GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC Level Two

Advanced Incident Handling and Hacker Exploits course

Practical - Option 2

Document an exploit, vulnerability or malicious program

TROJANS
APStrojan.qa

David A. Santoro
davsanto@hotmail.com

© SANS Institute 2000 - 2002, Author retains full rights.

SANTORO, DAVID
MBUS544

Table of Contents

INTRODUCTION 2
EXPLOIT DETAILS: 3
PROTOCOL DESCRIPTION 4
DESCRIPTION OF VARIANTS 4
HOW THE EXPLOIT WORKS 4
DIAGRAM 6
HOW TO USE THE EXPLOIT 7
SIGNATURE OF THE ATTACK 7
HOW TO PROTECT AGAINST IT 8
SOURCE CODE/ PSEUDO CODE 10
ADDITIONAL INFORMATION 11
REFERENCES 15

Figures and Tables

FIGURE 1 - TYPICAL TROJAN RELATIONSHIP 7
FIGURE 2 - APSTROJAN.QA PROCESS 7
TABLE 1- RATE OF INFECTION 13

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

INTRODUCTION

This paper concerns the practical associated with the *SANS Advanced Incident Handling and Hacker Exploits course.* This is Option Two, which is to "*Document an exploit, vulnerability or malicious program.*"

There are hundreds, if not thousands of malicious programs. Some of these programs are unique while many other are just variations of one another. Either way these programs are designed to perform an action that is not wanted. Many of these malicious programs are freely available via the Internet, such as sites as: technotronic.com, backcode.com, and anticode.com just to name a few. These programs usually and can end up in the hands of *Script Kiddiez.* And as Marcus Ranum presented to the 27th Annual CSI Computer Security Conference and Exhibition, stating that *Script Kiddies Suck because:*

1. *They represent a great deal of noise that must be filtered out*

2. *It's imperative to reduce the script kiddie population in order to be able to meaningfully quantify the size and talent of the real threat*

One particular type of malicious program that script kiddies and other may use is the Trojan.

> " A Trojan is a program that does something more than the user was expecting, and that extra function is damaging. This leads to a problem in detecting trojans. Suppose I wrote a program that could infallibly detect whether another program formatted the hard disk. Then, can it say that this program is a trojan? Obviously not if the other program was supposed to format the hard disk (like Format does, for example), then it is not a trojan. But if the user was not expecting the format, then it is a trojan. The problem is to compare what the program does with the user's expectations. You cannot determine the user's expectations for a program."[1]

[1] *All About Viruses* by Dr. Alan Solomon http://www.drsolomon.com/vircen/allabout.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A Trojan is made up of two parts, the client and the server. The server resides and hides on the host computer that opens a port or ports allowing the client part to access to the host computer.

Additionally Trojans can be classified according to three main types as described:

1) **Password stealing Trojan:** these steal passwords, cached and recorded then send them in some form to the hacker, sometimes by email sometimes or by other means.

2) **Basic file server Trojan**: these Trojans create a hidden file server onto the victims computer that allows the hacker access to the victims hard drive, these are sometimes used to upload more dangerous trojans

3) **Remote administration Trojan:** these are more sophisticated Trojans, such as Donald Dick, Doly and NetBus. Using a Trojan of this type the hacker can basically do anything. Such as accessing your keyboard, mouse, cam, passwords, and icq.

This paper will discuss the Trojan named **APStrojan.qa**. This Trojan is classified as a password stealing Trojan since it is designed to steal AOL Passwords. Additionally **APStrojan.qa**, because of the way it operates, can also be classified as a virus or Internet worm. Although it has been around in some form or another since 1998 there has been a reassurance of this Trojan since the January/February 2001 timeframe. The extent on the effect of this Trojan remains a controversy, which will be discussed latter.

EXPLOIT DETAILS:

Name: APStrojan.qa

Variants: APStrojan.pz, APStrojan.qa, MINE.EXE, ASPTrojanT.a, AOL.PS.Trojan**,** PWSteal.Trojan, AOL.Trojan, and AOL.PWSteal,

Operating System:

Windows 95, Windows 98, Running AOL version 4.0.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Protocols/Services:

AOL hosting service, SMTP since program is sent via email.

Brief Description: APStrojan.qa is a password stealer that affects users of America Online. It is spread via e-mails with the subject line "Hey You". The email contains an attachment called mine.exe, which installs the Trojan to the computer.

PROTOCOL DESCRIPTION

Since this Trojan works with the use of emails the protocols it uses are SMTP, POP3 and IMAP. SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. It is usually used with one of two other protocols, POP3 - Post Office Protocol Version 3 (Port 110) - or IMAP - Internet Message Access Protocol (Port 143), which allows the saving of messages in a server. Typically SMTP is used for sending e-mails and either POP3 or IMAP is used for receiving messages that have been received for them at their local server.

