

Network Box white paper: Hacks, Hoaxes and Horrors

Most of the hoaxes people encounter these days come to them via the Internet. The number of opportunistic and targeted Internet-based crimes and misdemeanours carried out every day results in stolen data and damaged systems, and costs companies many hundreds of thousands of pounds. Other threats are more personal, attacking individuals and stealing their money and in extreme cases, much worse. However, the vast majority of users' day-to-day experiences are positive, and being aware and prepared can help prevent them from falling victim to cyber-crime.

In this document, we will look at examples of Internet-based crime, and highlight some activities that have been used to access data or part unsuspecting victims from their (or their company's) money. You will be familiar with some of these exploits; others may be new. But most importantly, sharing these stories with your users might help prevent them from falling for scams which could damage either them, or your company network.

Hacks

The word 'hack' is much used and has many meanings – depending on who's using it. A 'quick' hack often describes a quick solution to a programming problem: it may not be the most elegant solution, but it gets the job done, and is carried out legally.

However, in what follows I will be using 'hack' to describe how individuals can hack *into* a system *illegally*.

Hackers in this context are looking for vulnerabilities. These are usually dependent on identifying what services are open and therefore vulnerable. So, if a company hosts its own website, it will have a web server available on TCP port 80 and probably 443 as well. The first step of any hacker is to 'enumerate' or identify what services are available for them to attack. If there is nothing responding, they will have to attack the firewall, and that should be a whole order of magnitude harder. If you can see what is responding, you may be able to see if you can identify the service's weakness.

Finding out the type and version number is a good first step in this process. Many email servers proudly announce which server they are simply by connecting to port 25:

```
#> telnet xxx.yyy.1.123 25
Trying xxx.yyy.1.123...
Connected to xxx.yyy.1.123.
Escape character is '^]'.
220 exchange.acme.co.uk Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959 ready at
Wed, 17 Jun 2009 14:13:51 +0100.
```

If there are any vulnerabilities in the version of Exchange you are using, the hacker can now try them out without wasting time on exploits that may have been patched by this version of the software. This is true of any applications that are facing the Internet: giving away information like the name of the application and its version number makes a hacker's life a lot easier.

However, many of these loopholes have been closed with IT managers being much more aware, and the vendors themselves having patched the vulnerabilities. So hackers have moved on. Attacking mainstream applications that are well-established, heavily-used and patched regularly with auto updates, is increasingly difficult. So, hackers want applications that have just been written by teams that may not use a secure development lifecycle (SDL) process. And with the advent of Web 2.0 and VM (Virtual Machine) software, there are a lot of these about.

Perhaps the saddest tale to tell just recently is of Kloxo, previously and better known as LXAdmin. HyperVM, a virtualization application made by LXLabs was riddled with vulnerabilities (listed here: <http://www.milw0rm.com/exploits/8880>) which had a number of exploits that allow hackers to access a system running HyperVM. Over the weekend of 6th/7th June 2009, Vaserv.com, a hosting company had over 100,000 websites deleted from their systems. Both Vaserv and their customers were devastated by the attack. Many customers did not have their sites backed up, as they had not taken up that service from Vaserv. Immediately, these companies were losing money, facing the possibility of having to recreate their websites from scratch. The story has a tragic ending. Kloxo's CEO, K T Ligesh, committed suicide on the Monday, presumably unable to take this final blow to a life already blighted by the suicide of his mother and sister. This is a salutary lesson that hacking is no longer the diversion for adolescences it used to be. The stakes are now much higher, and the impact not just financial.

Another form of attack that has been very common is Structure Query Language (SQL) attacks. The method is to use an ordinary entry field, usually on a website, like the login or password fields. Instead of putting in the expected data, put in a specially crafted command using SQL. The intention is that the command's input will be run against the database if the input is not correctly validated by the website's code. So, a simple example would be that instead of entering:

john.smith

When asked for a username, the hacker enters something like:

```
` or 1=1; delete from users where 1 or username = ''; --
```

The intention is to get the code to accept this and present it as a command straight to the SQL database. The result would be to delete all users from the database. Very complex SQL commands can be written to make this attack sophisticated. Indeed, many hackers will investigate forms and try and generate error messages so that they can find out the names of database fields. For instance, a deliberately obfuscated login form currently gives the following if a single quote is put in both username and password fields:

```
1064: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ')' at line 1
SELECT users.*, acme.company_name FROM users, acme WHERE users.username = '' AND users.company_id = acme.company_id AND users.password = password('');
```

