FEATURE 1

(Porn) Dialers – Another Class of Malware?

Andreas Marx, AV-Test.org
University of Magdeburg, Germany

When making small payments (of a few pennies or cents only) it does not make sense to use a credit card, bank transfer or other expensive transaction method, because the bank fees would exceed the payment. An alternative solution is to make payments by telephone. For example, the customer can call a chargeable number and get a key code which can then be entered into a web front-end to finalise a transaction. Later, the telephone company will charge the amount to the customer's telephone bill.

But another method of payment makes it easier still for the customer (or, perhaps, tricks him more effectively). Web dialer applications are very common now, especially associated with 'pay per view' websites. Dialers are small programs (usually only 50–80 kb in size) which are able to disconnect the current telephone line and dial a cost-intensive number automatically, allowing the user to access the web pages he has requested.

Of course, to be legal (at least in Germany), the dialer must display the telephone number it wants to call, the cost per minute, an identification code for the provider and it must show the general terms and conditions of the provider on request before starting to dial. In addition, an ISDN card or modem must be connected to the PC – users of DSL-only connections cannot use this 'automatic' payment method.

It is very common for pornography websites to use this form of transaction. But other users of this payment method include online games companies and larger download archives – you pay for the product by telephone.

Technically, this method is easy to use and inexpensive for both the contractor and the customer. The customer pays only for the content he receives, at a special per-minute rate. However, since the beginning of 2002, instances of misuse of such dialers (also known as porn dialers) have risen dramatically, both in Germany and across Europe.

A number of websites have been set up in the past few months specifically to address this issue – for example http://www.dialerschutz.de/ – and other security-related websites, such as http://www.trojaner-info.de/ have been extended with a section on porn dialers.

The Issues

First, there are a huge number of dubious providers whose dialers do not display all the relevant information – they 'forget' to include the costs, display inaccurate costs, or conceal the costs somewhere in a greyed-out text box. Others fail to display such a window at all, but call the built-in telephone number automatically or, more craftily, simply change the configuration of the standard Internet dial-up connection to their own (see http://www.heise.de/newsticker/data/uma-30.05.02-001/). A few dialers have been seen that delete their traces completely after this expensive change, leaving no evidence that this program was ever executed on the PC. The user can expect an interesting phone bill at the end of the month …

One very old trick that still seems to work well is to tell the user that they need a special download utility in order to connect to a website with high speed, or that such a utility is needed due to the 'frequently changing IP address of the download server to avoid prosecution, because of the huge amount of illegal software that can be found'. Of course, much is made of the fact that this download tool (EXE) is 'free of charge' – in fact, it is free of charge, but connections using it are not.

Some websites (you can find these easily if you try searching for 'license codes' or 'cracks' in your favourite search engine) will tell you that 'the complete hard disk of your PC can be accessed by everyone on the Internet' and that 'the only tool worldwide to be able to prevent this' can be downloaded from their website – of course, you need to install the 'free-of-charge connection tool' first. And indeed, the content of your C: drive will be displayed in the middle of the web page, using a simple IFrame HTML trick. And some other 'secret' information will be displayed as well – such as the referrer string, the computer's IP address or the browser identification string, so it looks more dangerous to the home user.

Spam Always Works!

Spam emails with an EXE dialer attachment, or at least a link to a website with a 'downloadable dialer', are quite common too.

Often, people will delete such spam emails quickly – but they are less likely to do so if the subject is sufficiently intriguing (for example 'Complaint against you', 'Notice of Cancellation'), if the email appears to be a greeting card from 'a person who likes you very much' (see http://www.intern.de/news/3617.html), or if it appears to contain pictures of body regions that only a gynaecologist would usually want to see.

The following is typical of the content of these spam emails:

```
  'Yes guys, we've cracked a dialer now. You
can get free access to the whole web page if
```

> `you use our cracked dialer. It has cost us days and nights, but finally we were successful. Have fun, but please do not use the connection for more than 30–40 minutes at once, because you could be detected.’`

And would you lodge a complaint against a dialer that has caused you such a huge telephone bill if you were the one who tried to cheat first by using a ‘cracked dialer’? It’s a perfect win-win situation – for the provider only, of course.