DESCRIPTION OF VARIANTS

According to the major anti-virus sites, such as Mcafee.com, this Trojan/virus is part of a family of similar malicious code. The variants are minor and mainly consist of differences in the names of the executable and other attached file names. Usually the executable is known as mime.exe but can also be known as:

WINPFC.EXE, POKEMON.EXE, PKG80B5.EXE, JPG.EXE, PKG3B0.EXE MY_NEW_P.EXE, FIX.EXE, BOUNCE.EXE, PUMA.EXE, AIY2K.EXE, OFFICE.EXE, AOL32.EXE, MAILTO~1.EXE, MYPICBMP.EXE, PUNTTEK3.EXE, MYPICVIE.TRJ, WINSPY.EXE, KING.EXE

Additional information on this Trojan/virus can be found at the major anti-virus sites such as mcafee.com, drsolomon.com or symantec.com.

HOW THE EXPLOIT WORKS

This Trojan is used in the following manner:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

APStrojan.qa is written in Visual Basic 5, which as discussed, is designed to attack America Online software installations to determine the password of user accounts. Additionally, it will send the account detail to the originator of the Trojan. And, if the victim is logged onto AOL v4.0, it will then send itself to AOL screen names listed in the buddylist who are currently logged onto AOL.

This file is usually received by email as an attachment named "mine.zip" (with a size of 77,855 bytes) and with a subject line of "hey you". The message body suggests that the attachment is actually scanned pictures. The email usually looks like the following:

> ***Beginning of message***
> *hey i finally got my pics scanned..theres like 5 or 6 of them..so just download it and unzip it..and for you people who dont know how to then scroll down..tell me what you think of my pics ok?*
> *if you dont know how to unzip then follow these steps*
> *When you sign off, AOL will automatically unzip the file, unless you have turned this feature off in your download preferences.*
> *If you want to do it manually then On the My Files menu on the AOL toolbar, click Download Manager. In the Download Manager window, click Show Files Downloaded. Select my file and click Decompress*
> ***End of message***[2]

The executable, mime.exe, creates several files:

```
c:\msdos98.exe
c:\WINDOWS\SYSTEM\mine.exe
c:\WINDOWS\SYSTEMS\ReadMe.Txt
c:\WINDOWS\uninstallms.exe
```

It also edits the WIN.INI file with the line `run=c:\windows\uninstallms.exe` so the Trojan can load when the PC reboots. The Trojan also detects a person attempting to log onto AOL and will record the username and password details. These details will then be forwarded back to the person who send the Trojan giving the hacker access to user's e-mail and other personal information. The Trojan will also try to e-mail itself to all of the contacts listed in the member's AOL Buddy List, thus spreading the program around.

---

[2] Sharon Gillian, www.about.com\bl_virus01.htm, Feb, 4th 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

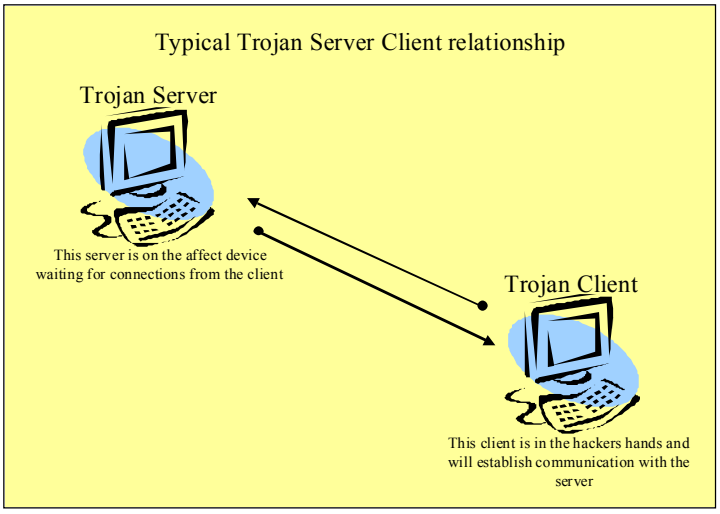
Additional problems are encountered if the malicious code has infected a system.

