Hacktivism: assessing the damage

Steve Mansfield-Devine

Steve Mansfield-Devine

With the rise to stardom of activists Anonymous and hacking group LulzSec, cyber-attacks have entered a new phase. There's nothing original in the technical exploits they're deploying – most are very basic. But unlike most attackers, these groups actually crave publicity and are eager to share the data they steal. They frequently claim that this is for the greater good, to encourage better security and a more responsible custodianship of personal data. These are issues close to the hearts of information security professionals; so will these attacks have an effect on organisations' attitudes to security? And has the infosecurity landscape changed forever?

First, we have to ask, who are these people? And there's no easy answer. These are not well-defined groups with membership lists. And their activities have spawned many imitators and fellow-travellers. There are also some distinctions between the groups defined by the 'members' themselves. This makes labels difficult: 'hacktivists', 'activists', 'hackers', 'members' – even the word 'group' itself – all map very poorly on to how these people organise and operate. However, for the sake of discussion, and brevity, we'll use words like 'group' and 'hacktivists' to encompass Anonymous, LulzSec and those who tag along in their shade.

Anonymous

Anonymous has a long track record of activism, only a portion of it involving hacking. The group first came to public attention as a result of its Project (or Operation) Chanology campaign against the Church of Scientology. This frequently involved 'Anons' gathering in street protests, many wearing the now-iconic Guy Fawkes masks. Anonymous quickly established a style characterised by anarchic wit and portentous (and, many would argue, pretentious) videos. This light-hearted posturing and the nature of its target won Anonymous widespread sympathy.

Its next major campaign could be said to have appealed to a narrower demographic: Operation Payback attacked the music industry for its heavy-handed legal pursuit of filesharers. It also foreshadowed what was to become a characteristic of subsequent operations – a certain superficiality in the arguments supporting them. Underlying Operation Payback (which continues, sporadically, to this day) was a dislike of copyright that was conflated with the self-serving interests of major media corporations and narrowly focused on music and movies. It's a crudity of argument that has resurfaced in the group's attacks on information security companies and 'whitehats'.

The group's ambitions are often couched in terms of uncovering corruption and fighting oppression and use the vocabulary of revolution, even though their activities are commonly perceived as little more than juvenile stunts or vandalism. But this isn't to doubt the authenticity of their motivations or feelings. These were particularly evident during the pro-Wikileaks campaigns which, famously, brought minor grief to the likes of Mastercard and PayPal.[1]

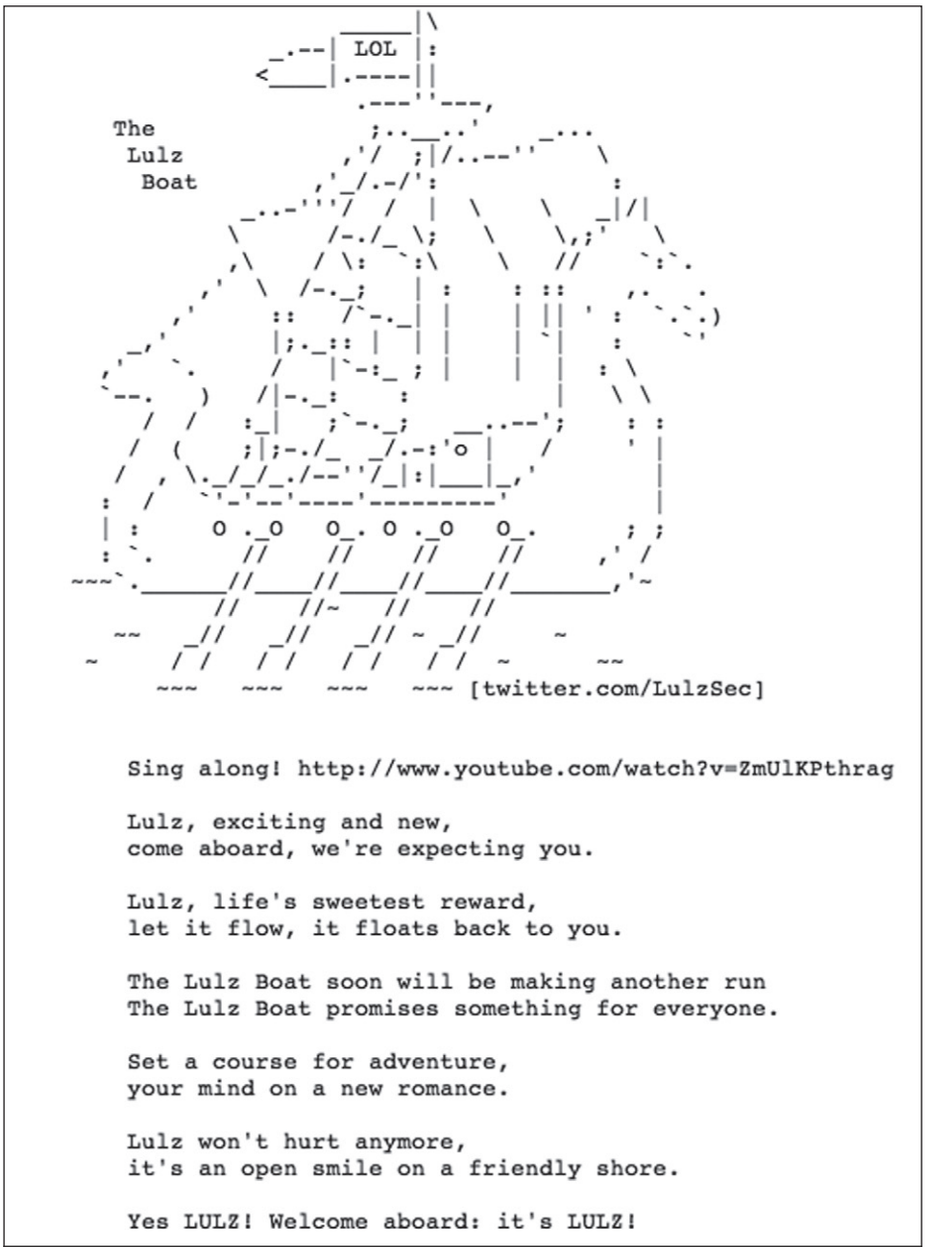
Anonymous says it is leaderless, a claim that is both partially true and disingenuous. Certainly, anyone can join in a campaign – or mount one of their own – under the Anonymous banner. At the same time, there is clearly a core group running key Twitter accounts, producing YouTube videos and controlling important channels (some closed to the general public) on IRC servers. While many of those who join in the campaigns will simply download and use the Low Orbit Ion Cannon (LOIC) DDoS tool, it appears to be this core group that is capable of wielding at least some basic hacking skills. Nevertheless, the key campaigns under the name of Anonymous have tended to use DDoS as the weapon of choice, and a new tool, RefRef, has just made an appearance.[2] This exploits resource exhaustion to take down targets.