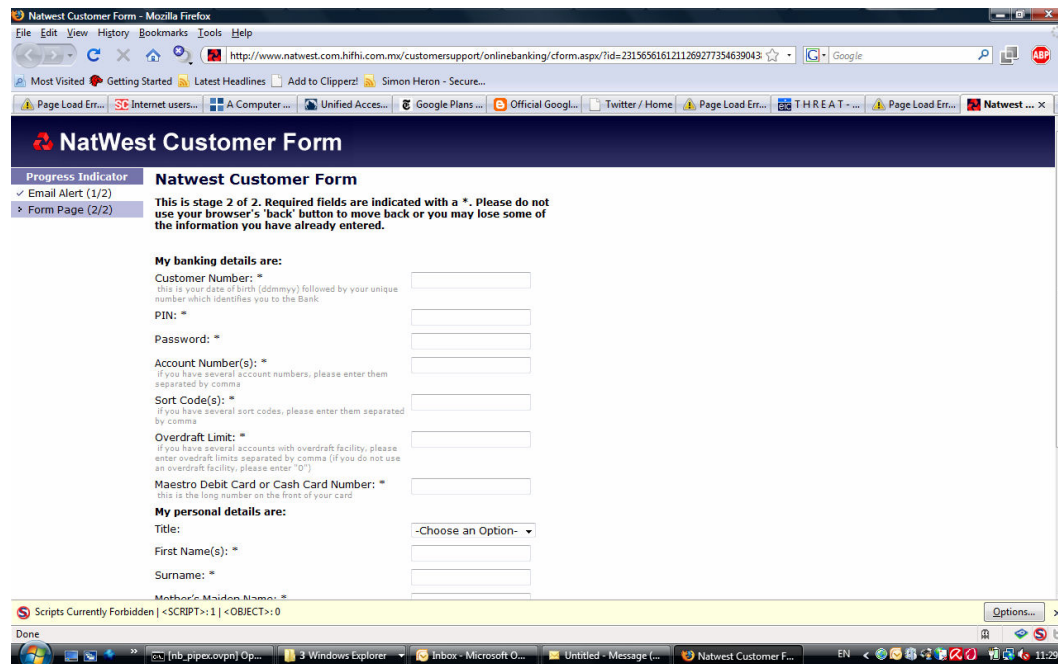
Now the hacker has the names of the fields. This is a good step towards manipulating the database if the correct validation and protection has not been put into the code.

In the summer of 2008, there were two attacks that infected more than half a million websites through SQL injection attacks. This meant that trusted sites which had a good reputation with their visitors would be serving up malware, which their users were much more likely to agree to run, as it was coming from a site they trusted – either having visited it safely before, or recommended to them.

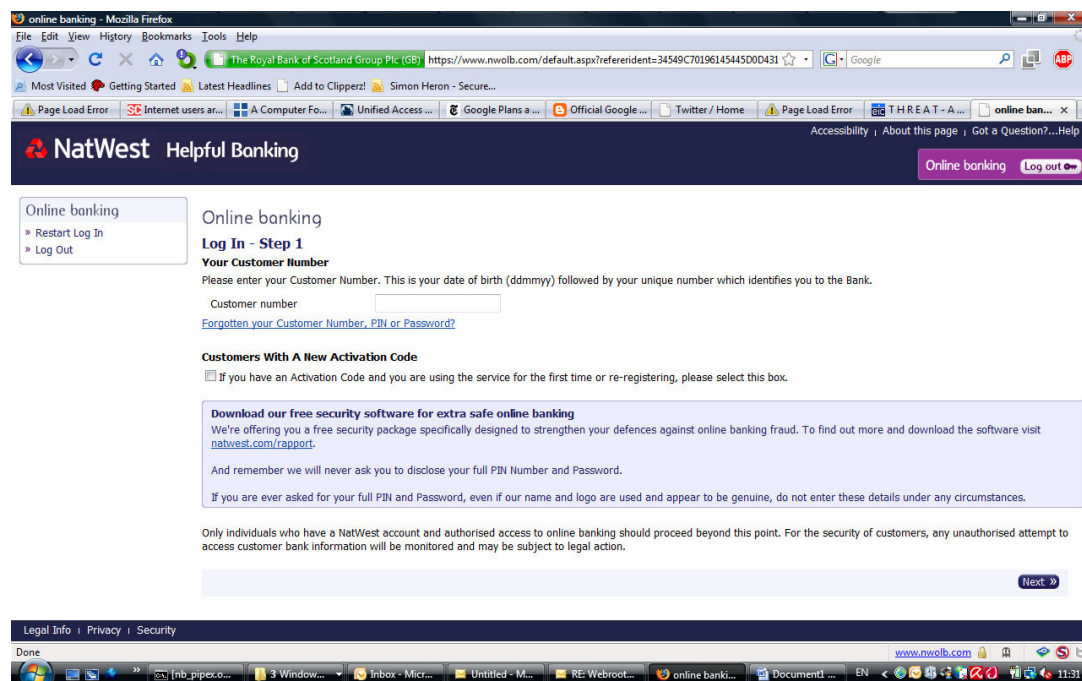
The lesson here is to take basic steps in protecting servers and websites. If you make it harder than the company at the next IP address, the hacker will move on. It's not personal.

Hoaxes

A recent survey by YouGov and VeriSign revealed that 88 per cent of web users were unable to distinguish a phishing site from an official page when presented side by side. This is not too surprising when you look at some of the sites being generated by phishers. As a test, is the following the real Natwest site?



Or is this?



A moment's pause will easily identify the first as the hoax:

- There is no padlock indicating the authenticity of the site
- There is no https, a must for when sending secure information across the Internet
- The URL is bogus: the most obvious and most easily overlooked hoax.