- Desktop background may not work
- Freeze computer once signed onto AOL
- Cannot shut down from start menu
- Cannot open win.ini or registry
- Password problems signing in AOL

AS shown this Trojan exploits AOL (America On Line) software version 4.0. But:

"Improvements to Versions 5.0 and 6.0 prevent the virus from replicating itself, although it can still steal passwords from users of those versions. In addition, when a user of AOL Version 6.0 is infected, the virus creates a pop-up message urging the user to switch back to Version 4.0 of the software."[3]

DIAGRAMS



[3] James Niccolai, Virus may steal AOL users' passwords,

http://www.nwfusion.com/news/2001/0201aolvirus.html, Feb, 1st 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 1 - Typical Trojan Relationship

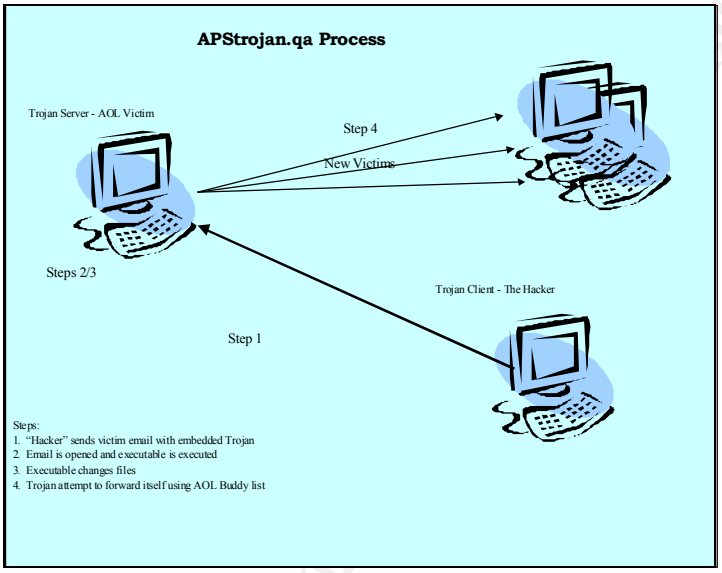


Figure 2 - APStrojan.qa process

HOW TO USE THE EXPLOIT

Again the exploit is used to obtain AOL user information and passwords and also to spread the exploit to other systems via email. Once the user information and passwords are obtained the hacker can log into AOL as the stolen identify and either masquerade as the other person or obtain additional information on that person.

SIGNATURE OF THE ATTACK

This attack is difficult to detect before any damage is done. Usually the anti-virus scanners can detect this Trojan only after a system is infected with the virus. In some Trojans, such as Doly or NetBus the server that is running on the infected system may not be detected. This server quietly runs waiting for a connection to the client. If right now one would look at the Processes Tab in the Windows Task Manager there are many processes running. If the system has a server part of a Trojan installed it would be listed as one of the processes. But which on is it? Unless the name is known of the Trojan's process it is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

difficult to determine which service it is. For example the Doly server lists its process as *memmanager.exe.* Just by looking at the name one could assume that is was some type of memory management program running on the system

HOW TO PROTECT AGAINST IT

The best course of action against this type of malicious code is vigilance against attachments in emails. Don't open emails that you are unsure of. And, of course have and keep the anti-virus up to date so when a system is compromised quick detection can minimize the impact.

> *(A personal note: Before I entered the IA field I was doing some work were I was requesting certain vendors to answer a questionnaire about their products. The most efficient way to present this questionnaire was via email. In my email I had an Excel Spreadsheet zipped in an attachment. Most vendors opened the attachment and provided me the requested information. But there was one vendor who replied that is was a security issue for them to open attachments of this type and that you should never open attachments from unknown or trusted sources.)*

Additionally in a corporate environment to protect against the Trojan threat, it is essential to foster a culture of safe computing that is supported by an effective security policy that has full management support. Safe computing should be defined by training courses where corporate users can learn that good security is in their best interests. The courses should teach practices, such as downloading software from unauthorized sources, running unsolicited programs or opening unsolicited email attachments, and not antivirus scanners.

There are other ways of "personal" protection against Trojans (not necessarily viruses) by installing software that scans for Trojans. Once such program that is installed on a single device is Lockdown 2000 (www.lockdown2000.com), which scans for Trojan signatures. This is a type of personal IDS. Or in an enclave or enterprise situation a Network IDS product, such as RealSecure, could be implemented and Trojan Signatures be activated to look for Trojan activity. Normally in this case the Trojan is already installed on a system or

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

systems and the IDS is monitoring and communication activity between the Trojan server and Trojan client. And depending on how the signature is written and the IDS configured the IDS can only detect certain instances of this activity.

(Personal note: Recently, one of the projects at my company was to test an IDS in beta form and determines how and what it detects. In one of the tests we set up a Doly Trojan server (Several variations of this program) on one device on the lab network and the Doly client on a different sub net of the network. A Network IDS agent was monitoring the network the Doly Trojan server was on. The IDS was configured to monitor this Trojan activity. The following shows the configuration and results:

Configuration

- *Doly Servers 1.6 and 1.7 were installed on device NT1 (192.168.5.6)*
- Security policy applied to network sensor was TEST. This policy includes the network signature for Doly.