The group also continues non-hacking campaigns. Recently, for example, it announced Operation UnManifest in which people are encouraged to modify copies of the manifesto written by Norwegian mass-murderer Anders Breivik, creating versions that ridicule his ideology. By flooding the web with these mauled copies, anyone seeking the manifesto can never be sure they are getting the real thing.[3]

LulzSec

According to LulzSec – or Lulz Security – its hacking activities had no higher purpose but were simply for the 'lulz' – the pure joy of creating mayhem. This assertion has been undermined by the group itself a number of times: in fact, the action that really brought it to public attention was the defacement of a website belonging to the Public Broadcasting Service (PBS) in the US because LulzSec was unhappy with the treatment of Wikileaks in a documentary.

What followed was 50 days of hacking stunts, including repeated attacks on Sony. Many of the attacks resulted in the theft of users' login credentials for websites and other online systems. There were government targets, too, including



LulzSec adopted a whimsical, piratical theme for its announcements.

the CIA and, in the UK, the website of the Serious Organised Crime Agency (SOCA), which was brought down by a DDoS attack.[4]

At first, LulzSec denied any connection with Anonymous. But it soon became apparent that LulzSec members, who probably never numbered more than half a dozen or so, were the same people behind many Anonymous activities and may even represent the people within the Anonymous core with genuine (albeit low-level) hacking skills. This became explicit when LulzSec later admitted responsibility for attacks against security firm HBGary, which were originally claimed by Anonymous. It's worth repeating, though, that the Anonymous name is adopted by a wide variety of people around the world.

AntiSec

In mid-June 2011, LulzSec suddenly announced it was disbanding – or rather, merging with Anonymous as part of a new campaign, AntiSec.[5] The reason for the change was never clear. 'Topiary' – regarded as the mouthpiece of LulzSec – claimed in an interview that the group wanted to quit on: "A high note, a classy ending".[6] Most onlookers, however, believed the decision was driven by the heat the group was starting to feel from law enforcement: the move was part of the hackers' constant attempts at misdirection and disinformation. Shortly before this issue went to press, the Metropolitan Police arrested Jake Davis who, they claim, is Topiary.

The AntiSec campaign is focused on alerting the world to security weaknesses – particularly on the part of government entities and corporates – and what AntiSec sees as dishonesty and ineffectiveness on the part of the information security industry. One early action was the leak of 700 confidential documents from Arizona's Department of Public Safety. Although still seen as a LulzSec attack, it was accompanied by an attempt at justification: "We are targeting AZDPS specifically because we are against SB1070 and the racial profiling anti-immigrant police state that is Arizona," said a statement.[7] Other high-profile stunts included the downloading of large numbers of documents from defence and FBI contractor ManTech, the leaking of emails from the Department of Homeland Security, 90,000 email addresses – many of them military – from defence firm Booz Allen Hamilton, and the defacement of 77 law enforcement websites and the leaking of the personal details (including social security numbers and home addresses) of 7,000 law enforcement officers.[8,9]

Security awareness

AntiSec supporters are not slow in taunting or denigrating 'whitehats'. In a discussion on the AnonOps IRC server, in the #reporter channel used to talk to the press, someone identifying himself as 'joepie91' explained: "The problem most people have with the majority of 'whitehat security researchers' is that they charge insane amounts of money for supposed 'security', and then fail to protect from even the most basic attacks."

(It's important to note that, while joepie90 had admin privileges for the #reporter channel, and others seemed to defer to him, as they did to Anonymous9 during a later chat, this does not make either of them a

spokesman for Anonymous. It is part of the fiction of Anonymous being 'leaderless' that no-one speaks in an official capacity. However, the personal opinions offered during IRC chats echoed those frequently stated by Anons.)

The hostility towards whitehats could be brushed aside as nothing more than name-calling, but perhaps it is more revealing than that. It may demonstrate a fundamental lack of understanding when it comes to the root cause of security vulnerabilities, which isn't a lack of skill or understanding among security professionals, but among those who pay them. It's an institutional or business problem.

"There are lots of good information security professionals out there that have great technical skills, but technical skills alone will not protect your company," says Brian Honan, an independent consultant based in Dublin who specialises in the strategic risk aspects of information security. "You also need to have management skills, budgeting skills and political skills – because you have to make sure that your agenda is part of the company's agenda – and you need to have risk management skills. If I'm an attacker, I can take my time and focus on one element of your infrastructure and try to chip away at that. As an information security professional I have to cover everything. I wouldn't think that many of these people involved in LulzSec or Anonymous have had major networks of tens of thousands of computers spread over different time zones in different jurisdictions with different legal and regulatory requirements and had to try to manage and keep all those things running together at the same time with a very limited budget."

