



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials Bootcamp Style (Security 401)"  
at <http://www.giac.org/registration/gsec>

## SANS-GIAC Practical Assignment for Security Essential Certification

*Title* : What is [VBS.SST@mm](mailto:VBS.SST@mm) worm?  
*Author* : Eka Hartono  
*Date* : February 2001

---

### Introduction

On February 12, 2001, the world is once again awakened by a new worm attack. The worm was called [VBS.SST@mm](mailto:VBS.SST@mm), was also known as the VBS.Lee-o, VBS.OnTheFly, VBS.Vbswg.gen, Anna Koumikova, and [VBS/VBSWGJ@mm](mailto:VBS/VBSWGJ@mm).<sup>i</sup> The worm circulated rapidly hiding itself as an electronic picture of the famous Russian tennis star Anna Koumikova.<sup>ii,iii,iv</sup>

### What is VBS.SST@mm?

[VBS.SST@mm](mailto:VBS.SST@mm) is a VBS email worm that was being coded using a virus creation tool.<sup>v</sup> The worm arrives as an email attachment called AnnaKournikova.jpg.vbs. Upon execution, the .VBS worm automatically email itself to the email address list in Microsoft Outlook. In addition, the worm comes with a message: “Hi: Check This!” and at least three subject lines were identified: “Here you are”, “Here you have”, and “Here you go” followed by a smiley face.<sup>vi</sup> There is no damaging payload of the worm, except for automatically directing the infected user’s web browser an Internet address in Netherlands (<http://www.dynabyte.nl>). The Internet address is apparently a Dutch’s shop website.<sup>vii</sup> According to Symantec AntiVirus Research Center, the worm is considered highly in the Wild and has high distribution capability.<sup>viii</sup> However, since the worm will just tied up the mail server with its’ action of sending mass mailing, the worm is considered at a low damage level.

### How does it work technically and how to get rid of it?<sup>ix</sup>

When the user clicks on the attachment, the worm will run and create the registry key:

```
HKEY_CURRENT_USER\Software\OnTheFly
```

Once January 26 of each year hits, the work will attempt to direct the user’s web browser to <http://www.dynabyte.nl>.

In the mean time, the worm will check if mass mailing to all the email address in Microsoft Outlook has been sent. If such an action is not yet executed, it will send the mass mailing and set the registry key:

```
HKEY_CURRENT_USER\Software\OnTheFly\mailed ; to “1” (value one), to prevent the mailing routine to execute again.
```

Within a period of time after the first attack of this worm, major anti-virus vendors managed to provide solution to prevent and remove the worm. One of the major Internet security vendors, Symantec Corporation, recommends its' customers to download the latest virus definition to detect the worm and do the following action to remove the worm from their systems:

1. Run Live Update to make sure the system has the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and run a full system scan, making sure that NAV is set to scan all files.
3. If any files are detected as infected by VBS.SST@mm, click Delete
4. (Optional) Delete the following registry key:

HKEY\_CURRENT\_USER\Software\OnTheFly

In fact, users who are fairly educated on the fact that that .EXE and .VBS files are executable and worm/virus prone, would have already deleted the attachment. Thus, prevent them from being infected. However, as mentioned by Vincent Weafer and Stephen Trilling of Symantec, "Close to Valentine's Day, anything novel or different like this will get people's attention more than normal"<sup>x</sup> and since the .VBS extension may be hidden and people are attracted to the .JPG attachment of the tennis star, it increases the likelihood of a user "clicking" on the attachment.<sup>xi</sup> Unlike .EXE and .VBS, .JPG is not typically viral.

In addition, since the removal of the worm is considered easy, IT personals can now better filter these types of scripts worms and users now know not to click on AnnaKoumikova.jpg.vbs, the worm should start dying out quickly.

### Who wrote the [VBS.SST@mm](#) worm and why?<sup>xii, xiii</sup>

According publications referred in this paper, the worm was written by a young Dutch man who claimed to have no intention on creating such havoc and was apparently surprised with the damage it potentially created. Even more interesting, the writer claimed to have no programming skill and used a "virus toolkit" known as a Visual Basic Worm Generator to create the worm.

In addition, he claimed to be a big fan of Anna Kournikova, thus the Anna Koumikova photo masquerade, and simply needed an internet site to be attached to the program, thus [www.dynabyte.com](http://www.dynabyte.com) was chosen.

### Conclusion

Asserting my own opinion to this recent outbreak, you do not have anti-virus software in your system or have not recently up-date your anti-virus software,

please do so immediately. This latest news definitely creates an alarming awareness of the potential of major virus/worm outbreaks, simply because of the wide spread availability of virus/worm generator toll kits.

