vb Spam supplement

CONTENTS

# FEATURE 1

## A PHISH WITH A STING IN THE TAIL

*Martin Overton*
Independent researcher, UK

Phishing is big news at the moment, not only from the point of view of the victim, and the spiralling costs of this type of fraud to the banks and other financial institutions, but also from the perspective of the cyber-criminal. There is money to be made, and lots of it, from these scams.

The following is the Anti-Phishing Working Group's definition of 'phishing' [1]:

> 'Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use "spoofed" emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware.'

A recent news story brings this into very sharp focus [2]:

> 'Russian hackers have stolen 800,000 euro from Sweden's largest bank *Nordea* after a sophisticated phishing attack tricked some of its Internet customers into downloading a Trojan horse that recorded their account login details.
>
> 'The first attack took place in August 2006 and was detected a month later. Around 250 of *Nordea*'s customers have been hit by the attack to date.
>
> 'Hackers targeted the bank's customers with emails, purporting to be from *Nordea*, which told them to download an anti-spam tool. But those who downloaded the attachment were infected by the trojan haxdoor.ki.' [3]

The incident described above reminds me of a rather unusual phishing scam that I came across towards the end of 2006. Let me tell you the tale of the one that *didn't* get away.

## A 'PHISHY' TALE

Over the last year the number of phishing scams I have seen each month has risen. I usually report around 150 to 500 phishing scams in a 'normal' month (if there is such a thing as a 'normal' month in computer security), but during November 2006 I reported over 3,000 new phishing URLs, many of which were trawling for customers of the UK-based *Barclays* bank.

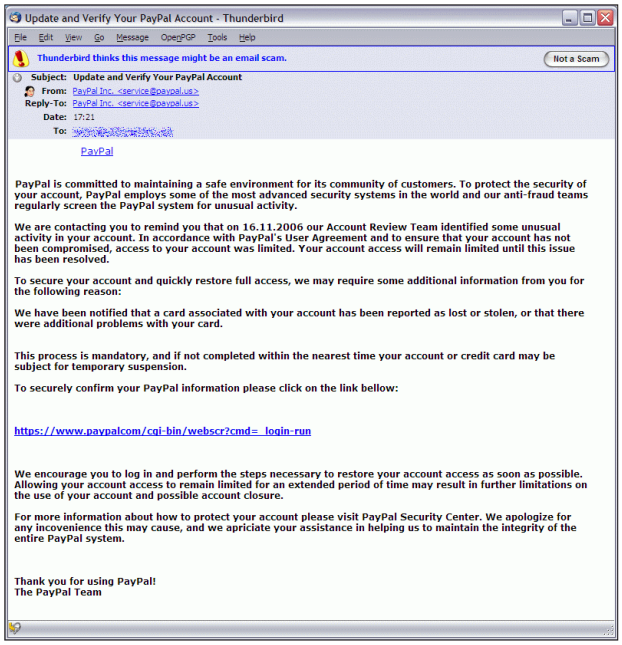
Each phishing scam email I receive is investigated thoroughly. All links are tested against the *Netcraft* toolbar (as well as other toolbars and anti-phishing solutions), and any new ones that it doesn't yet know about are submitted to *Netcraft* for inclusion in the database. This means that many of the new phishing scams have only a very small window of opportunity to hook any new victims that use the *Netcraft* toolbar.

However, once in a while I spot something that makes a new phish stand out from the rest of the shoal. One such time was in November 2006. This article explains why I considered this phish to be something different from the run-of-the-mill phishing scams.

Now, pretend I'm a typical user (it's easy if you try).

## FIRST WE BAIT THE HOOK ...

Figure 1 shows a screenshot of the 'baited hook' received by the typical user (who luckily happened to use *PayPal*).


Update and Verify Your PayPal Account - Thunderbird

File Edit View Go Message OpenPGP Tools Help

Thunderbird thinks this message might be an email scam. Not a Scam

Subject: Update and Verify Your PayPal Account
From: PayPal Inc. <service@paypal.us>
Reply-To: PayPal Inc. <service@paypal.us>
Date: 17:21
To:

PayPal

PayPal is committed to maintaining a safe environment for its community of customers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We are contacting you to remind you that on 16.11.2006 our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

To secure your account and quickly restore full access, we may require some additional information from you for the following reason:

We have been notified that a card associated with your account has been reported as lost or stolen, or that there were additional problems with your card.