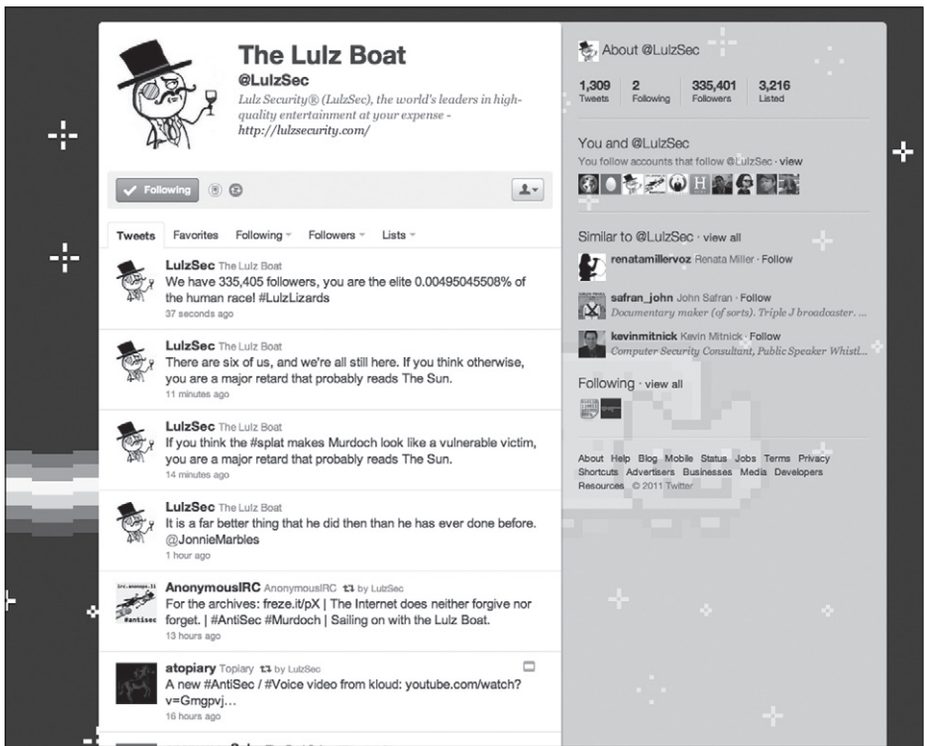
There is some awareness of these issues. In the IRC chats, joepie91 outlined two reasons firms have poor security (chat logs are presented verbatim):

- joepie91: 1. the managers and others in charge of deciding the budgets etc, are underestimating the importance of IT security, and do not have the necessary skills to determine whether their security is acceptable
- joepie91: 2. the 'whitehat security researchers' take advantage of this incapability on the managers side, and charge outrageous amounts of money for things that do not appropriately secure the systems

But even this basic understanding is often skewed by the crude ideology that drives Anonymous. The following is from a chat with Anonymous9, discussing 'whitehats':

- Anonymous9: They like to think of themselves as "the good guys" of hacking, but are they really?
- Anonymous9: Is providing services to governments to allow them to spy on people, to allow them to cover up their abuses, to allow them to break the law – is this positive?
- Anonymous9: "White hat" is a term which essentially describes someone who co operates with the authorities, and often includes co operating with their crimes. So I for one object to the term white hat because it implies they are doing good, when in fact in many cases, they are aiding corruption.

Do they have a point? Richard Hollis is a director of Orthus, an information risk management consultancy in London that works with organisations of all sizes. He believes that the security industry has been fuelling fear, uncertainty and doubt. "I think this is, by and large, pushed by vendors who are saying, be afraid, be very afraid," he says. "In the past two months I've seen the vendors capitalise on what has happened … These guys have a huge marketing machine and have pushed the fear button."



Following a number of arrests, LulzSec announced via Twitter that it was unaffected – but it was clearly feeling the heat.

Illegal activity

None of this alters the fact that most of the hacktivist actions are illegal. And the motivation is largely irrelevant to the victims. "Whether they have an agenda or not, they should be looked at as the same thing," says Chris Wysopal, CTO of Veracode, a firm that provides software security testing. "If you're an organisation trying to figure out if you're at risk from one of these groups and whether you're vulnerable, it doesn't really matter what their motivations are. You want to make sure you're not at risk and your corporate data's not exposed."

In many ways, for infosecurity professionals it's business as usual. "We're

Chris Wysopal, Veracode.

dealing with this stuff every day anyway," says Honan. "Attacks are increasing, but they're increasing because the number of targets is increasing. It's just the natural way of things. The more systems and people come online, the more it's going to attract criminals. What Anonymous and LulzSec seem to have that we haven't had in the past is, to put it bluntly, a better PR machine."

Hacking skills

Although the activities of the hacking groups have been highly effective in generating headlines, the actual results have been mixed. For example, the DDoS attacks by Anonymous in support of Wikileaks achieved only partial and fleeting success. It's assumed that some hacktivists have access to botnets for their DDoS attacks, but even so, DDoS is a crude weapon that requires no hacking at all. So are these skilled hackers?

Francis Brown and Rob Ragan, researchers at Stach and Liu and specialists in the use of search engines for finding web vulnerabilities, have suggested that so-called Google Hacking is a key part of the Anonymous/LulzSec attack toolkit. Basic SQL injection is also clearly used for most of the breaches, and logs leaked by the attackers themselves suggest the use of automation tools such as Havij. And chat logs also suggest remote file inclusion and cross-site scripting are also techniques commonly deployed.

