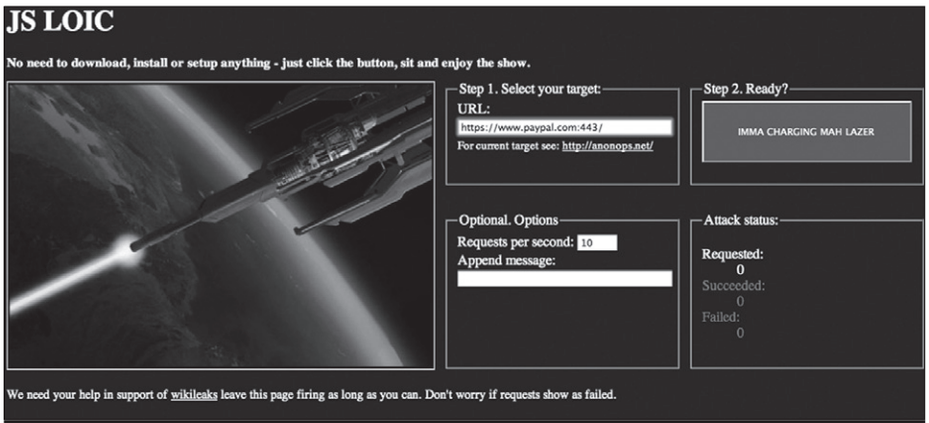


Figure 2: JS-LOIC, the Javascript version of the LOIC DDoS tool. The precise appearance depends on how it is implemented by each site's webmaster.

DDoS tool

The tool of choice for Anons is the Low Orbit Ion Cannon (LOIC). This was originally developed by 'Praetox Technologies' (a suitably anonymous coder), allegedly as a network stress-testing tool.[4] The source code for LOIC is still available on the now-unmaintained Praetox website, but the version used by Anonymous has been updated and retrofitted with a crude command and control capability.

LOIC comes in two main forms – a Windows executable that Anons download and run from their own machines; and a Javascript-based version (JS-LOIC) designed to be integrated into a web page and therefore usable by anyone who visits the site. (Other ports of the tool are available but appear little used so far.)

Distribution of the tool is widespread – you can find it in any number of locations and there is no attempt to verify the authenticity of the code. There is nothing to stop someone injecting malware into the tools and making the malicious version available in multiple places on the net: most users would be entirely unaware as the technical sophistication of Anons tends to be very low.

No skill is required to use LOIC. The Javascript version just needs the user to enter a target address and click the 'fire' button, although there are some optional settings. The Windows executable can be equally simple to use, and also offers a 'hive mind' option in which it will attempt to discover the current target from an IRC channel (with the IRC server and channel specified by the user). This makes it even easier for the user, who simply has to start the program running. Knowledgeable users can select a variety of options, such as type of packets sent (TCP, UDP or HTTP), port numbers and so on.

In hive mind mode, operation of LOIC clients is controlled by plain text messages posted in the topic of the chosen IRC channel. In their analysis of LOIC, researchers Pras et al give the following example of a command that initiates an attack and provides various parameters, such as target:[5]

```
!lazor default targethost=www.moneybookers.com subsite=/
speed=3 threads=15 method=tcp
wait=false random=true checked=false
message=Sweet_dreams_from_AnonOPs
port=80 start
```

LOIC sends repeated messages containing a string defined by the user to the target machine, opening several connections. With TCP and UDP attacks, the packets sent consist of just the plain text of the message: in HTTP attacks, the string is included in a GET request. The Javascript variant only uses HTTP but attempts to make the attack more effective by including random numbers in the URLs it generates, in an effort to prevent caching.

Other, more sophisticated tools have appeared. The High Orbit Ion Cannon (HOIC) claims a number of advanced