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject for temporary suspension.

To securely confirm your PayPal information please click on the link bellow:

https://www.paypalcom/cgi-bin/webscr?cmd=_login-run

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account closure.

For more information about how to protect your account please visit PayPal Security Center. We apologize for any incovenience this may cause, and we apriciate your assistance in helping us to maintain the integrity of the entire PayPal system.

Thank you for using PayPal!
The PayPal Team

*Figure 1: The 'baited hook' – the email received by our typical user.*

There's nothing too unusual about this, it looks like a typical phishing email aimed at *PayPal* customers. The usual social engineering tricks are used, complete with a fake URL. As you may have guessed, the website the browser ends up at if you click on the link is not the one shown in the email, but it will look very much like the real website.

## WE HAVE A BITE ... STRIKE!

Well, the typical user did bite. After panicking and running around like a headless chicken for a while, they clicked on the link. Figure 2 shows what they saw in their web browser (the site has now been closed down).


*Figure 2: 'Phishy' PayPal website.*

You can see clearly that at the time I took this screenshot the site was not detected by the *Netcraft* toolbar, or even the *Firefox* anti-phishing functions which are now built into the browser.

As with the original phishing email, there's nothing too surprising here; this is a typical *PayPal* phishing scam site – very believable to those that are not paying attention.

The typical user logged in and filled out the required forms with their name (*Mickey Mouse*), address (*Disneyland, etc.*), social security number (*123-45-6789*), date of birth (*01-01-35*), credit card details including CVV (the three-digit security code) and PIN (when researching this phish I used false credentials, including a computationally valid credit card number from a 'non-existent' credit card).


*Figure 3: 'Phishy' PayPal website: the confirmation page.*

Everything was just like most other *PayPal* phishing sites, until the confirmation page. Figure 3 shows what our typical user saw.

'Oh goody', the typical user thought, 'they're offering me a free download of an *eBay* Toolbar called *VGuard*, and it is at version 10, that's awfully decent of them!' Of course, the typical user downloaded and installed it immediately – as most users do, don't they?

All seemed to be fine – until the rude message in Romanian appeared and the machine rebooted.

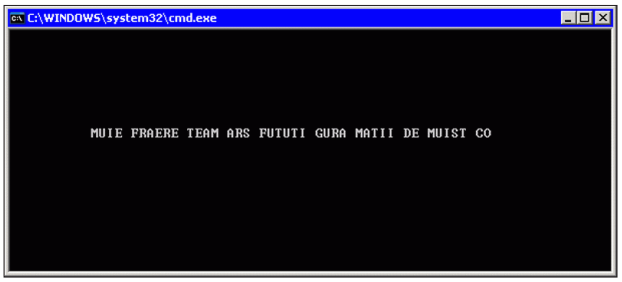



*Figure 4: 'The sting in the tail'. (Picture courtesy of F-Secure. Apologies to Romanian readers.)*

## THE 'TYPICAL USER' HAS [BEEN] LANDED

Not only has our typical user been landed, they have been gutted and prepared to be devoured – or at least their computer has (more on that later).

So, let me now be the *real* me. What did I do once I had downloaded the 'useful' *eBay* toolbar?

Of course, I started to analyse it. The following is the file information:

```
FileName: Guardv10.exe
FileDateTime: 16/11/2006 17:44:35
Filesize: 149254
MD5: 2fadb5a4f3c80e78197d733255136ba7
CRC32: 7B3A6C60
File Type: PE Executable
Packer: Standard PE File
```

That's interesting, I thought, it isn't even packed using the usual malware authors' tools, such as *UPX*, *FSG*, and so on. Next, I had a quick peek at the internals of the file and discovered that it would create some files and execute them. Not just any files, but a DOS batch (.BAT) file – which was very suspicious.

So, like a good malware analyst, I sent it off to be run in a sandbox. The following are the results (from *Norman Sandbox*):

```
Guardv10.exe : Not detected by Sandbox Signature:
NO_VIRUS)
[ General information ]
* File length: 149254 bytes.
* MD5 hash: 2fadb5a4f3c80e78197d733255136ba7.
[ Changes to filesystem ]
* Creates file C:\TEMP\bt8323.bat.
* Deletes file C:\TEMP\bt8323.bat.
[ Process/window information ]
* Creates an event called .
```

The results from the sandbox confirmed that the downloaded executable created a batch file.