"These guys aren't terribly sophisticated," says Wysopal. "They're certainly a step above script kiddies, but there's a lot of individuals that have the skills sets that these guys do."

Hollis agrees. "I'm a 50 year-old guy and I can do a SQL injection," he says. "And that scares me. So no, they're not impressive. The attacks are not impressive. They've impressed no-one I've ever met in the industry; they're kid's stuff."

The low level of skills displayed is a worry in itself. If hacktivists are achieving this level of mayhem, imagine what real hackers might do. Their apparent high frequency of success is most likely a result of them going for the weak, finding sites and servers with poor security.

"I think they're opportunistic," says Wysopal. "Most attacks of this type are opportunistic. It's rare that you're targeting one piece of data in one organisation. They might pick an organisation, but then they're trying to find any weakness they can. Certainly, there are organisations they've tried to attack and they haven't been able to get in, and you just don't hear about that."

The bigger an organisation is, the more likely it is to have a weak spot somewhere. "Sony is a perfect example of that – the fact that they have so many business units operating in dozens of countries," Wysopal says. "It shows that when you have a far-flung organisation like that it's hard to have a consistent security policy unless you build a security programme that's designed to do that. And most companies do not have a programme like that when it comes to things like the security of their web applications. These web apps are built all over the place by different teams. Some are outsourced. And a lot of organisations don't have any consistent view of the security of those web apps. So you end up with some decent secure ones but you also end up with some insecure ones and these hacktivists take advantage of that to embarrass the whole organisation."

Anonymous boasted that it was holding an archive of NATO documents.

Simple weaknesses

If the skills are basic, that means the flaws they're exploiting are too. Most of the SQL injection flaws should simply not exist. "It's pretty basic," says Wysopal. "I think it just shows that there's been no care to build a lot of these web apps securely, even though they're putting things like their customer data in there."

Anons agree:

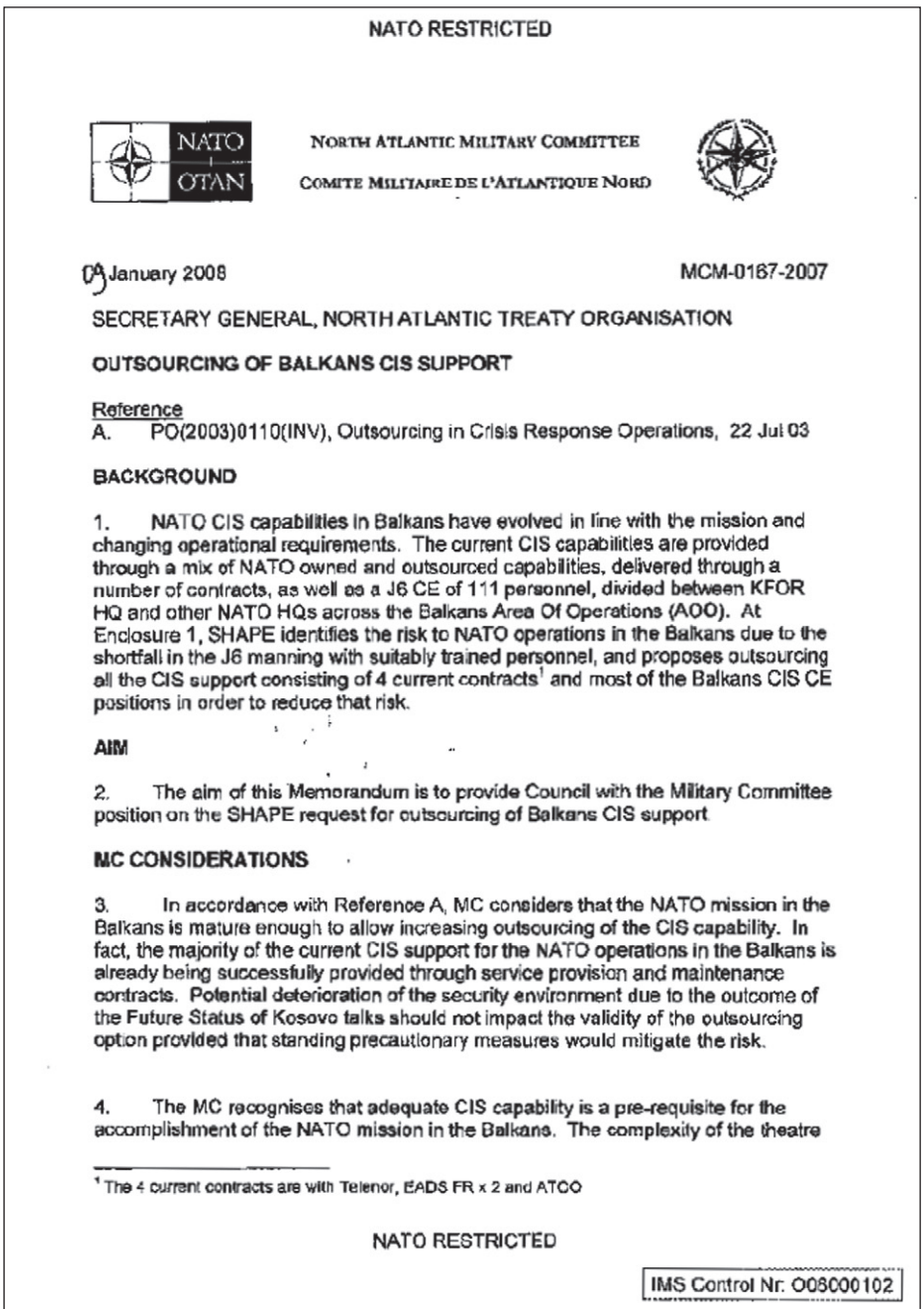
- joepie91: while I am fairly sure that not everything is SQL injection, there have been a *lot* of intrusions that were so basic they shouldn't have been possible
- joepie91: points of entry you would have expected from a 13 year old kids self-programmed forum, but not from a large corporation and/or 'respectable' security firm