---

## Glossary

Worm - Is an independent program that replicates itself, crawling from machine to machine across network connections. It often clogs networks as it spreads -- often via e-mail.<sup>xiv</sup>

Virus - A program that can "infect" or "contaminate" other programs by modifying them to include a copy of itself. Viral code is typically malicious and detrimental to data or system integrity.<sup>xv</sup>

Wild – The extent to which a virus is already spreading among computer users. This includes number of independent sites infected, the number of computers infected, the geographic distribution of infection, the ability of current technology to combat the threat, and the complexity of the virus.<sup>xvi</sup>

Payload – This is the malicious activity that the virus performs. Not all viruses have payload, but there are some that perform destructive actions.<sup>xvii</sup>

---

## Related Readings

McCargo, Bernard. How Viruses Attached. 8 December 2000. URL: <http://www.sans.org/infosecFAQ/malicious/attach.htm> (19 February 2001)

Whalen, Tracey. "I Love You" Worm. 9 September 2000. URL: [http://www.sans.org/infosecFAQ/malicious/iloveyou\\_worm2.htm](http://www.sans.org/infosecFAQ/malicious/iloveyou_worm2.htm) (19 February 2001)

Dooley, Patricia. What is the VBS.Stages.A Worm? 28 November 2000. URL: [http://www.sans.org/infosecFAQ/malicious/VBS\\_stages.htm](http://www.sans.org/infosecFAQ/malicious/VBS_stages.htm) (19 February 2001)

Williams, Gary. VBS\_NEWLOVE.A Worm. 1 December 2000. URL: [http://www.sans.org/infosecFAQ/malicious/VBS\\_NEWLOVE.htm](http://www.sans.org/infosecFAQ/malicious/VBS_NEWLOVE.htm) (19 February 2001)

---

## References

---

- <sup>i</sup> Chien, Eric and Hindocha, Neal. SARC Write-up – [VBS.SST@mm](http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html). 15 February 2001. URL: <http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html> (19 February 2001).
- <sup>ii</sup> E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: <http://espn.go.com/tennis/news/2001/0212/1079565.html> (16 February 2001)
- <sup>iii</sup> Lemos, Robert. From Russia with Love? Koumikova Virus Smashes Net. ZDNet News. 12 February 2001. URL:[http://dailynews.yahoo.com/h/zd/20010212/tc/from\\_Russia\\_with\\_love\\_koumikova\\_virus\\_smash](http://dailynews.yahoo.com/h/zd/20010212/tc/from_Russia_with_love_koumikova_virus_smash) (16 February 2001)
- <sup>iv</sup> Sieberg, Daniel. New Email Virus Preys on Anna Koumikova fans. 12 February 2001. <http://www.cnn.com/2001/TECH/internet/01/12/anna.worm/index.html> (16 February 2001)
- <sup>v</sup> Chien, Eric and Hindocha, Neal. SARC Write-up – [VBS.SST@mm](http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html). 15 February 2001. URL: <http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html> (19 February 2001).
- <sup>vi</sup> E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: <http://espn.go.com/tennis/news/2001/0212/1079565.html> (16 February 2001)
- <sup>vii</sup> Delio, Michelle. Anna Worm Write Tells All. 13 February 2001. URL:<http://www.wired.com/news/technology/0,1282,41782,00.html> (17 February 2001)
- <sup>viii</sup> Chien, Eric and Hindocha, Neal. SARC Write-up – [VBS.SST@mm](http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html). 15 February 2001. URL: <http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html> (19 February 2001).
- <sup>ix</sup> Chien, Eric and Hindocha, Neal. SARC Write-up – [VBS.SST@mm](http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html). 15 February 2001. URL: <http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html> (19 February 2001).
- <sup>x</sup> E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: <http://espn.go.com/tennis/news/2001/0212/1079565.html> (16 February 2001)
- <sup>xi</sup> Head of Research at Symantec's Anti-Virus Research Center discussed about Anna Koumikova Virus. 12 February 2001. URL: <http://www.usnewscast.com/messageboard/NASDAQstocks/symc/index.html> )19 February 2001)
- <sup>xii</sup> Delio, Michelle. Anna Worm Write Tells All. 13 February 2001. URL:<http://www.wired.com/news/technology/0,1282,41782,00.html> (17 February 2001)

---

<sup>xiii</sup> Koumikova Virus Suspect Arrested. 14 February 2001. URL: <http://www.cnn.com/2001/TECH/internet/02/14/kournikova.virus/index.html> (17 February 2001)

<sup>xiv</sup> Symantec Anti-Virus Research Center. URL: <http://www.sarc.com> (19 February 2001)

<sup>xv</sup> Symantec Anti-Virus Research Center. URL: <http://www.sarc.com> (19 February 2001)

<sup>xvi</sup> Symantec Reference Area – Glossary of Terms. URL: <http://www.symantec.com/avcenter/erfa.html> (19 February 2001).

<sup>xvii</sup> Symantec Reference Area – Glossary of Terms. URL: <http://www.symantec.com/avcenter/erfa.html> (19 February 2001).

© SANS Institute 2000 - 2002, Author retains full rights

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor