

GERMANY:

MALWARE LEARNS THE LANGUAGE

By Toralv Dirro and
Dirk Kollberg



The threat landscape in Germany, and all over Europe, has differed from North America’s since the 1990s. The main reason for this difference is the variety of languages; in the European Union alone there are 23 official tongues. Furthermore, we’ve seen for a long time that a language barrier stops most malware and other attacks from succeeding.

The barrier went up when paths on the file systems differed depending on the language of the operating system. Malware often used hard-coded paths to determine where to put files or where to seek information. And it failed miserably. (We still see commercial software failing to function properly from time to time for this very reason.)

Microsoft Word macro viruses were the next class of malware to find the language barrier difficult to cross. The first macro viruses didn’t work at all; many of the macro viruses we have seen since then have had some problems too. The reason for this is that in localized versions of Word the functions had been localized as well. So if a virus tried to hook the function FilePrint, for example, it would have to hook DateiDrucken in a German version of Word and FichierImprimer in a French version. This led to malware authors creating viruses that specifically targeted German Word, French Word, Spanish Word, etc. Of course it is possible to create macro viruses that do not hook any function that is translated to local languages; those have been successful in Europe.

The next wave was mailers and mass mailers, viruses that actively created emails to send themselves to other people. This was the first kind of malware that relied on social engineering to be successful. (Social engineering in this context means that the receiver must be convinced that it’s worthwhile to open the email and attached file.) The problem for the attacker today is exactly the same as it was when mailers first appeared: creating a message that looks authentic and makes a user open the attachment. Using the receiver’s native language for the message text is a good start. Or use little or no text at all. A long English-language message claiming that there is something very important in the attachment that I absolutely have to open, apparently sent by a friend or coworker, just won’t cut it in Germany.

Some very primitive viruses were successful because they used hardly any text. Some of these were created with VBSWG, a virus construction toolkit that allowed anyone to create simple mass mailers that used Visual Basic Script. In the following example all that matters is the name of the attachment, so the language barrier makes little impact.

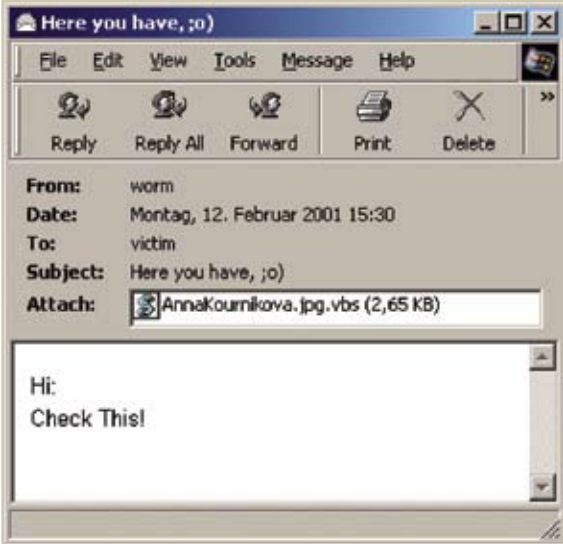


Figure 1: Social engineering is the key to this tempting file attachment.

With Windows Explorer preferences set by default to hide known file extensions, the name of this malware would appear as AnnaKournikova.jpg, and fool the user into assuming it’s a picture.

Other threats used the local language for the text of an email. Although this tactic made malware successful in one region of Europe, they were hardly a threat outside that area. Thus we have seen a number of local outbreaks, in which one particular virus blankets a region, yet is hardly

seen outside it. This extreme regional focus makes it very difficult for researchers to provide an accurate assessment of the risk posed by the malware. Having local virus research labs throughout European countries proved very helpful in these cases.

Now that we've seen the big shift in the malware scene caused by the potential profits of the botnet business, data-stealing Trojan horses and phishing scams in email messages are getting more sophisticated every day. In the early days messages were composed in a crude German notation that looked like it was an English or Russian text translated by Babel Fish. That's probably what happened.