Other basic mistakes are evident, too. LulzSec's hack of *The Sun* started with the breach of a temporary system, set up when News International was creating a paywall for its online content. Although no longer in use, this system still had

links through to the company's main servers, including the content management system for its newspaper websites and the email system. It was a classic lateral entry from an unregarded, insecure server into a business-critical (and presumably better secured) system.[10]

Before dismissing hacktivists as script kiddies, though, it's worth considering if these basic techniques are all they need.

"I suspect they're doing whatever's necessary, as a real penetration testing outfit would," says Peter Wood, CEO of security consultancy and pen-testing firm First Base Technologies and member of the ISACA Security Advisory Group. "If you can make your point and get the board's attention – legitimately and legally, of course – by a simple attack, surely that's almost more important because the simpler the attack the more likely it is to take place in the real world. I don't denigrate people for using simplistic attacks. If people are operating outside the law using attacks to show how clever they are, then I'd imagine they'd want to make as sophisticated an attack as possible. But if they have another agenda, which is, perhaps, to make the target organisation look stupid, or to make a political point, they all they need to do is whatever they need to do. It's whatever anybody would do – you take the easiest route. I'm not sure if it reflects what they're capable of: I think it reflects what was open to them."



NATO RESTRICTED

NATO OTAN

NORTH ATLANTIC MILITARY COMMITTEE

COMITE MILITAIRE DE L'ATLANTIQUE NORD

09 January 2008 MCM-0167-2007

SECRETARY GENERAL, NORTH ATLANTIC TREATY ORGANISATION

OUTSOURCING OF BALKANS CIS SUPPORT

Reference
A. PO(2003)0110(INV), Outsourcing in Crisis Response Operations, 22 Jul 03

BACKGROUND

1. NATO CIS capabilities in Balkans have evolved in line with the mission and changing operational requirements. The current CIS capabilities are provided through a mix of NATO owned and outsourced capabilities, delivered through a number of contracts, as well as a J6 CE of 111 personnel, divided between KFOR HQ and other NATO HQs across the Balkans Area Of Operations (AOO). At Enclosure 1, SHAPE identifies the risk to NATO operations in the Balkans due to the shortfall in the J6 manning with suitably trained personnel, and proposes outsourcing all the CIS support consisting of 4 current contracts[1] and most of the Balkans CIS CE positions in order to reduce that risk.

AIM

2. The aim of this Memorandum is to provide Council with the Military Committee position on the SHAPE request for outsourcing of Balkans CIS support.

MC CONSIDERATIONS

3. In accordance with Reference A, MC considers that the NATO mission in the Balkans is mature enough to allow increasing outsourcing of the CIS capability. In fact, the majority of the current CIS support for the NATO operations in the Balkans is already being successfully provided through service provision and maintenance contracts. Potential deterioration of the security environment due to the outcome of the Future Status of Kosovo talks should not impact the validity of the outsourcing option provided that standing precautionary measures would mitigate the risk.

4. The MC recognises that adequate CIS capability is a pre-requisite for the accomplishment of the NATO mission in the Balkans. The complexity of the theatre

[1] The 4 current contracts are with Telenor, EADS FR x 2 and ATCO

NATO RESTRICTED

IMS Control Nr: 008000102

The NATO documents that Anonymous leaked actually had the lowest level of security.

Getting results

So how impressive were the results? A recent CNN Money story started "LulzSec took down the CIA's website in mid-June".[11] That's a good way of grabbing people's attention, but it's not as serious as it sounds. Many of the recent hacktivist attacks resulted in simple website defacement or denial of service. And where information has been leaked, most of it is low-grade and insignificant.

For example, one attack that was touted by the press as hackers breaching NATO's defences, turned out to be a relatively trivial breach of a NATO bookshop. LulzSec has even 'leaked' publicly available information.[12] In mid-July, Anonymous announced that it had hacked into Monsanto – known for its work in genetic modification – and posted information on what the group claimed were 2,500 employees.[13] Monsanto admitted that the breach had occurred but countered that much of the information was publicly available anyway, and that most of the 'employees' were not actually connected to the company, but worked for other firms.

Around the same time, Anonymous announced that it had hacked NATO and was sitting on 1GB of documents, which it wasn't yet releasing because to do so would be "irresponsible". This apparent attack of scruples struck many as a new development. But it's possible there was another reason for the lack of disclosure. The one document the group did release – HQ ISAF JOINT CIS CONTROL CENTRE – dating from 2007, was classified as 'NATO restricted', which is actually the lowest level of protective classification. In fact, according to Lewis Page, ex-Royal Navy officer and now journalist, writing on The Register website, documents intended for NATO distribution rarely contain sensitive information, and with those carrying such a low classification, it's pretty much assumed that they will be leaked.[14]

A hack of The Sun newspaper resulted in LulzSec posting a fake news story.

"RESTRICTED information is so unimportant that hard copies don't even have to be shredded on disposal," he wrote. "Add a NATO prefix and you have something completely insignificant." So the decision by Anonymous not to publish may have been motivated by the sheer triviality of the material. Of course, the fact that a NATO site was hacked at all is an embarrassment for the organisation.