But it is not a bad pass at the site. It is certainly sufficiently professional to fool a significant number of people, and these forgeries are getting better all the time. While the tests indicated above are being also mimicked by fraudsters, they will still allow users to identify the majority of sites. In fact, many fraudulent sites have bad spelling and grammar, so it pays to read the text carefully before committing any information.

Advance-fee fraud still persists even after all these years. It is frequently referred to as 419 fraud (the number 419 referring to the article of the Nigerian Criminal Code banning this practice). This fraud entails conning the victim out of a relatively small amount of money by the lure of a large amount. For an idea of the lengths to which scammers will go to, it is worth reading some of the interchanges at:

<http://419eater.com/html/letters.htm>

Though we would not recommend that anyone engages directly with the criminal; it can be dangerous as the scammer can become aware of being scammed and in turn try to turn the tables on the target.

This type of fraud can end up costing the victim more than just money. In some cases, the victim may be lured to a place where they are kidnapped, robbed, and even murdered. Twenty-nine year old George Makronalli, a Greek man, was murdered in South Africa in December 2004 after responding to a 419 scam. In November 2003, Leslie Fountain, a senior technician at Anglia Polytechnic University in England, set himself on fire after falling victim to a scam; Mr. Fountain later died of his injuries.

In some cases, the victim may not realise he has been defrauded. One version of the scam is for the thief to claim to have contacts who will facilitate legitimate business loans; the victim here is not persuaded that he is doing anything illegal. The fraudster meets the victim, and must be able to act the part of a well-connected and experienced loan broker. He asks for payment in advance, which is normal for large loans. Then the loan gradually falls through in a plausible way, and the victim may end up being defrauded of tens of thousands of dollars or pounds, thinking only that the deal simply failed. These frauds often go unreported, either because the victim does not realise he has been cheated, or because he is reluctant to admit the facts of the con. Reporting may be delayed until the victim becomes certain he has been cheated, by which time the criminal has disappeared.

With the advent of social networking and certain security flaws, it has been possible for fraudsters to use the power of the 'relationship' they have either created with an individual, or, in certain cases, (such as that of Jack Straw) that they have stolen. In this case, to make the con seem authentic, the fraudster pretends to be someone that victim knows. Variants of these scams continue with any new form of social media - whether it is Facebook, Myspace, IM or Twitter - and range from luring victims into infecting their machines through false anti-virus programs, to wiring money to a person claiming to be a friend stranded in a foreign country (in the case of Mr Straw).

Then there is the exploitation of disasters to entice users to read attachments. The "Storm Worm" (so named because the spam email messages that carried it commonly bore the subject line "230 dead as storm batters Europe") began hitting computers around the world in mid-January 2007. The malicious payload it carried affected most Windows-based platforms. It was spread as an attachment to an email message that installed a Trojan horse onto the message recipient's computer.

The Storm Worm arrived with many subjects lines but some of the more grim ones were:

- Death toll in China exceeds 1000000
- Recent china earthquake kills million
- 230 dead as storm batters Europe.
- A killer at 11, he's free at 21 and...
- British Muslims Genocide

Each email had an attachment with a tempting filename like:

- Full Clip.exe
- Full Story.exe
- Read More.exe

False Anti-virus Programmes

In April 2007 a new variant of Trojan.Peacomm was unleashed on the Internet. This is slightly different from the previous Storm Worm attack in that the attachments carrying the payload are password-protected .ZIP files (which recipients are tricked into unzipping and running to putatively protect themselves from some other worm). This has been developed so that visitors to infected websites are told that an anti-virus scan is being run (no surprise that these scams always 'find' a virus that can be 'fixed' by downloading a program). This seems surprisingly crude, but to some computer users who have heard of viruses but who are not savvy about the risks of downloading files from an unknown source, it is very attractive. Like all the best cons, it plays on the victim's fear – in this case, ironically, fear of being infected with a virus – and cons them into taking the wrong action.

The hackers' calendar

Spammers, hackers and phishers tap in to key dates in the calendar to lure their victims. Dates such as Christmas, Easter, Mother's Day, April Fool's Day, Valentine's Day and even Independence Day (the next major date in the hacker's calendar, coming up soon on 4th July) all offer easy pickings for criminals to send out tailored, seasonal attacks.

It's important to pay even more attention than usual to these key dates, which see spikes in the number of spam, malware downloads and phishing attacks. Headlines such as these are common:

"Spammers target users at Christmas"

"Valentine's Day spam currently accounting for nine per cent of all malware"

"Users warned against April Fool emails as history shows it as an opportunity for malware"

"Experts warn of Mother's Day hacking attack"

We should never underestimate how low hackers will stoop, or what they will try next in their quest to con money out of unsuspecting victims.

So what is the conclusion to all this? Education is the most important weapon in the war on cyber-crime. If users are alert to a scam, they are less likely to fall for it. In the same way that people are more alert to strangers coming to their door, they should be alert to strangers coming to their computer. We recommend all companies carry out regular training sessions to keep users up to date with the latest tricks that are being played. As Internet use grows more sophisticated, so too do the scams that lurk in its shadows.