Syrian Electronic Army's attack on Reuters makes a mockery of cyber-security (again)

June 25 2014, by Bill Buchanan

Hacktivist group SEA's message for Reuters users on Sunday SEA

One big security issue that has arisen lately concerns control of news media. National boundaries have become blurred on the internet, and the control any nation can have over information dissemination has been eroded – on news websites but especially on open platforms such as Twitter and Facebook.

Witness the activities of the Syrian Electronic Army (SEA), a pro-Assad group of "hacktivists", which despite limited resources managed to

compromise one of the leading news agencies in the world. It wasn't even the first time – it has already attacked the agency several times before, not to mention its other attacks on the Financial Times, Washington Post, New York Times and Associated Press.

At midday on Sunday, people reading Reuters content found themselves redirected to a page which stated:

Where last year, for example, the SEA attack involved tweeting links to pro-Assad propaganda from the Reuters Twitter account, this time it targeted Reuters content directly. But instead of targeting the agency's site, the hack attacked the news content that it hosts on the sites of a large number of media outlets.

This is not the first time the SEA had attacked in a way that compromised the trusted partners of the major media outlets. It did something similar to the New York Times last August.

In this most recent case, the SEA appears to have redirected viewers to the bogus pages by compromising advertising hosted by a Reuters partner site called Taboola. This could have serious consequences for Taboola's other clients, who include Yahoo!, BBC Worldwide and Fox News; and will generally be great worry to many sites.

Look what the spear phishing dragged in …

Another possibility for what lay behind the latest Reuters attack was one of the most common methods of compromise – a spear phishing email, similar to the one that the SEA used to attack satirical site The Onion last year.

This involved a person in the company clicking on what seemed to be a link to a lead story from the Washington Post but turned out to be

malicious. It re-directed the user to another site and then asked for Google Apps credentials. Once these had been keyed in, the SEA gained access to The Onion's web infrastructure and managed to post a story.

While it took a while for The Onion to understand what had happened, Reuters quickly detected the compromise and had fixed the content within 20 minutes. But in classic form, when The Onion had got on top of the problem, it posted an article whose headline read, Syrian Electronic Army Has A Little Fun Before Inevitable Upcoming Death At Hands of Rebels.

These examples illustrate that organisations need to understand that there are new risks within the information age and there are new ways to distribute messages, especially from hackers skillful enough to be able to disrupt traditional forms for dissemination.

The nature of the cause is likely to vary widely. In 2011, for example, Tunisian government websites were attacked by dissident group Anonymous because of Wikileaks censorship.

The same year, the Sony Playstation Network was hacked after Sony said it would name and shame the person responsible for hacking its consoles. This showed that just because you are small on the internet doesn't mean you cannot have a massive impact. Sony ended up losing billions on its share price and lost a great deal of customer confidence.

HBGary Federal vs Anonymous

The attack on security firm HBGary Federal is perhaps the best one in terms of how organisations need to understand their threat landscape. It started when Aaron Barr, the security firm's chief executive, announced it would unmask some of the key people involved in Anonymous, and contacted a host of agencies, including the the US National Security

Agency and Interpol.

Anonymous bounced a message back saying HBGary shouldn't do this, as it would retaliate. As a leading security organisation, HBGary thought it could cope and went ahead with its threat.

Anonymous then searched the HBGary content management system and found it could get access to a complete database of usernames and hashed passwords by inserting a simple PHP embed.

As the passwords were not encrypted, it was an easy task to reverse engineer the hashes back to the original password. Their target, though, was Aaron Barr and his chief operating officer, Ted Vera, each of which used weak passwords of six characters and two numbers, which are easily broken.

Having obtained their login details, Anonymous moved on to other targets. Surely they wouldn't have used the same password for their other accounts? Sure enough they had, including the likes of Twitter and Gmail, which allowed access to gigabytes of research information. Then the hackers noticed that the system administrator for their Gmail email account was called Aaron. As a result they managed to gain complete control of the company email system, which included the email system for the Dutch police.

Latterly they went after top security expert Greg Hoglund, who owned HBGary. This involved sending him an email from within the Gmail account, from the system administrator, asking for him to confirm a key system password. After Hoglund replied back with it, Anonymous then went on to compromise his accounts.

HBGary Federal ended up being closed down due to the adverse publicity around the hack. Having said that, its partner company,

HBGary, has gone from strength to strength. Hoglund is well known for making visionary presentations on computer security around the world. The word in the industry is that HBGary still did pass the Anonymous names to the American authorities, but no one knows for sure.

Conclusions

One lesson from all of this is that a focus of any attempted hack will be a spear phishing email. Tricking users into entering their details may be simple, but it can be very serious. For example the Reuters site integrates more than 30 third-party/advertising network agencies into its content. A breach on any of these could compromise the agency's whole infrastructure.

I'll end with a few straightforward pieces of advice that anyone who cares about security ought to follow:

- Use strong passwords
- Never re-use passwords
- Patch systems
- Watch out for internal emails from bogus sources
- Beware external websites that integrate with your organisation's site.
- Get a service level agreement (SLA) from your cloud provider. This should state how quickly the provider will react to requests for a lockdown of sensitive information, along with providing auditing information to trace the compromise
- Don't store emails in the cloud
- Test your web software for scripting attacks

Source: The Conversation