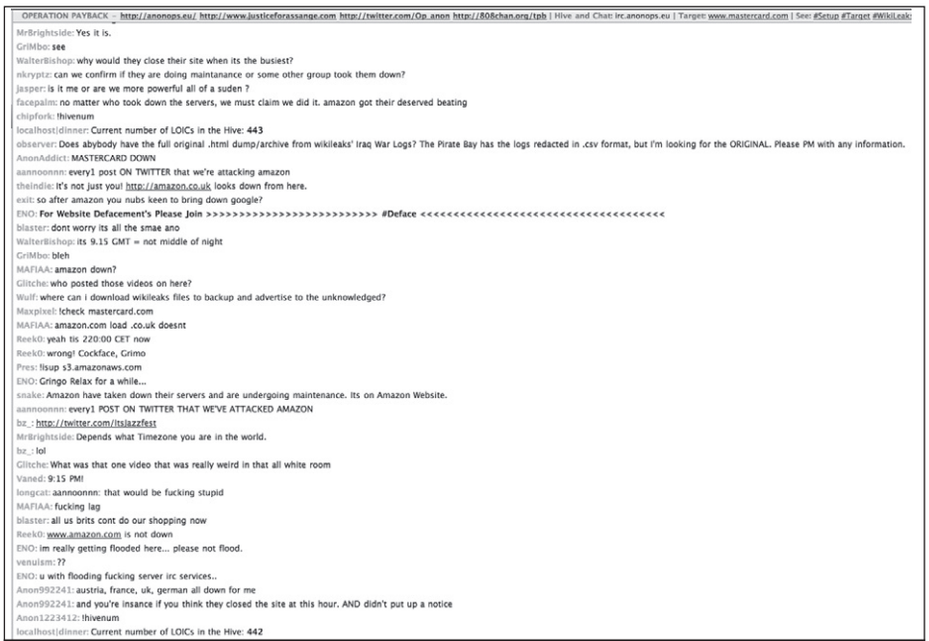


Figure 3: IRC chatrooms are used by Anonymous for both command and control and discussion of topics such as the next target.

Figure 4: Network status (as of 10 Dec 2010) showing the effects of retaliatory strikes by the authorities and 'patriot' hackers.

features, including high-speed, multi-threaded HTTP flooding, the ability to attack up to 256 websites at once and scripting.[6] Code for the Geosynchronous Orbit Ion Cannon (GOIC) variant appeared on the web in the middle of December 2010.[7] But neither HOIC nor GOIC played any significant part in the Operation Payback campaign.

An updated version of the original tool, LOIC2, has also appeared which can use Twitter, Facebook and RSS as command and control channels and can employ slow HTTP transactions to over-burden servers.

Cannon fodder

Given that the DDoS attacks mounted by Anonymous are unambiguously illegal in most countries (and all of the countries in which Anons are likely to have been operating), it's interesting to note that one thing the LOIC tool makes no attempt to do is conceal the identity of the attacker. The IP address of each attacker will be readily available in the victim's system logs, and it's a safe bet that at least some of the larger firms involved in the recent campaign will now be sitting on databases of attacker IPs.

LOIC cannot be used via proxies (including anonymising systems such as TOR) because that would just end up DDoSing the proxy. Inevitably, some Anons will have used the tool on other people's machines – perhaps at school and, for those old enough, at work. This should give pause for thought for corporate infosec practitioners: do your security policies properly cover such misuse?

"Most of them are script kiddies caught up in the excitement and the prospect of being able to create havoc with no apparent consequences"

The attacks mounted by Javascript versions of LOIC will be easily traced to the websites on which the tool was hosted. In most cases, however, the logged IPs will point to the personal computers of individual Anons.

It's quite probable that the majority of Anons have no idea that this is the case.

Most of them are script kiddies caught up in the excitement and the prospect of being able to create havoc with no apparent consequences. They are, in fact, little more than cannon fodder for the Anonymous campaign.

Some are aware of the dangers, but there is a dangerously high level of naivety present. On IRC channels and websites affiliated to Anonymous, advice on how to protect yourself includes claiming your computer was infected with a virus and setting your wifi router to be open so that you can claim someone else used it – neither of which would stand up in court. Some Anons suggest that the authorities would be unable to prosecute such a large number of people. But they wouldn't have to. A few test cases would probably be enough to discourage people from joining in – at least, enough people so that Anonymous wouldn't get the volume of DDoS traffic required to be successful. At the time of writing, two teenagers had been arrested in the Netherlands in connection with the recent attacks, and in the US, the FBI seized a server.[8]

That said, there is reason to believe that the majority of Anons are probably safe. Most authorities, and victims, are likely to have little interest in prosecuting script kiddies, especially with the complications involved in pursuing people in foreign jurisdictions.

Organisational channels

IRC was key to Operation Payback. Channels such as #loic and #target were used to direct LOIC clients to their victims. The #operationpayback channel was buzzing with frequently over-excited debate about who to attack and the effects of the campaign. Sometimes the chatter was so rapid that it was hard to read anything before it scrolled off the page. Twitter was also a key communications channel, mainly for directing Anons to IRC domains. This was desperately needed because Anonymous wasn't the only group on the attack – others were fighting back.