Today we read text written in perfect German, referring to current events and playing on people's hopes. During the FIFA soccer World Cup in the summer of 2006, German fans had trouble finding tickets. So we saw emails promising details in an attachment with information about buying those rare tickets. The illegal sharing of music and videos has been in the news for a long time; German authorities have proposed an online search of computers using a special "BundesTrojaner." This has been a hotly debated topic and has led to the following email:



Figure 2: The text says "Your IP address has been logged while illegally sharing files with other users. Your computer has been searched using the BundesTrojaner and evidence has been secured. A criminal complaint is going to be filed; the attachment contains a protocol of the online-search conducted on your computer."

This is one example of the notorious Downloader-AAP, which is a very common threat in Germany. This malware was spammed to users with email addresses that ended with ".de"; the text was in German. For many months we have seen several spam runs each week, all with different messages in the mail body and different variants of the downloader and the password-stealing Trojan that the downloader installs.

In the message, the recipient gets an invoice from an attorney or a well-known German company, such as Deutsche Telekom, eBay, or GEZ, the federal service that collects fees from anyone who owns a TV or radio. These "senders" catch the reader's interest: No one likes to receive a bill, particularly if might be a case of fraud.

The Downloader-AAP example employs the fear factor, in this case due to file sharing and its associated legal problems being big news in Germany. The message says that the user was caught red-handed downloading copyright-protected files from a file-sharing network and the IP address was logged. The user's PC was already examined by the BundesTrojaner and admissible evidence was found. The Bundeskriminalamt (BKA, similar to the FBI in the United States) will report the offense.

As in all of these spam runs, the mail promised further details in the attachment, which appeared to be a bill, often named Rechnung.pdf.exe. Depending on system settings, some users may notice only the PDF extension and assume the file is safe, but it's actually a malicious executable—Downloader-AAP.

These messages scared many people, and they clicked before thinking twice. Due to a lack of evidence, however, this example does not work in other countries.

Focus on Germany

Why do the bad guys focus only on a single country?

Downloader-AAP downloads a text file that contains an encrypted URL. This file gets decrypted and the file hosted at the URL gets downloaded. It turns out to be Spy-Agent.ba, a Trojan that attempts to steal confidential account information and focuses on financial institutions. It's designed to "hijack" home-banking connections and to steal user credentials and transaction authentication numbers (TANs). These functions within the Trojan are optimized for different corporations in Germany; the Trojan injects itself into the communication between the user at home and the bank. Depending on the institution the Trojan has different ways of infiltrating communications.

On September 13, 2007, Germany's BKA announced that they had busted an international group of phishers, arresting 10 persons and seizing a number of computers and other evidence.¹ The BKA's press release claims this is a group that has been harassing the world with phishing emails containing Downloader-AAP as an attachment.

But this is unfortunately not the end of Downloader-AAP. Just a week after the arrest, McAfee® Avert® Labs received a new sample distributed in a similar way and downloading Spy-Agent.ba.

Trojans targeting financial institutions do not plague only Germany; they also occur in other European countries and they are also a big threat in Brazil.

Germans care a lot about their banking security and were very hesitant to adopt technologies such as online banking.

Phishing itself has had less impact in Germany than in many other countries. And this is not solely due to the language barrier. The Germans care a lot about their banking security and were very hesitant to adopt new technologies such as online banking. This reluctance forced banks to offer a security scheme that makes it much more difficult to take over someone's bank account. The current system requires not only an account name and PIN to log in, but every transaction also needs a TAN. The bank sends those on paper to the user. Every transaction needs to be submitted with an unused TAN. This strong security has forced criminals to pursue online banking opportunities in other countries.

Phishing for TAN

Some Trojans were written to extract the TAN list from the user's machine if those numbers were stored electronically, and, of course, we did see the occasional dumb phishing mail that tried to get those TANs.