My next question was: what anti-malware tools detect it? To find out I scanned the file using over 30 'up-to-the-minute' updated anti-malware tools. Here are the results (from *AV-Test*):

```
Scan report of Guardv10.exe
@Proventia-VPS Malicious (Cancelled)
AntiVir -
Avast! -
AVG -
BitDefender -
ClamAV -
Command -
Dr Web -
eSafe -
eTrust-INO -
eTrust-INO (BETA) -
eTrust-VET -
eTrust-VET (BETA) -
Ewido -
```

```
F-Prot -
F-Secure -
F-Secure (BETA) -
Fortinet -
Fortinet (BETA) -
Ikarus -
Kaspersky -
McAfee -
McAfee (BETA) -
Microsoft -
Nod32 -
Norman -
Panda Suspicious file
Panda (BETA) Suspicious file
QuickHeal -
Rising -
Sophos -
Symantec -
Symantec (BETA) -
Trend Micro -
Trend Micro (BETA) -
UNA Trojan.BAT.Small.BC0B
VBA32 -
VirusBuster -
WebWasher -
YY_Spybot Jupilites,,Installer
```

As you can see, hardly any of them detected anything at all. I sent the file off to all the anti-malware companies so that they could add detection for it to their products.

## PREPARE TO FEAST!

The sting in the tail mentioned in the title of this article is not that the phishers have used a bit of social engineering to get a phished target to give away their personal and financial data, but that they have also got them to download and run a piece of malware – which the typical user thinks is a useful toolbar.

In fact, the 'useful toolbar' does the following [4]:

- It attempts to remove the first four boot configurations from the 'boot.ini' file and then delete the 'hal.dll' file in the Windows '%System%' directory.
- It copies itself to the Windows 'Startup' folder and proceeds to shutdown (reboot) the computer.
- If it is successful, this will make the infected computer unbootable and it may also show a rude message in Romanian on the screen.

Not only have the phishers made off with the user's data, but they are also trying to cover their tracks by making the system unusable.

Any half decent security professional or system administrator could, of course, resolve the matter fairly easily, but most average users would be completely stumped as to how to proceed at this point.

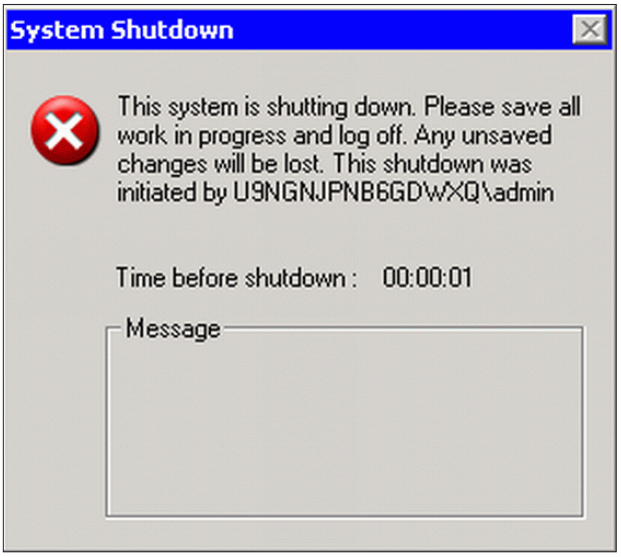



*Figure 5: 'The sting in the tail' going down! (Picture courtesy of F-Secure.)*

In most cases they would probably take it to their local PC expert or repair centre and wouldn't realise that it was that 'useful tool' that did the dirty deed.

## CONCLUSIONS

As illustrated by the news snippet at the beginning of this article, it seems that typical users are being fooled by this type of phishing scam in which malware is used either to make stealing personal or financial data easier, or to cover the attackers' tracks.

Meanwhile, back at the bank ... well you know how this story ends, and at the moment it's not often a happy ending. The typical user ends up not with a fish supper, but as 'phish phood' instead.

## REFERENCES & NOTES

[1] Source: http://www.antiphishing.org/.

[2] Source: http://www.businessweek.com/globalbiz/content/jan2007/gb20070119_387969.htm.

[3] Haxdoor.ki was, allegedly, authored by '*Corpse*' a Russian malware author of some notoriety. More details can be found here: http://www.f-secure.com/weblog/archives/archive-012007.html#00001096.

[4] http://www.f-secure.com/v-descs/killwin_ar.shtml.