Some of the retaliation was by the authorities. DNS listings were withdrawn, so that domain names used for

Figure 5: Twitter was used to co-ordinate attacks, although accounts associated with Anonymous were quickly shut down.

Anonymous IRC servers and websites became unusable. The domains also came under regular DDoS assaults themselves – notoriously by so-called 'patriot' hackers (including the relentlessly self-promoting 'Jester', or 'th3j35t3r' if you prefer).[9]

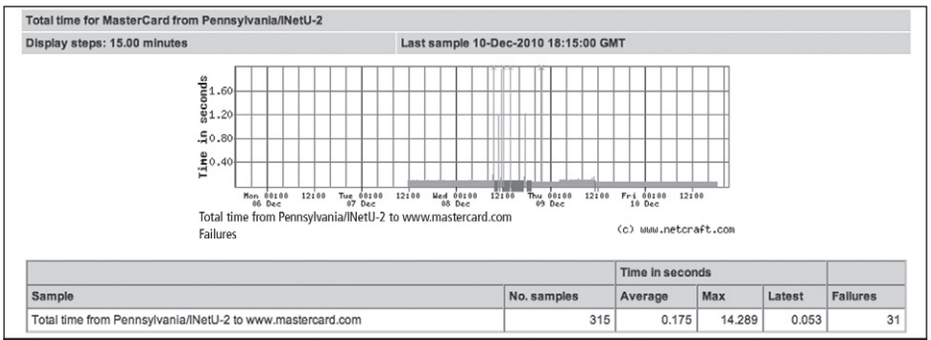
"As soon as one account was shut down, another popped up – like a game of cyber whack-a-mole"

The result was that Anonymous was constantly having to find new homes for its IRC and web servers. The anonops-irc.org domain was one of the early casualties. The group switched to .eu domains (eg, anonops.eu), which didn't last long, then to .tk addresses (eg, anonymous-payback.tk) and even anonops.ru. For most of the time, users could connect to IRC servers only by using IP addresses.

Twitter also closed one Anonymous account after another. Naturally, as soon as one account was shut down, another popped up – like a game of cyber whack-a-mole. However, it was often impossible to tell the difference between accounts opened by people with a genuine connection to the Anonymous leadership and those of fellow-travellers and people just in it for fun.

The apparent resilience of these 'fire and reposition' tactics was hailed by Anonymous as proof that its amorphous, allegedly leaderless structure is immune to suppression. In fact, the constant domain-shifting and problems with Twitter proved to be a major weakness for Anonymous. Anons were forced into hunting around for the address of the current IRC server, dramatically reducing the number who could participate in the DDoS attacks at any one time. Often, Anons would attack different targets, misled by 'unofficial' Twitter accounts or websites or by out-of-date information. The result was a significant watering down of the group's efforts.

To any visitor to the IRC channels (and the number of press visitors prompted the IRC operators to set up a dedicated #journalists channel) it quickly became clear that Anonymous does have leaders. Only operators can set the topics of the channels that direct Anons to their next target. The 'discussions' in channels such as #operationpayback verged on the rabid and unintelligible. Picking any kind of consensus out of this anarchy would have been impossible. To say that the 'group' decided on the next target is not credible. Somewhere, a person or small group of people, made that decision. Perhaps they were guided by what they'd read in the channel. It seems more likely that they seeded the channel with their own ideas for targets and used the eagerness of the members to launch attacks as a justification. Anonymous later issued a press release – another sign of leadership: anarchic mobs don't write press releases.



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Pennsylvania/INetU-2 to www.mastercard.com	315	0.175	14.289	0.053	31

Figure 6: Netcraft uptime stats show periods of unavailability for MasterCard's website. Visa was hit with similarly short spells of downtime.

Damage assessment

While there were many claims – in the press and in IRC channels – that targets had been brought to a grinding halt, the effects of the Anonymous DDoS attacks were patchy to say the least. Frequently, there would be claims made on IRC that the target of the moment was 'down'. In fact, it's highly likely that the Anon reporting victory was actually having his or her IP address blocked by the victim. A standard defence against DDoS is to identify IPs responsible for the attack (usually readily identifiable given the classic behaviour of making repeated requests in a short space of time) and filter them. The site would appear to be down to any such attacker but would work normally for everyone else.