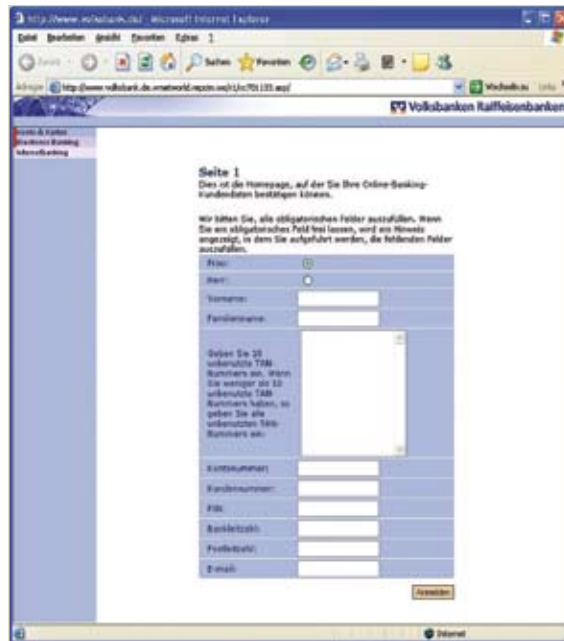


Figure 3: This phishing request asks for 10 unused TANs, in addition to lots of personal data.

In recent months we have seen Trojans that specifically attack German banks, hooking into the user's browser and emulating the behavior of each online banking site with fake error messages to get at the TANs the attacker needs. Those Trojans are available for sale on certain web sites for would-be criminals; the authors have released videos demonstrating their features and effectiveness online. German online banking is very likely to be attacked more often in the near future.

¹ "Success against internationally organized online criminals" (in German), BKA. <http://bka.de/pressemitteilungen/2007/pm070913.html>

W32/Sober@MM is a mass mailer that has gained a lot of attention in Germany, Austria, and Switzerland. The first variant was seen at the end of 2003, the most recent in March 2007. Like many other mass mailers, W32/Sober harvests email addresses found on the local system and sends out mails to users in different languages, depending on the top-level domain of each recipient's address.

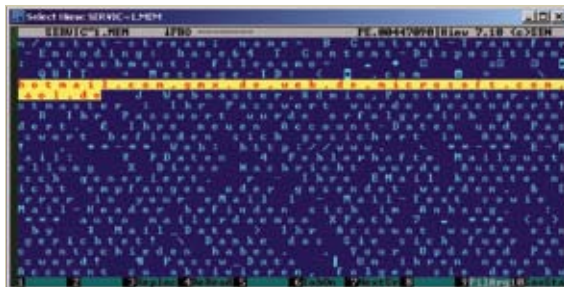


Figure 4: W32/Sober@MM can send messages in different languages. It "decides" after reading the top-level domain of the addressee.

In another popular attack, W32/Sober.p@MM sent to German users a mail stating that the recipient had won tickets to the soccer World Cup:

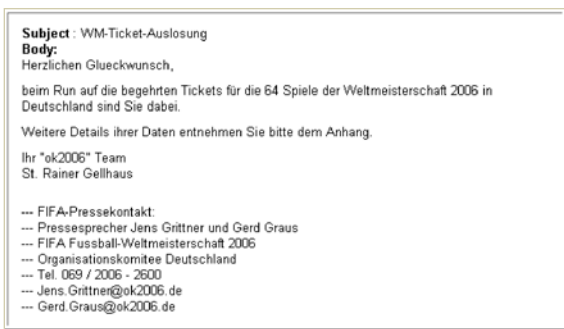


Figure 5: This message informs the happy receiver that soccer tickets are available.

The World Cup scam promised further details, but inside the zipped attachment was the file winzipped-text_data.txt.pif. Of course there were no details; it was just a copy of the worm.

The worm's timing was excellent: It was released when many people were waiting for a mail from the FIFA ticket lottery. Even the address and the phone number listed in the German text are accurate. In effect, the worm caused a distributed-denial-of-service attack on the FIFA office because so many users who received the worm called the number and asked for details.