Easy Money

These providers are often very hard to catch, because the cost-intensive telephone number may have been rented to a German company first, but they subsequently rented it to a Canadian company, and this company rented it once more to an Indian one, the next step is a Spanish one, then a Haitian one and so on. It’s virtually impossible to track down the real ‘bad guys’ who finally get the money. Furthermore, companies that rent telephone numbers this way tend to be very short lived.

To make matters even more difficult, these companies usually have special ‘webmaster program’ offers. A so-called ‘webmaster’ (or, more accurately, spammer) can get up to 50% of the telephone fee if a user is online for long enough. And the more users and minutes, the more money. This way, it’s easy for the providers to tell everyone that they have not sent out a single spam message that could be in conflict with existing laws (see http://www.heise.de/newsticker/data/jk-16.06.02-001/).

A recent study in the German *PC-WELT* magazine (issue 12/2002, p.14) reveals that only about one or two in a thousand users will install the dialer – whether by accident or intentionally – but such users have to pay about 100 Euros. If only half of the people pay this telephone bill (this can happen quite quickly if the telephone company warns the user that they are going to disconnect him if he does not pay straightaway!), and a spam message is sent out to about two million people at once, that’s about 100,000 to 200,000 Euros in a few minutes!

What about AV and Firewall Protection?

Until now, the standard user has been completely unprotected. Anti-virus programs usually do not find dialers, and identify only viruses, worms, Trojan horses and other programs that are malicious (or that are almost certainly malicious, e.g. Win32/Friendgreeting).

A few attempts by German AV vendor *H+BEDV* to detect dialers at the beginning of this year were unsuccessful. They made the mistake of detecting dialer programs and giving the alert message ‘Infection: some dialer virus’ – of course the dialer developers did not like this classification very much.

Eventually, the signatures had to be removed from the anti-virus program for legal reasons and the matter has cost *H+BEDV* both a lot of time and a lot of money (for more about the case see http://www.heise.de/newsticker/data/ku-14.05.02-000/ and http://www.pcwelt.de/news/software/23834/).

On the positive side of things, a lot of web dialers try to install themselves automatically using well-known security holes in *Internet Explorer*, just like the Win32/Nimda virus, for example. And most AV programs are able to intercept this – there may be a confusing warning such as ‘Infection: Mime-Exploit.gen virus detected’, but the result is that the dialer is blocked!

Personal firewalls do not protect the user either. Such programs check only the data packets which were sent over an existing connection. Currently, personal firewalls do not check the dial-up of the connection itself, e.g. the telephone number dialled using a white- and/or black-listing approach like the one used for applications for a long time now.

However, a lot of hobby programmers have created dialer protection programs, or warners, that work in exactly this way – they check the telephone numbers called, check whether a called application looks like a dialer, and so on. The most well known of these are *YAW* (*Yet Another Warner*, http://www.yaw.at/) and *0190 Warner* (http://www.wt-rate.com/).

Cat and Mouse

But the dialer industry does not sleep and has reacted very quickly to the appearance of these warner programs – and the events which currently take place within a matter of weeks remind me of the whole 15-year history of the anti-virus industry (the usual ‘cat and mouse’ game).

One of the first actions the dialer developers took was to change the telephone number to avoid detection. As well as ‘0190’ in Germany, a lot more numbers are billable, like ‘118xx’ which is reserved for information desks, or ‘0191’ and ‘0193’ which are reserved for Internet service providers, and even ‘005xx’ numbers for a connection to some far away islands in the Atlantic Ocean. It’s not easy to blacklist all of these numbers, because ISPs like *T-Online* and *AOL* use these numbers legitimately, as do thousands of other providers. But these problems are solvable using black- and white-lists.

The next reaction of the dialer developers was to avoid using the controlled *Windows* built-in dial-up networking and communicate directly with the modem instead, using Hayes-compatible ‘AT’ commands or ISDN using CAPI (Common ISDN Application Programming Interface) or TAPI (Telephony Application Programming Interface). In addition, some dialers try to access the serial interface (e.g. COM3) directly, in order to bypass any dialer protection programs. The warner applications were updated accordingly.