"The impact on the primary operations of larger firms, such as MasterCard, is likely to have been minimal"

There are no available figures with which to measure the damage done by Operation Payback. Netcraft statistics for uptime give a clue and show that some major organisations saw short periods of downtime while others suffered outages of a day or more.

Given that availability is critical to organisations that process financial transactions, any amount of downtime is likely to be expensive. However, Anonymous succeeded in attacking only minor parts of those companies – in the case of PayPal, for example, the initial attack was just against the site's blog. While the smaller organisations, such as the Swedish law firm, are likely to have had all their Internet-based activities disrupted by the over-stressing of their web servers, the impact on the primary operations of larger firms, such as MasterCard, is likely to have been minimal. In addition, those transactions that were affected were most likely only delayed. For example, someone trying to make a PayPal payment probably just waited an hour and tried again.

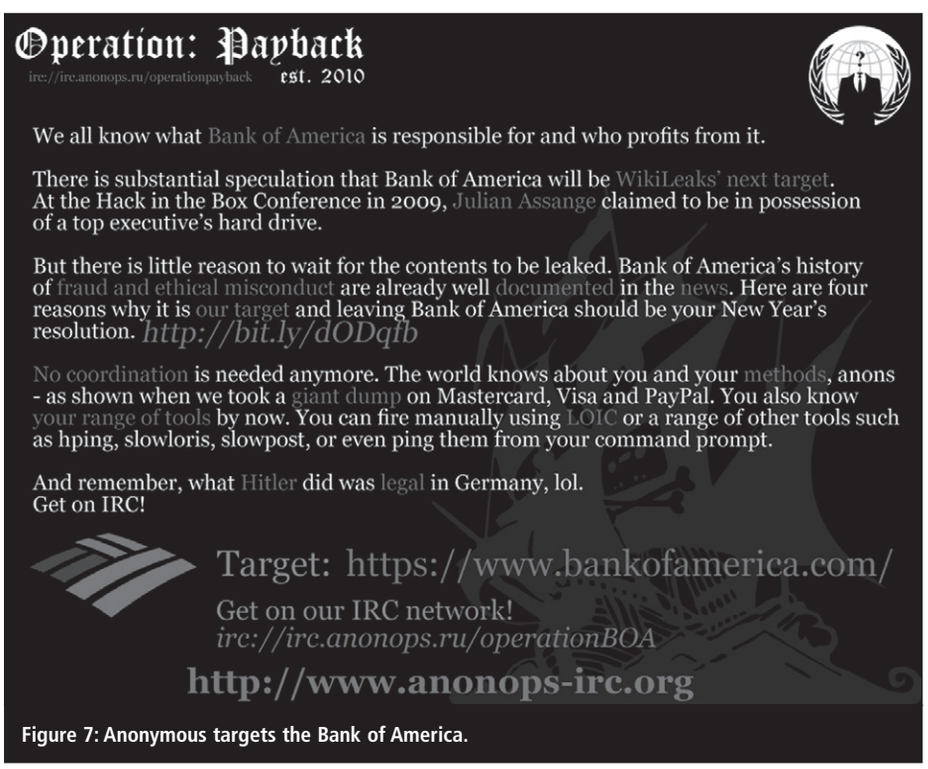


Figure 7: Anonymous targets the Bank of America.

Critical mass

The Anonymous attacks illustrated a fact of life known by any student of DDoS attacks – that it's all about numbers. Cybercrime gangs using DDoS as a blackmail tool, or state-sponsored hackers using it as a weapon of war, will deploy botnets comprising tens of thousands of machines focused on a single target. Even at the peak of the Anonymous attacks, the number of participants was in the low thousands, and most of the time there were only hundreds of LOIC clients firing at the same time at the same target.

There were reports that the LOIC tool had been downloaded at least 40,000 times by mid-December. But there's no way of telling how many of these downloads were used in anger. And, of course, they have to be used at the same time to achieve the proper DDoS effect.

"Even a little time spent in the IRC channels is enough to convince you that trying to organise Anons is like herding cats"

Co-ordination was a big problem. Botnets are automated: with the LOIC-based Anonymous DDoS, you're relying on individuals who must be available and willing at the same time, and who must all have their clients configured to fire at the same target (only those clients set to hive mind mode benefited from any degree of automation).