LulzSec briefly came out of 'retirement' to hack *The Sun* newspaper, briefly putting a spoof story on its website. The stunt provided some entertainment, but was generally overwhelmed by the far more significant story of phone hacking that was consuming the attention of most people in the UK. LulzSec claimed to have a large hoard of emails but withdrew its early promise to publish them. The group made a vague statement about working with news organisations – in the manner of Wikileaks – but that has yet to come to anything.[15] A couple of weeks later, *The Sun* was hacked again by someone operating under the name Batteye, who leaked a database containing details of Miss Scotland 2010 contestants – hardly a revolutionary act, although it has forced the organisation to contact a number of people to warn that personal details have been leaked.[16]

Collateral damage

Indeed, the organisations targeted by hacktivists are not the only victims. The spilling of personal details, such as login credentials, email addresses and even physical addresses puts many innocent people at greater risk of phishing, spamming and ID theft. Or worse. The attacks against Arizonan law enforcement, for example, have put into the public domain sensitive information about police officers. This is information that could be used by criminals seeking revenge.

The hacktivists' response to this is typically cavalier. Mentioning it usually elicits a blithe assertion that, once leaked, this information becomes useless to the genuinely bad guys, because people will change their login details. This assumes, of course, that everyone affected knows their details have been leaked (reflecting, perhaps, the high opinion Anons have of their own social significance) and understand that they need to do something about it – which may not be easy. In one instance, LulzSec actually encouraged followers to use leaked information to take over people's Facebook and Twitter accounts to embarrass them. This was in connection with login details taken from a porn site, adding a surprisingly conservative element of moral judgement.

Damage done

The public nature of the disclosures is important, and the facet of this hacktivism phenomenon that so crucially distinguishes it from other forms of hacking. Organisations affected have no choice about whether they disclose the breach. And the hacktivists are not just announcing that the breach has happened, but often share details of how it happened. And they usually share the spoils.

One problem for hacktivists looking to make a point is that their activities are generally of such low impact that they fail to rise above the overall noise. For example, many of the attacks by Anonymous and LulzSec have been website defacements – an activity that happens practically every day, for a variety of motives or no motive at all. Even the data breaches have to compete with a flood of others. Ironically, the very transparency that Anonymous claims it wants is presenting it with a problem. In many places now, companies are obliged to confess data breaches. This makes them a wearily familiar occurrence. It's therefore difficult for politically motivated data breaches to differentiate themselves and gain public awareness. The high profile – or notoriety, if you prefer – that Anonymous and LulzSec have achieved is the result more of the groups' self-publicity than the significance of their actions.

There is an associated problem, too, which is to do with reputational damage. Although it seems self-evident that, for example, the leaking of customer data will erode the public's confidence in an organisation and degrade the value of its brand, there is a question mark over just how important this is, especially over the long term. The worry for a hacked company is that customers will abandon it at the time the breach is made public, and other people will be disinclined to buy products or services in the future.

- Anonymous9: For example, you would hope to trust a company like Viacom with your data when you subscribe to them. You're handing over your credit card, contact details, media preferences, the lot.
- Anonymous9: Now, how do you feel knowing that a small team of Lulzsec hackers managed to breach their servers and download an absolutely colossal amount of information from them?

However, there's no proof that this has happened to any of the commercial organisations attacked by hacktivists (with the possible exception of Sony).

For people in the security business – infosec professionals, geeks and hackers – having a database of login credentials leaked is close to a cardinal sin. To the general public, it's yet another data breach in a daily litany of such failings. And the fact that these breaches do not involve sensitive data, such as health records or credit card information, means they probably barely register on the public's radar. Far from discouraging future customers, it's just as likely that these attacks won't be remembered by most people outside those keenly interested in this subject. And if they are, they will be recalled as the work of just another bunch of cyber-criminals. Sony is a special case, but even there a cynic might conjecture that antipathy towards the firm (perhaps even among Anons) might last only up until the release of the next cool PlayStation game.

Business and market sentiment is another matter. In assessing the damage, one can track stock prices, but only over the very short term – long-term there are too many other factors in play to isolate the impact of just the hacking attacks.

Periodic problem

Even those firms that care about reputational damage (and not all do) generally treat this as a phase they need to go through. Put simply, they know that time is a healer. For all the public humiliation and apologising, Hollis believes that most executives in Sony do not regard the recent breaches as a 'significant' hack. "You know what Sony thinks is a significant hack?" he says. "Taking their avatars for their games. That's big money … that would have a genuine impact on them, on their business, their bottom line."

Sony came under repeated and sustained attack. In the US, the firm is facing as many as 55 class-action suits following the breach of up to 100 million records containing personal information. There are three more cases in Canada. Normally, an organisation would look to its insurers to protect it from financial damage under these circumstances, but its insurer – Zurich American Insurance – has gone to the courts seeking absolution from any requirement to cover the costs. Zurich American is claiming the policy only covers "bodily injury" and "property damage".[17] So Sony may be seriously out of pocket when the dust settles. Or not, depending which way the courts decide. In any case, Sony might be calculating that the cost of this kind of action is still less than ensuring that all its servers are secured.

"We haven't seen a lot of credit card danger exposed," says Wysopal, "which has a real cost associated with the type of response – sending out notices to customers, perhaps re-issuing credit cards – those things have real significant cost associated with them." The leak of customer logins or email addresses might be seen as relatively unimportant by many firms, he adds. "There's no real hard cost. You have to investigate it and you have to fix the problem, but it's not as bad as if it was PII [Personally Identifiable Information] exposed."

This may explain why the sites were so poorly protected. "Protected against what?" asks Hollis. "If this was bank account numbers and authentication, then we'd be having a different conversation, but I don't see any value in this material. While it's private, the severity of disclosure of this causes little or no impact on corporations other than this reputational damage. This is not low-hanging fruit – this is fruit that's on the ground and you're stepping on it, as far as security is concerned."