A lot of dialers try to kill warner applications in memory automatically, without further notice. Some also delete installation files, or their activation 'Run' key in Registry, so the warner program is unable to start. Another method we've seen is to add the dialer application or telephone number to the white-list simply by changing the warner's configuration file. (Should we call them 'retro dialers', just like 'retro viruses'?)

Newer versions of the warner programs have increasingly robust protection against such kill attempts – for example, *YAW* 'injects' itself into all running processes. This method works better than expected (and more reliably!), because it does not cause any problem to the user (besides higher memory requirements) and it really is unkillable. To enforce it even further, all of the program files are always open and cannot be deleted. The activation points in the Registry (the 'Run' key, for example) will also be checked every 1/10 seconds. Perhaps anti-virus and firewall programmers could learn from such dialer protection programs and prevent Win32/Bugbear-like 'anti-virus killers'.

A few warner programs have replaced the Windows DLL with their own – and if the main program is not loaded, no Internet or other connection is possible. (Some personal firewalls have similar features now.) But even this line of defence was penetrated easily – a lot of dialers include a list of renamed original DLLs or functions the dialers can use 'safely'.

As soon as some dialer protection programs started to include signatures and checksums to detect known dialers easily, the strike-back was that the developers changed their creations. At first they changed every day, but now some developers release new (slightly changed) dialers every hour.

The first dialers were runtime-compressed using UPX mainly to reduce the size, but as soon as some warning programs included a UPX unpack routine, this method changed. A lot of dialers now have a significantly changed UPX extraction routine, they are compressed using other programs and hardly even protected by a lot of anti-debugging tricks and additional encryption routines. (Isn't this the method to hide Trojan horses and backdoors in the virus world right now?)

One interesting point the dialer developers forgot at first was the (mostly uncompressed) resource section of every program where a lot of information is stored, for example the program name or version as well as icons. I hardly need to tell you what happened after the first dialer protection programs checked this section, too …

There is still one Joker left however: if the EXE program has a digital certificate, the name of the company is always included in plain text. I have seen companies that have more than one certificate, even if it's a little more expensive, but think about what you can get back in return.

You may ask why such dialers are digitally signed. The answer is that a lot of dialers try to install them as ActiveX controls first (usually making multiple attempts, if the user does not want this) – disguised as 'chat plug-in', 'security update', 'special graphic viewer (with extreme zoom)', and so on.

If this fails (for example when the browser being used is *Netscape* or *Opera*, neither of which support ActiveX), the user will be prompted to save an EXE file (multiple times, too). In order to avoid an ActiveX warning at the next installation, a number of dialers install their certificate as a trusted publisher in the *Windows* certificate list. Alternatively, they try to execute a small (only 5–7 kb) program automatically, using web browser security holes and later they can install any kind of ActiveX control (not only dialers) without further unwanted questions.

Last, but not least, many dialers – once executed – install themselves in the Registry (Run key), Autostart group, win.ini so that they are always started. In addition they put their logo on the desktop, in the Start Menu, Systray etc. and they change the standard web page ('Home') to their own.

Usually, it's very difficult to get rid of dialers even if they have not been able to dial and cause the user unexpectedly high costs.

Conclusion

Now you've read the full text of this article, wouldn't you agree that dialers as they exist now could be classed as malware? They have been created as a small, inexpensive micro payment method, but a lot of companies use such dialers now for Internet fraud. An ideal protection program should prevent possibly malicious dialers, but allow 'good' dialers the user has accepted.

But existing solutions – anti-virus scanning and firewalls – do not protect the user from this threat. At the moment, many more integrated security products are becoming available – why not include dialer protection in these packages as well? In this case, we would be in a much stronger position to protect the user. For example, if a dialer tries to delete or deactivate the security product, we can call it a Trojan horse and can add detection for it easily.

At the moment, dialers are extremely common in German-speaking countries, but the number of dialers is growing very rapidly across Europe and worldwide, because it's an extremely lucrative billion-dollar business. And it will probably take a very long time (a matter of years?) before the law in so many countries has been changed.

A few weeks ago I saw the first OEM AV package that was bundled with a dialer protection program. When can we expect more?

[*VB is interested in hearing readers' opinions on this issue. Should we classify porn dialers as malware, and should detection of dialers be incorporated into security products? Send your thoughts to comments@virusbtn.com*]