We've already seen how the constant disruption to IRC hosting and Twitter accounts played havoc with co-ordination efforts. And while Anonymous clearly has some degree of central control, even a little time spent in the IRC channels is enough to convince you that trying to organise Anons is like herding cats.

On 10 December, Anonymous issued a press release – partly, it seems, to put a face-saving spin on its failures. Famously, these failures included an abortive attack against Amazon. Many Anons wanted to attack Amazon.com for booting out Wikileaks from its S3 service, and there is some evidence that some Anonymous members mounted just such an attack. Certainly, there was an attack against Amazon.co.uk for selling an e-book containing some of the Cablegate memos. This attack had no effect.

In part, the press release read:

"While it is indeed possible that Anonymous may not have been able to take Amazon.com down in a DDoS attack, this is not the only reason the attack never occurred [sic]. After the attack was so advertised in the media, we felt that it would affect people such as consumers in a negative way and make them feel threatened by Anonymous. Simply put, attacking a major online retailer when people are buying presents for their loved ones, would be in bad taste.

"The continuing attacks on PayPal are already tested and preferable: while not damaging their ability to process payments, they are successful in slowing their network down just enough for people to notice and thus, we achieve our goal of raising awareness."

Claiming consciousness-raising as the real aim of the attacks is entirely contrary to the evidence of the IRC channels, in which Anons were clearly interested only in taking down their targets. The press release is also notable for the inherent hypocrisy in claiming the moral high ground when choosing not to attack Amazon – because it would spoil Christmas – while failing to acknowledge that attacks against payment-processing companies could have had the same effect.

Continuing attacks

Although the first two weeks of December saw the main frenzy of activity, Anonymous hasn't stopped attacking sites in its support for Wikileaks. There were more attacks against MasterCard and other payment-processing firms. But when it became clear that the DDoS attacks simply weren't working, Anonymous switched briefly to a somewhat bizarre strategy of attempting to overload the fax machines of a number of organisations. When attacking a little-used technology from a previous era brought only derision, it went back to DDoS assaults. The Bank of America was briefly inconvenienced because, like Visa and MasterCard, it stopped processing payments for Wikileaks – partly because it believed itself to be the next subject of leaked memos.

Anonymous has also turned its attention to countries that have tried to impose restrictions on Internet use following embarrassing revelations in Wikileaks cables – including Zimbabwe and Tunisia.[10,11] We can expect this campaign to continue for some time, but without the press attention it had in early December.

The future

Several pundits have speculated that we can expect to see more of this kind of hacktivism. And while, this time around, Anonymous was little more than an irritation, with more focused leadership and improved co-ordination, it could be a far more dangerous threat. That would make it a more viable target for legal action – by the authorities and victims. And if Anons were more frequently arrested and jailed, it would be interesting to see how much support Anonymous could muster: the experience of visiting the IRC channels suggests that most Anons are driven more by a desire for some anarchic cyber-fun rather than any ideological conviction.

Large organisations proved themselves fairly resilient to these attacks – at least, the scale of attack available to Anonymous. Amazon, with its cloud-based infrastructure, was particularly immune. This may prompt more organisations to look to the cloud for safety.

Media speculators and Anons alike went so far as to say that the first real cyberwar has begun – between Anons on one side and a strange alliance of authorities, corporates and 'patriot' hackers on the other. Like much of what comes out of Anonymous (including its press release and hilariously pretentious YouTube videos) that's so much self-aggrandising hyperbole. But this campaign did point to a line of tension running through the Internet that is likely to produce many entertaining – and perhaps dangerous – incidents in the future.

About the author

Steve Mansfield-Devine is the editor of Network Security *and its sister publication* Computer Fraud & Security. *He is also a freelance author and journalist specialising in technology and security.*

Resources

PandaLabs maintained a blow-by-blow account of the Anonymous campaign, which makes for entertaining reading: <http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/>.

References

1. 'Project Chanology'. Wikipedia. Accessed Jan 2011. <http://en.wikipedia.org/wiki/Project_Chanology>.
2. Prolexic Technologies. <http://www.prolexic.com/>.
3. Leyden, J. 'Second man jailed over Scientology DDoS attacks'. The Register, 25 May 2010. Accessed Jan 2011. <http://www.theregister.co.uk/2010/05/25/second_scientology_ddoser_jailed/>.
4. 'Wall of sauce'. Source code for original LOIC tool. Praetox Technologies. Accessed Jan 2011. <http://praetox.com/n.php/sw/sauce>.
5. Pras, A; Sperotto, A; Moura, G; Drago, I; Barbosa, R; Sadre, R; Schmidt, R; Hofstede, R. 'Attacks by "Anonymous" Wikileaks proponents not anonymous'. University of Twente, 10 Dec 2010. CTIT Technical Report 10.41. <http://www.utwente.nl/ewi/dacs/news/archive/2010/wikileaks.doc/index.html>.
6. High Orbit Ion Cannon DDoS tool. <http://hoic.99k.org/>.

