

## FEATURE

### YOU ARE THE WEAKEST LINK, GOODBYE! – PASSWORDS, MALWARE AND YOU

*Martin Overton*

Independent Researcher, UK

With jokes it is often said that the old ones and the obvious ones are the best. How else can you account for the popularity of slapstick and other physical humour and the 'You've Been Framed' style of TV programme?

According to a number of recent surveys and recent worms, it seems the same is true of computer users' passwords. In other words, the joke is on us, the computer user community!

#### HAVE YOU HEARD?

Have you heard the one about the user who ...

1. Wrote their password on a post it note and stuck it on their screen or 'hid' it under their keyboard?
2. Used their phone number, car number plate, names of family members, pets or their own name?
3. Used 'Password', 'Secret', 'qwerty', '12345' or their user ID as their password?
4. Used the same password repeatedly or re-used a small number of easy-to-remember words/names?
5. Used a repeating character, such as space or z or an x six times?

If you haven't then you have not been involved in computer security for long enough, or worked in a support department – or you are from another planet or universe entirely! Welcome to the 'real' world.

#### TRUST ME, I'M A SECURITY SPECIALIST

This article will lance the festering boil of computer security; passwords. Just like an embarrassing itch that you don't or won't tell the doctor about, users refuse to seek help or take the medicine that's good for them when it comes to the key to their computer's front door – the humble, but oh-so-important password.

I will also cover some of the recent pieces of malware that have password lists and cracking tools as part of their payload to allow propagation on internal (and external) networks.

The main problem, as demonstrated by Nebiwo (aka Deborm), Mumu (aka SpyBot), Deloder and Lovgate, is that

of weak, easily guessable passwords – or even worse, no password at all – on user accounts and *Windows* shares. Finally, I shall gaze into my crystal ball and try to predict what may be inflicted on us with next from the ‘fevered pits’ of the malware authors’ minds.

## DOWN THE WORMHOLE

‘You take the red pill and you stay in wonderland and I show you how deep the Wormhole goes ...’ (borrowed and adapted from *The Matrix*). First, let us investigate in brief just some of the worms that like to carry passwords around with them to use against those who rely on weak or non-existent passwords.

### Mumu (aka Bat.SpyBot)

This is a collection of 17 components (including batch files) which spreads via SMB (port 139/tcp) and attempts to gain access to remote systems via the nine passwords held within its code.

The interesting aspect of this piece (or should that be *collection*?) of malware is that, like several other new-ish malware threats, it uses security tools that are more commonly employed by network administrators or other IT support staff. Is this yet another trend? I certainly believe that it is – at the time of writing this article another new variant has been found in the wild.

### Nebiwo (aka Deborm)

This piece of malware is not really a password-carrying threat, but it steals credentials from the user logged in on the infected system, and uses them, as well as the following accounts with blank passwords:

- Administrator
- Guest
- Owner

It attempts to use C and C\$ shares. This worm has spread quite widely and, like Opaserv, I regularly catch quite a number of infected samples on my SMB-Lure, so it seems to be quite well established in the Internet user community.

### Opaserv

On the subject of that large family of worm variants, Frédéric Perriot’s analysis of this worm (see *VB*, December 2002, p.6) describes the fact that it carries a distributed DES cracker as part of its body. Could this be a model that other malware authors will follow?

*‘You take the red pill and you stay in wonderland and I show you how deep the Wormhole goes ...’*

Borrowed and modified from *The Matrix*

I am still catching thousands of samples of Opaserv variants each month. Over 60,000 samples in total have been captured between October 2002 and the end of May 2003. In the last week alone my SMB-Lure caught four brand new variants of this family, as well as several new malware variants from other families.

### Lovgate.K

Lovgate is another well-established family of malware variants (see *VB*, April 2003, p.9 and this issue p.8). Lovgate.K carries a backdoor and mails itself out as well as spreading via SMB, as did other variants of its family.

The .K variant carries a list of 83 passwords in its body for use in a dictionary-style attack on remote hosts found via SMB scanning. However, unlike several other password-carrying malicious programs it, allegedly, uses only the Administrator account.

The problem here is that many default installations of *Windows 2000* and *XP* don’t allow you to set/reset the administrator password until after the operating system has been installed.

If, like many companies, you use a static build snapshot, then you may be facing a different problem. Why? Well, unless you have set a ‘strong’ password on the original system you imaged, you may well have given away the keys to your kingdom!

Furthermore, if you have the same default administrator password on all systems, then you will have a major problem when a brute force attack is successful on just *one* of your systems – effectively, the others are also owned by the malware. Game, set and match to the malware author.

### Deloder

Another interesting example of password-carrying malware is W32/Deloder (see *VB*, May 2003, p.5 and [http://vil.nai.com/vil/content/v\\_100127.htm](http://vil.nai.com/vil/content/v_100127.htm)).