Raising security awareness

So if the reputational damage is short-lived and the material leaked insignificant, what about the other hacktivist ambition of raising security awareness? Wood believes that these high-profile hacks have achieved that, although he's uncertain for how long.

"Every time there's some kind of very high profile event, or series of events, it seems to capture the attention of, for example, risk insurance committees, non-executive directors, senior people," he says, "and they will inevitably bring it to the table at audit and risk meetings. As a result, we see a lot more attention being given to information security than when these events don't happen." But, he adds, senior executives, "have about a three-week memory for these things."

He adds: "I think what we're seeing here is what the industry's been saying for years and years – that systems aren't patched up to date like they should be. We continually say to clients that the general public isn't interested in understanding the difference between a well-protected database containing their credit card data and some marketing database put in place with your badge on by a third party. As far as they're concerned, it's all you. If they're not going to do due diligence across the whole estate, understand what they've got in place and make sure they're all secure to a decent standard, they're going to get this sort of problem."

It's the old story of security operations being under-resourced. But that is unlikely to change, thinks Hollis, because firms aren't seeing this as a serious issue. "I haven't seen any difference whatsoever in implementing a more heightened defence mechanism because of this. In the last two months I've probably discussed this with at least 50 clients and across the board I can say, without a doubt, everybody sees this as nuisance hacking by a bunch of kids who are looking for some press."

And Honan isn't seeing companies beat a path to his door because of LulzSec and Anonymous. His clients, he explains, are already security aware. "If companies are reacting only to Anonymous and LulzSec attacks, I would posit that they have bigger security issues than having to deal with Anonymous and LulzSec because there would be motivated criminals and organised crime who will be taking advantage of these weaknesses and causing more long-term damage than simply

defacing your website or giving you bad publicity for a few weeks."

Good effect?

Nevertheless, maybe the attention might have some beneficial effects, if only to change attitudes towards the value of security professionals. "A large number of people in the infosecurity community are relieved that someone has finally got the attention of so many major organisations," says Wood. These attacks, he adds, highlight, "the difference between vulnerability assessment and penetration testing." They're like penetration testing with no holds barred. "And, of course, without permission, which is the bad bit. We find that a lot of organisations are reluctant to have a proper, ethical, approved penetration test against live systems because they're concerned that it could damage uptime. It's very common for penetration testing companies to be asked to do a penetration test that's really nothing more than a glorified vulnerability scan. Sometimes that's more than adequate, other times it isn't. As a result, these systems never get properly tested."

The result, according to Honan, is that, "It's made our jobs a bit more under the spotlight. Anybody in that [security] role needs to take advantage of that and try to use it to highlight any issues – but be very aware that if anything does go wrong, well the spotlight is still shining there." And while these events have put more pressure on infosecurity professionals, they haven't necessarily given them any more prestige within the company, he warns. "I haven't seen any major change in corporate culture with regard to security. What has happened is that the senior management have turned around to the security guys and said 'make sure it doesn't happen to us', which is a very reactive way to deal with security. The mature way is to do the risk analysis."

What firms need to do right now, according to Wood, is, "invest internally in sufficient resources, listen to the security people inside your organisation and actually examine the systems from inside. That's going to give you the best picture of what's right and wrong. And I'd start the remediation now."

This means examining all your systems, and in many cases asking whether you really need them. A full audit and pen-test of every server may be unfeasible, says Wysopal, but you at least need to do lightweight testing across the board, "to keep out the lowest level attackers." But remediation is going to be a major undertaking for many firms. "There are companies out there that literally have thousands of websites," he adds. "And there are plenty of companies that have over 100. That's a significant amount of assessment work."

Changed equation

Companies balance the cost of such work against the likelihood of attack and the resultant impact. These hacktivist attacks may have changed that risk equation. "Most companies that have brand names to protect, or who have to have an image of trust, are looking at this and saying, this is a new threat to my organisation that wasn't in my equation before and I have to deal with that," says Wysopal. "And it's not hypothetical: it's very palpable to companies now."

But Hollis isn't convinced that every organisation will make changes. He believes that many have looked at the risk equation and have concluded it's fine as it is. "Right now, they're as tight as they want to be," he says. "This is not a new development, it's low-level hacking on a high-profile scale. They're already pretty much aligned and focused on what they're trying to protect online."

The basic weaknesses the hackers exploited weren't always due to laxity, Hollis feels. The firms could easily have made the systems secure. "The reason they're not is that they have bigger fish to fry and it's not part of their business plan to protect logons and passwords on that scale. They never set out to protect this information. So while it's embarrassing on a public scale, on a risk-assessment scale, this doesn't even register."

Encourager les autres

Are we likely to see more of this in the future? "Inevitably," says Wood. "It appeals, particularly to younger people, to be anti-establishment. It's bound to be appealing to people of an impressionable age."

And Hollis adds: "Wait until the next LulzSec. The part that worries me is that the next group will have to out-do LulzSec." Sooner or later the breaches will become serious, he says. "They're going to cross a line. It's like reality TV – it just can't get bad enough to make us stop watching it. This is nuisance hacking, and the next guys that come along are going to take it to a new height and somewhere a line is going to be crossed. I think it's a year away myself."