7. Geosynchronous Orbital Ion Cannon source code. Accessed Jan 2011. <http://pastebin.com/FH6njMew>.
8. Moyer, E. 'Report: FBI seizes server in probe of Wikileaks attacks'. CNET, 1 Jan 2011. Accessed Jan 2011. <http://news.cnet.com/8301-13578_3-20026908-38.html>.
9. 'Jester's Court'. <http://th3j35t3r.wordpress.com/>.
10. Leyden, J. 'Anonymous hacktivists fire ion cannons at Zimbabwe'. The Register, 31 Dec 2010. Accessed Jan 2011. <http://www.theregister.co.uk/2010/12/31/anon_hits_zimbabwe_sites/>.
11. Cluley, G. 'Pro-Wikileaks hackers bring down Tunisian government websites'. Naked Security blog, Sophos, 3 Jan 2011. Accessed Jan 2011. <http://nakedsecurity.sophos.com/2011/01/03/pro-wikileaks-hackers-tunisian-government-web-sites>.

Cyber attacks: awareness

Edward G Amoroso, AT&T

In this excerpt from his book, Cyber Attacks: Protecting National Infrastructure, cyber-security expert Edward G Amoroso looks at how you detect infrastructure attacks, manage vulnerability information and manage risk.

Real-time understanding

'Situational awareness' refers to the collective real-time understanding within an organisation of its security risk posture. Security risk measures the likelihood that an attack might produce significant consequences to some set of locally valued assets. A major challenge is that the factors affecting security risk are often not locally controlled and are often deliberately obscured by an adversary. To optimise situation awareness, considerable time, effort and even creativity must be expended.

Sadly, most existing companies and agencies with responsibility for national infrastructure have little or no discipline in this area. This is surprising, as a common question asked by senior leadership is whether the organisation is experiencing a security risk or is 'under attack' at a given time.

Awareness of security posture requires consideration of several technical, operational, business and external or global factors. These include the following:

- **Known vulnerabilities**: detailed knowledge of relevant vulnerabilities from vendors, service providers, government, academia and the hacking community is essential to effective situational awareness. Specific events such as prominent hacking conferences are often a rich source of new vulnerability data.
- **Security infrastructure:** understanding the state of all active security components in the local environment is required for proper situational awareness. This includes knowledge of security software versions for integrity management and anti-malware processing, signature deployments for security devices such as intrusion detection systems, and monitoring status for any types of security collection and processing systems.
- **Network and computing architecture**: knowledge of network and computing architecture is also important to understanding an organisation's situational security posture. An accurate catalogue of all inbound and outbound services through external gateways is particularly important during an incident that might be exploiting specific ports or protocols.
- **Business environment**: security posture is directly related to business activities such as new product launches, new project initiation, public relations press releases, executive action involving anything even mildly controversial, and especially any business failures. Any types of contract negotiations between management and employee bases have a direct impact on the local situational security status.
- **Global threats**: any political or global threats that might be present at a given time will certainly have an impact on an organisation's situational security posture. This must be monitored carefully in regions where an organisation might have created a partnership or outsourcing arrangement. Because outsourcing tends to occur in regions that are remote to the organisation, a global threat posture has become more significant.
- **Hardware and software profiles**: an accurate view of all hardware and software currently in place in the organisation is also essential to situational awareness. A common problem involves running some product version that is too old to properly secure through a programme of patching or security enhancement. A corresponding problem involves systems that are too new to properly characterise their robustness against attack. In practice, an optimal period of product operation emerges between the earliest installation period, when a product or system is brand new, and the latter stages of deployment, when formal support from a vendor might have lapsed (see Figure 1).

Each of these factors presents a set of unique challenges for security teams. An emerging global conflict, for example, will probably have nothing to do with the vulnerability profile of software running locally in an enterprise. There are, however, clear dependencies that arise between factors in practice