Malicious Code: VBS/OnTheFly (Anna Kournikova)

Marco Smitshoek

March 2nd 2001

Introduction

On February 12 CERT Coordination Center received more than 100 reports about a new virus spreading rapidly: VBS/OnTheFly also known as the Anna Kournikova virus or SST. This paper covers both technical and social aspects concerning this virus.

First the technical aspects will be explained: description, effects, response to it and how it was created. Secondly some social aspects will be discussed: who created the virus, for what reasons and with which consequences?

Finally the conclusion will cover some general protection measures against such viruses.

Technical aspects

Description

The virus uses encryption to hide itself and is attached to an e-mail message with the following characteristics:

- subject: “Here you have, ;o)”
- body: Hi:
  Check This!
- attachment: “AnnaKournikova.jpg.vbs”

When the recipient opens the attachment, the virus executes and it will send copies of itself using Microsoft Outlook to all entries in each of the address books. The sent messages have the characteristics as described above.

Effects

What does the virus exactly do on execution?

1) it attempts to create the following registry key:
   HKEY_CURRENT_USER\Software\OnTheFly="Worm made with Vbswg 1.50b"

2) it copies itself to the Windows directory, always using the same filename:
   C:\WINDOWS\AnnaKournikova.jpg.vbs

3) it sends an infected e-mail message to all entries in all address books using Microsoft Outlook

4) to make sure these messages are only sent once, the following registry key is created after sending out the messages:
   HKEY_CURRENT_USER\Software\OnTheFly\mailed=1

5) on January 26th each year, the virus will automatically connect the infected computers to the web site of Dynabyte, a Dutch computer company.

The sending of the infected messages can lead to congestion of mail servers, which causes interruption of mail services. By connecting the infected computers to the web site of Dynabyte this web site could suffer a denial of service, although chances for this are very small. Besides these there seems to be no further destructive effects caused by this virus.

Response
How to prevent/recover from infection by this virus (and others)?

- update your anti-virus product. Most large anti-virus software vendors have updates available quickly, so your anti-virus product will detect the virus and infection can be prevented.

- apply the Microsoft Outlook E-mail Security Update and other security patches This patch can be downloaded from: http://office.microsoft.com/2000/downloaddetails/Out2ksec.htm

- Since the description of the virus is available, filtering can be done to delete the infected messages at the perimeter of your site. Messages can be filtered on subject line, body text or attachment.

- instruct the user community to not open suspicious messages, even if they appear to come from known sources. Users should also disable auto opening or previewing of e-mail attachments in their mail clients.

How was this virus created?
One could expect such a virus to be written by someone with excellent programming skills, but the opposite is true. The creator of this virus declared that he doesn't have any programming skills whatsoever. He used a so-called virus generator (of which many exist!), in this case the VBS Worm Generator 1.5b written by [K]Alamar from Argentina. Bryan Fansler decribes in his paper how he tested the VBS Worm Generator 1.5b (see References).
With this Worm Generator the only thing the virus creator had to do is fill out some fields in the GUI of the Worm Generator and have the virus built. Some choices offered by the Worm generator are: to name the virus, select the way the virus will spread (MS Outlook/mirc), the payload it will carry and some more. For a more detailed description of the VBS Worm Generator 1.5b see Bryan Fansler's paper.

Social aspects
People create viruses. People trigger viruses. People suffer the results. So besides the technical aspects also social aspects are involved.

The reason why the Anna Kournikova virus could spread so rapidly in the first place was that many people were interested in looking at a picture of the famous young Russian tennis star Anna Kournikova. This is an aspect of social engineering: making people believe they're opening a picture of Anna Kournikova instead of your malicious code. A technical feature that could help this social engineering trick, is the possibility in Windows to hide known extensions. This way the second extension showing it is a Visual Basic script, could be hidden and only the jpg extension will then be visible. This and the fact that some time had passed since a major virus outbreak, which leads to people being less cautious, resulted in the virus entering more than 50 enterprise companies, including Fortune 500 firms, within half a day.

Happily the virus died out quite soon. On one hand because information technology workers can better filter messages for this virus, because of the experience with the Love Bug attack. On the other hand, people are warned by many sources like the CERT/CC and SANS, so the user community is prepared and the social engineering trick will not work anymore on a large scale.

The virus creator, his motivation and the consequences

Many times the creator of a virus is only known by his alias, which is hard to relate to a real world person. This time, on February 14, two days after the outbreak, the creator of the Anna Kournikova virus handed himself over to the local police in his hometown of Sneek in the northern province of Friesland, The Netherlands. He was arrested on suspicion of damaging computer programs and property. He was questioned for several hours and then released. The reason he had turned himself in for was that he was shocked at the damage caused by the virus. This had never been his intention, he declared to the police.

One day earlier, the 20-year-old Dutchman declared on his homepage to be the creator of the Anna Kournikova virus. The reason why he created and released the virus is that he is a great fan of Kournikova. He said to be no expert at all: he doesn't know anything about programming whatsoever. He used a virus generator as mentioned before in this paper. Another important reason for him to release the virus was a recent IDC-report stating the Internet world had not learned anything from Love Letter. This gave him the idea to verify this and his virus infected indeed many computers. The service provider has removed the homepage.