For English recipients, W32/Sober sent out a different mail with a copy of itself attached:

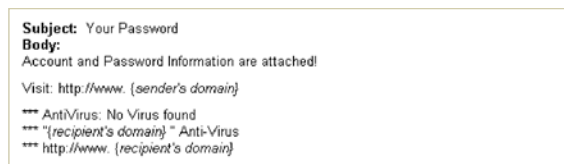


Figure 6: W32/Sober's English-language message used a generic appeal.

Making a local appeal

Another example of localized malware is the Zunker Trojan. It's also a password-stealing Trojan that also sends spam emails or links to malicious sites, in order to infect other people. The nasty thing with this Trojan is that it connects to a server on the Internet and, based on the victim's IP address, the Trojan receives the spam messages the user is supposed to send.

Zunker not only sends spam emails in the way you would expect. It also injects some text into the emails the users send. To do this, Zunker installs a Layered Service Provider on the compromised machine. Whenever the user sends an email, Zunker alters the text and adds a malicious link. The recipient of the mail probably knows the sender and thus might trust both the message and the link. Zunker also injects these messages into ICQ, AOL, and Yahoo instant messages.

The key localization aspect in this case is the injected message. If the IP address of the victim is registered in Italy, for example, Zunker will inject an Italian quote and the link. In Sweden, it would be a Swedish quote, and so on.



Figure 7: The Zunker Trojan can localize its messages in various languages, appealing to users in many countries.

You can see in Figure 7 where Zunker’s victims are located and how it spreads out the spam. The same web interface controls the Trojans and sets up the messages they’re spreading—either for all victims or separate messages for each country.

Infected web servers

Another way to distribute localized malware is via web servers. When a browser requests a file from an HTTP server, it establishes a TCP network connection. The server receives the request, loads the file from the hard drive, and sends it back. Servers that host malicious files have another feature. After they receive a request, they first look at the IP address of the connecting system, using a database to resolve its country host. With this information, the infected server can deliver localized files to each country.

With this system there’s just one link to a web site. Depending on where your IP address is registered, users in the United States or United Kingdom receive an English-language Trojan, while someone from Germany or Austria receives German-language malware.

These infected servers are hard to monitor for anti-virus vendors, because they need to send several requests to the same URL, each from a different IP address, in order to receive all variants of the malware.

Another way to serve localized files is to look at the request the browser sends to the server:

```
000000 GET / HTTP/1.1
000010 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-
000058 shockwave-flash, */*
000071 Accept-Language: de
000088 Accept-Encoding: gzip, deflate
0000A8 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.0)
0000C8 Host: 127.0.0.1
0000F7 Connection: keep-alive
00010F
000111
```

Figure 8: A Trojan could determine the nationality of this client request—and choose a local language for reply—by reading the Accept-Language line.

In Figure 8, you can see the user is from Germany (de) and uses Internet Explorer Version 6 on Windows 2000. Anti-malware researchers have little trouble dealing with these servers; it’s easy to send different requests to a server from a single IP address and receive the various files the Trojan has to offer.

Conclusion

Many attackers now understand that it is important to take regional customs into account if they want to be successful. We’ve seen that this lesson has been well learned in Germany and the trend of localizing attacks is certain to continue. Phishing attacks are getting more sophisticated and will become harder to spot. Fraudulent job offers seeking financial agents, a thinly veiled attempt to hire innocent people for laundering money, look very professional today and are likely to adapt to local factors even more in the future. It’s likely that German speakers will soon face the same level of exposure to phishing, Trojans distributed by email, and even spam as people in English-speaking countries do.



Toralv Dirro is a Security Strategist in the Hamburg office of McAfee Avert Labs. Dirro, a researcher since 1994, is a well-reputed

expert on next-generation anti-virus technology and network intrusion prevention; he is a frequent speaker on those topics.



Dirk Kollberg works as Malware Research Lead in Hamburg for McAfee Avert Labs. An eight-year veteran, he analyzes worms, peer-

to-peer network and service-exploiting threats, as well as Trojans, bots, and other viruses. Kollberg blames the Commodore PET for his addiction to bits and bytes.