Like a growing number of other pieces of malware, Deloder carries other non-malicious programs or components to enable it to spread and/or function. In Deloder’s case the components are from VNC (see <http://www.uk.research.att.com/vnc/>), Cygwin (see <http://www.cygwin.com/>) and the well-known PSEXEC

tool from SysInternals (see <http://www.sysinternals.com>). Another variant uses a different remote access tool from that used in the original (VNC). Both of the major variants drop backdoors (Backdoor-ARG) and an IRC bot (IRC-Pitchfork).

Interestingly, Deloder probes not only for C\$ and IPC\$, but also for ADMIN\$, D\$, E\$ and F\$ shares. Basically, the worm looks for the default admin shares that exist normally on the vast majority of *Windows 2000* and *XP* systems – that is, unless your IT department has removed or disabled them.

Deloder carries a list of 86 passwords (the number of passwords varies from one vendor’s description to another). As it uses port 445 (Microsoft-ds) to spread, it will only function on *Windows 2000* and *XP*.

As a final and somewhat ironic side note on Deloder, this worm was found happily spreading on the many wireless networks that were set up for the *Infosecurity Europe 2003* show in London in April 2003. It turned out that many of these networks had no security enabled at all, and this was an event *about* security!

### Ex-terminate! Ex-terminate!

What’s more worrying about this trend is that a number of these worms now carry backdoors, key-loggers and Trojans to disable many AV, personal firewall, IDS and related programs.

What is even more worrying is that some security tools still don’t seem to have addressed this problem, and allow themselves to be terminated in this manner.

*‘84 per cent of computer users consider memorability to be the most important attribute in selecting a password, and 81 per cent of users select a common password where possible.’*

Source: 2002 NTA Monitor Password Survey

### SURVEYS

The following are some of the results from a number of recent polls and research projects on computer security.

These demonstrate that it is the human element that poses the biggest risk to computer security: no matter how strong your security, it is only as strong as its weakest link – the human behind the keyboard.

### NTA 2002

The 2002 NTA Monitor Password Survey (see <http://www.nta-monitor.com/fact-sheets/pwd-main.htm>) found that 84 per cent of computer users consider memorability to be the most important attribute in selecting a password, and that 81 per cent of users select a common password where possible.

### Pentasafer 2002

According to this survey (see <http://www.cnn.com/2002/TECH/internet/04/08/passwords.survey/>) around 50 per cent of computer users base their passwords on the name of a family member, partner or a pet, while 30 per cent look to a pop idol or sporting hero.

Meanwhile, 25 percent of employees would consider a word as simple as ‘Banana’ to be a safe and acceptable password – even though it would take a hacker seconds to break into a corporate network using it.

### Egg 2003

Below is a list of the most common passwords used as reported in this survey (see <http://news.bbc.co.uk/1/hi/sci/tech/2061780.stm>):

Child’s name	23%
Partner’s name	19%
Birthdays	12%
Football team	9%
Celebrities and bands	9%
Favourite places	9%
Own name	8%
Pet’s name	8%

### Infosecurity 2003 Europe

Here’s an interesting quote from another recent survey (source: <http://www.securityvoice.co.uk/art.php?art=49>): ‘90% of office workers at Waterloo Station gave away their computer password for a cheap pen, compared with 65% last year.’

The report goes on to say: ‘The most common password was “password” (12%) and the most popular category was their own name (16%) followed by their football team (11%) and date of birth (8%).’

Finally, ‘Men were slightly more likely to reveal their password with 95% of men and 85% of women giving away their password.’

*'... 90% of office workers at Waterloo Station gave away their computer password for a cheap pen, compared with 65% last year.'*

From [www.securityvoice.co.uk](http://www.securityvoice.co.uk)

## CRACKING PASSWORDS, GROMIT!

There are a number of methods by which a password for a computer can be obtained or otherwise cracked.

### Social engineering

The social engineering approach goes straight to the weakest link in your security: the human behind the keyboard.

Techniques used include:

- Persuading the user to disclose their login credentials (ID and password). We have seen this in the recent PayPal and online banking scam emails, with the perpetrators pretending to be from 'security' or 'the helpdesk' and needing to confirm 'your' password and login ID.
- Key loggers.
- Trojans, including RATs and backdoors.

### Guessing

If you know someone quite well – for example a friend or a close work colleague – and they do not follow good password rules, then it is very likely that you would be able to guess their password within a dozen guesses, possibly fewer.

### Dictionary attack

This could be as simple as having a list of a few dozen words or many, many thousands of possible passwords and trying each of them.

### Brute force

This is the most intensive method; it involves simply trying every possible combination of letters, numbers and in some cases punctuation and other ASCII characters until the correct password is found.

Typically it would start at a, then try aa, then aaa and so on, until either it runs out of combinations to try or finds the right combination, to crack your 'Pa5Sw0rD'.