About the author

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

References

1. Mansfield-Devine, Steve. 'Anonymous: serious threat or mere annoyance?'. Network Security, Jan 2011, pg4.
2. '#RefRef – Denial of Service (DDoS) Tool Developed by Anonymous'. The Hacker News, July 2011. Accessed Aug 2011. <http://www.thehackernews.com/2011/07/refref-denial-of-service-ddos-tool.html>.
3. Ramadge, Andrew. 'Anonymous bid to destroy Norwegian killer Anders Behring Breivik's manifesto'. News.com.au, 26 Jul 2011. Accessed Aug 2011. <http://www.news.com.au/technology/anonymous-bid-to-destroy-norwegian-killer-anders-behring-breiviks-manifesto/story-e6frfro0-1226102267855>.
4. Cluley, Graham. 'SOCA website scalp claimed by LulzSec in apparent DDoS attack'. Naked Security, 20 Jun 2011. Accessed Aug 2011. <http://nakedsecurity.sophos.com/2011/06/20/soca-website-scalp-claimed-by-lulzsec-in-apparent-ddos-attack/>.
5. 'Operation Anti-Security'. Pastebin 19 Jun 2011. Accessed Aug 2011. <http://pastebin.com/9KyA0E5v>.
6. Gallagher, Ryan. 'A passion for change – LulzSec interview'.

OpenDemocracy, 22 July 2011. Accessed Aug 2011. <http://www.opendemocracy.net/ryan-gallagher/passion-for-change-lulzsec-interview>.
7. Beschizza, Rob. 'LulzSec leaks Arizona law enforcement papers'. BoingBoing, 23 Jun 2011. Accessed Aug 2011. <http://boingboing.net/2011/06/23/breaking-lulzsec-lea.html>.
8. Lennon, Mike. 'Anonymous Hacks ManTech, FBI Cybersecurity Contractor'. Security Week, 29 July 2011, Accessed Aug 2011. <http://www.securityweek.com/anonymous-claims-it-hacked-mantech-fbi-cyber-security-contractor>.
9. '90k email accounts exposed in Military Meltdown Monday'. CSO Online, 11 Jul 2011. Accessed Aug 2011. <http://blogs.csoonline.com/1591/90k_email_accounts_exposed_in_military_meltdown_monday>.
10. Leyden, John. 'How LulzSec pwned The Sun'. The Register, 19 Jul 2011. Accessed Aug 2011. <http://www.theregister.co.uk/2011/07/19/sun_lulzsec_hack/>.
11. Goldman, David. 'LulzSec and Anonymous are the least of your hacker worries'. CNN Money, 25 Jul 2011. Accessed Aug 2011. <http://money.cnn.com/2011/07/25/technology/lulzsec_anonymous_hackers/>.
12. Chirgwin, Richard. 'Operation Antisec lames out again'. The Register, 4 jul 2011. Accessed Aug 2011. <http://www.theregister.co.uk/2011/07/04/when_is_a_leak_not_a_leak/>.
13. Lemos, Robert. 'Hacktivism moves from pranks to problems'. InfoWord, 14 Jul 2011. Accessed Aug 2011. <http://www.infoworld.com/d/security/hacktivism-moves-pranks-problems-997>.
14. Page, Lewis. 'NATO Restricted: The lowest possible classification'. The Register, 1 Jul 2011. Accessed Aug 2011. <http://www.theregister.co.uk/2011/07/21/nato_restricted/>.
15. Leyden, John. 'LulzSec hacker Sabu: Murdoch emails sometime soon'. The Register, 20 Jul 2011. Accessed Aug 2011. <http://www.theregister.co.uk/2011/07/20/lulzsec_ni_hack_latest/>.
16. 'The Sun – Hacked Miss Scotland 2010'. Pastebin, 30 Jul 2011. Accessed Aug 2011. <http://pastebin.com/ymrB97iR>.
17. Vijayan, Jaikumar. 'Zurich lawsuit against Sony highlights cyber insurance shortcomings'. Computerworld, 26 Jul 2011. Accessed Aug 2011. <http://www.computerworld.com/s/article/9218639/Zurich_lawsuit_against_Sony_highlights_cyber_insurance_shortcomings>.

IPv6: new technology, new threats

Avi Turiel, Commtouch

Avi Turiel

As wider deployment of IPv6 begins, organisations need to consider the security risks. In February 2011 the final blocks of IPv4 addresses were allocated to the five Regional Internet Registries around the world. The regional registries will continue to allocate these IPv4 addresses (each allocated block represents about 16 million IP addresses) among the numerous ISPs and organisations in each region until the IPv4 addresses are exhausted, which is estimated to occur in late 2011. As a result of this impending IPv4 address exhaustion, many organisations have begun to more seriously consider their roadmaps to IPv6, the successor to IPv4. As the global implementation of IPv6 becomes a reality, the associated security concerns must be considered.

IPv6 technology overview

IPv6 was standardised in 1998 by the Internet Engineering Task Force (IETF) primarily to deal with the anticipated IPv4 address exhaustion. IPv6 includes several enhancements over IPv4 such as simplified address assignment with no need for the DHCP (Dynamic Host Configuration Protocol) used in IPv4.

There are also enhancements to quality of service and security – for example, IPv6 includes IPSec, an end-to-end security protocol that operates at the Internet layer and includes authentication and encryption capabilities. The primary driver for IPv6 adoption, however, is the vastly increased address space:

- IPv4 allows about 4,294,967,296 addresses (32-bit address).
- IPv6 allows 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (128-bit address).

For a global population of 7 billion people this equates to 48,571 trillion trillion addresses per person (although the structure of the allocations will not allow this). In such an environment, Internet addresses can be provided not only to current 'users' such as the computers, tablets and smartphones that are networked today, but also cars, refrigerators, microwaves, light bulbs, watches and many more everyday household devices.

To better understand IPv6, it is important to note that the new address representation differs from that of IPv4 due to the larger address field. IPv6 addresses use hex notation – for example: 3FFE:1900:4545:3:200:F8FF:FE21:67CF. Web