Mikko Hypponen, virus research manager at F-Secure Inc.'s European headquarters in Espoo, Finland, had also tracked him down. One of F-Secure's "informants" alerted them to the presence of an anonymous letter on a Dutch Web site hosted by service provider Tripod.com. The letter was written by someone calling himself OnTheFly and claimed responsibility for creating the virus.
"From there it was fairly easy tracking him down," says Hypponen. "Typically a guy like this has been active in the Internet underground before. They change their names all the time, but by watching carefully you can follow the chain of aliases back and locate the guy in the real world. We just turned over all our information to the Dutch authorities."

On Thursday February 15, WEBwereld announces that OnTheFly has gone into hiding. After being released by the police he has disappeared. His mother declared he would not speak to anyone. Before he went into hiding, OnTheFly sent an e-mail message to Wired, repeating he had never expected the virus to spread so quickly and he regrets having released the virus.

At this moment the Dutch attorney general has to decide what charges OnTheFly will face. Under Dutch law OnTheFly can face up to 4 years of prison and a fine of 25.000 Dutch guilders.

On Friday February 16, it is announced by WEBwereld, that the creator of the virus generator VBS Worm Generator 1.5b, [K]Alamar, an 18-year-old guy from Buenos Aires Argentina, has removed the virus generator from his web site. When his name was mentioned on TV, he was advised by friends to remove the program from his site. Because [K]Alamar wants to remain anonymous, he removed the program, so he will not be in the picture anymore.

Conclusion

On February 12 the Anna Kournikova virus broke out. Replicating itself as an attachment through infected e-mail messages faking to be a picture of Anna Kournikova. Many people buy the trick and at first the virus spreads rapidly. Lessons learned from this are to keep the user community educated and alert for suspicious e-mail messages. Also keep all your software up-to-date, especially regarding security updates. Another lesson which can be learned is to have incident response policies in place, so one can react quickly and effectively when such a virus outbreak takes place by for example applying correct filtering rules on your mail servers and getting the latest updates for your anti-virus products as soon as these become available.

The Anna Kournikova virus was created using a virus generator called the VBS Worm Generator 1.5b. Since OnTheFly, the creator of the virus, declared he doesn't know anything about programming, this proves that with more than 100 virus generators available on the Internet, it's quite simple for people to create their own viruses, without being able to program a computer at all!
So it's not unlikely that the Internet community will be exposed to a lot more of this kind of viruses in the near future. This emphasizes the importance of preparing against these viruses (and other threats) before it is too late.

What precautions can be taken to minimize risks against such a threat?

- as mentioned before: keep your anti-virus product and other software up-to-date
- apply all relevant security patches when they become available
- educate, educate, educate your user community to create awareness
  Make clear to not run programs of unknown origin, regardless of who sent it. Also convince your users to not send or forward programs of unknown origin just because they are amusing. They could be sending a Trojan horse…
- some software products, such as many Microsoft products and Lotus Notes, include the ability to automatically execute embedded code. Default this ability is activated for convenience. For security this ability should be disabled
- make use of strong authentication where possible. Using products and technologies like PGP, GPG and S/MIME to encrypt and sign e-mail messages

can help ensure that mail is not altered in transit and can help reducing the ability of an intruder to forge e-mail

- report suspicious activity to your local Computer Security Incident Response Team (CSIRT) Your CSIRT may be able to help you distinguish viruses from ordinary failures and may be able to correlate your report with others they have received.

- subscribe to mailing lists from your software vendors and organizations like CERT and SANS to keep informed about the latest security issues

- have your security management policies in place and up-to-date

And what can be learned from the story regarding OnTheFly, the 20-year-old guy who created the Anna Kournikova virus? On releasing the virus, he is amazed and shocked at the results of his action. People are coming after him, investigating the source of the virus. He turns himself in, has to go into hiding to avoid all the publicity, has a criminal record for life and is now facing a probable sentence of 4 years in prison and a big 25.000 Dutch guilder fine. One can say it turned his life up side down and I think he would not have created the virus if he had known all this beforehand.

Even the creator of the virus generator got involved and removed the software from his web site, because he doesn't want to become publicly known.

This story hopefully makes clear to potential virus creators what the consequences can be, so they'll think it over twice and finally decide not to do such a thing.

References

CERT/CC, "CERT® Advisory CA-2001-03 VBS/OnTheFly (Anna Kournikova) Malicious Code", last revised: February 13, 2001
http://www.cert.org/advisories/CA-2001-03.html

CERT® Coordination Center, "Protecting Yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond", latest revision: January 17, 2000
http://www.cert.org/tech_tips/virusprotection.html

CNN.com, "Kournikova virus suspect arrested", February 14, 2001
http://www.cnn.com/2001/TECH/internet/02/14/kournikova.virus/index.html

Sieberg, Daniel, "New e-mail virus preys on Anna Kournikova fans", February 12, 2001
http://edition.cnn.com/2001/TECH/internet/02/12/anna.worm/index.html

Analysis: Katrin Tocheva, Mikko Hypponen, Sami Rautiainen, F-Secure; February 2001
http://www.f-secure.com/v-descs/onthefly.shtml

WEBwereld news site (Dutch)
http://www.webwereld.nl/nav/n?6736 (and related articles)

Fansler, Bryan. “Virus Generators and Their Implications”, February 19, 2001
http://www.sans.org/infosecFAQ/malicious/generators.htm

VX Heavens, “Virus Creation Tools (54)”
http://vx.netlux.org/dat/vct.shtml

[K]Alamar / Argentina, “VBS Worm Generator 1.5b” - 4 Aug 2000
http://vx.netlux.org/dat/tv07.shtml