The main problem with this technique is that it tends to be computationally expensive, and most users would realise that their system was running more slowly than usual.

### Sniffing and session hijacking

Both of these methods use tools to perform 'electronic eavesdropping'. Session hijacking tools allow the attacker to steal your credentials as they are sent to the remote system. This can be used to allow the attacker to impersonate you and gain access to the system you were trying to log into or, more often, to modify data in transit between you and the intended recipient.

Packet sniffing tools and protocol decoders are easily used and very effective, especially those that have been written to 'decode' password data. Both sniffing and session hijacking normally require your traffic to pass through a system on the same subnet as the 'sniffer'.

## GOOD PASSWORD GUIDE

Below are some basic, but generally sound, guidelines for improving the quality and strength of your passwords.

- Passwords should be a minimum of eight characters.
- Try to include some form of punctuation or one or more digits.
- Use mixed case (include upper case and lower case letters) passwords if possible.
- Choose a phrase or a combination of words, which makes the password easier to remember.
- Do not use a word that can be found in any dictionary (including foreign language dictionaries).
- Do not use a keyboard pattern such as 'qwertyui' or 'oeuidhtn' (look at a Dvorak keyboard).
- Do not repeat any character more than once in a row (e.g. ZZZZZZZ).
- Do not create a password consisting entirely of punctuation, digits or letters.
- Do not use things that can be easily determined such as: phone numbers, car registration numbers, names of friends or relatives, your name or employment details, any date. Never use your account name as a password.
- Always use different passwords for different machines.
- Change your password regularly and do not reuse passwords.
- Do not append or prepend a digit or a punctuation mark to a word.

- Do not reverse words.
- Do not replace letters with similar-looking numbers. For instance, the letter i should not blindly be replaced by the digit 1.

Here are a few example passwords that meet many of the above criteria, and none of the pitfalls:

Password: VB2k3+btORb2

(VB2k3) = VB2003 + (b) = be (t) = there (OR) = or (b) = be (2) = square.

Password: TiaS!2Bm1st

(T) = This (i) = is (a) = a (S) = story (!) = not (2) = to (B) = be (m1st) = missed.

Other useful guides on selecting good passwords can be found at the following:

- <http://www.alw.nih.gov/Security/Docs/passwd.html>
- <http://www.securitystats.com/tools/password.asp>
- <http://www.securityfocus.com/infocus/1537/>.

## RISKY BUSINESS

So, how can you attempt to redress the current balance of power that seems to be in the malware authors', and end-users' hands?

Here are a few suggestions – and these are not just for the *Windows* users out there:

- Remove or rename the default Administrator account.
- Disable the Guest account.
- Use the PASSFILT.DLL program on *Windows NT/2K* and *XP*, as this will not allow poor passwords to be used (for instructions see <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/passfilt.dll.asp>).
- On \*NIX systems, use a replacement PASSWD binary that will not allow passwords that are weak or that can be guessed easily. Examples include Epasswd (see <http://www.nas.nasa.gov/Groups/Security/epasswd/>), Npasswd (see <http://www.uts.cc.texas.edu/~clyde/npasswd/>) or Passwd+ (Passwd+ <ftp://ftp.dartmouth.edu/put/security/>).

Just like us, passwords need regular breaks in order to be at their most effective – with this in mind, change them regularly, and do not re-use them.

## OTHER OPTIONS

Instead of relying on passwords, why not consider the following technologies – some of these effectively replace,

or seriously augment password-based systems, thereby making it harder for the malware authors and easier on the end-users without sacrificing the keys to your kingdom:

- biometrics
- smartcards
- tokens.

Yes, there is a cost associated with the use of these, but will not using such technology end up costing you more?

## WHAT'S NEXT?

Oh, I hate to crystal ball gaze, both because it can put ideas into the heads of those on the other side and because it often proves to be wide of the mark ... but here goes!

I imagine we will see:

- Malware that uses 'brute-force' password cracking methods to defeat 'stronger' passwords, as well as carrying other nasty payloads.
- Malware that uses social engineering to obtain the users' passwords and logon IDs by spoofing a website and email headers, in much the same way as the recent PayPal and bank scams.
- Malware that uses captured SMB packets relating to NT login processes to gain valid account credentials and password hashes. Known as 'Passing the Hash' (see *Hacking Exposed*, second edition pp. 156–159 for more details).

And there are many others ...

*'No matter how strong your security, it is only as strong as its weakest link – the human behind the keyboard.'*

## CONCLUSIONS

In the future we will see increasing numbers of new malicious programs that will take advantage of the 'human element'. Social engineering and weak passwords will be the key areas here.

As stated previously, it is the human element that presents the biggest risk to computer security. You can now tell your staff it's official (see <http://nl1.vnunet.com/News/1136127> and <http://news.com.com/>); 'You are the weakest link ... in security.' This is something many of us knew already, but were too polite to mention – especially to *<insert your favourite weakest link here>*!