Execution

- *Using Doly client GUIs, connections were established to the Doly servers, and various commands executed.*

Results

- *The IDS did not detect the connection or commands.*

  The IDS did not detect Doly versions 1.6 or 1.7. Both versions communicate on port 1016. The Doly Signature is written to look only at port 1015.

Comments

- *There are several versions of the Doly Backdoor. Apparently, different versions use different ports. The IDS signature is written to listen on port (1015). Both versions tested (1.5 and 1.6) as installed in our test environment used port 1016. Documentation was found that indicated Doly might use ports 1010, 1011 or 1012, also (in addition to 1015 and 1016).*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *As a "sign of life" test, a connection event was configured on the Network Engine to detect all connections to port 1016. This event was successfully triggered when the Doly client connected to the Doly sever.*

The results are interesting because it shows the limitations of the IDS signature especially when the Trojan is designed to operate on different ports. Of course in this case with the ASP Trojan/virus the IDS would be of little use in detected the initial installation of the Trojan. Additionally depending on the IDS signature and the operation of the Trojan's Server and Client, the IDS will either only detect the initial connection and not subsequent connections or will detect each and every connection made between the server and client.

Other observations in this test were the fact that all Trojans are not created "equally." Meaning that the Trojans downloaded from the Internet did not work or were difficult to get to work properly. I suppose hackers have little quality assurance. This being the case we found some Trojans difficult to install in our test environment. Imagine a Script Kiddie downloads a Trojan and attempts to install the Trojan server on a suitable device and then the Trojan doesn't work. (Which is probably a good thing.) The difficulty we had in the lab where we have all the access to devices now becomes a greatly difficulty for the amateur hacker. Bottom line is that it may not be as easy as it seems to install and operate Trojans.

SOURCE CODE/ PSEUDO CODE

There are numerous sites and newsgroups that contain source codes for malicious programs like:

www.tlsecurity.net
www.zarr.com
www.nitro2000.de
www.neworder.box

But the source code the **APStrojan.qa** could not be located. In lieu of this source code, attached as directed, is the source code for a similar Trojan/virus called Atomic2 – which is primarily a Dial Up password retriever. According the readme file:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"Once Atomic2 executes it copyies itself to "dialupsc.exe" in your windows system directory and creates a registry entry under "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run" named "DialUpSecurity". Then waits for a Dial Up connection to be made and when the connection is alive it sends all the information via a SMTP server to one ore more email addresses. After that it saves all information that was sent to a file in the system directory ("rasxnfo.dll") and closes itself. When restarting windows it will close automatically if the new information match the information that was already sent. The data is encoded (use "decode.exe" to decode it, input file: encode_in.txt , output file: decode_out.txt)"

(Spelling errors are original)

ADDITIONAL INFORMATION

It this a Trojan or Virus?

Reading this paper the **APStrojan.qa** has been referred to both a Trojan and a virus but:

"A Trojan is not the same thing as a virus because it does not tend to replicate itself. But, according to Graham Cluley, of antivirus software vendor Sophos, most antivirus products detect a number of Trojan horses. 'Even though they aren't technically viruses, users still lump them in with the virus problem."[4]

In this case the **APStrojan.qa** is both a Trojan and a virus. A Trojan because part of the code is monitoring the infected device for attempted connections to AOL in order to capture user information and password to be deliver to the hacker. It is a virus because it is attempts to spread itself around by using the AOL Buddy list and email itself to other users, which in turn become infected.

Virus Alert Controversy

[4] David Norfolk, http://www.zdnet.co.uk/itweek/analysis/2000/45/internet/, Jan, 27th 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As discussed in the beginning of this paper **APStrojan.qa** has been around for sometime and the recent activity of this code has caused some controversy some claim that a virus alert made by anti-virus companies made be done so for their own benefit and not really reflect the actual threat. "McAfee.com reported on its Web site that more than 72 million computer files and as many as several million personal computers have been hit with the virus--known as APStrojan.qa--in the last 30 days." [5] Yet sites like SecurityPortal.com which tracks virus did not list the APStrojan.qa or any of its variants in the top 20-virus list. A look at the reported numbers as told by Mary Landersman, Antivirus Software guide at about.com claims the following:

"Of the 31 variants of AOL Password Stealing Trojans, McAfee is reporting that of the 78,912,499 files (not computers, but individual files) scanned, 230,497 were infected with some variant of an AOL Password Stealing Trojan. Now we're focusing only on the reports of this particular type of Trojan, so we can make another assumption that this report is dealing with only a very small percentage of the 1,050,000 we determined had their system scanned during the last thirty days at McAfee.com. Of this very small percentage, only .58 (that's just over half of one percent) were infected with any variant of AOL password stealing Trojans. Now, I'm going to withhold judgement and let readers decide. Do you think this virus alert is justified?"[6]

The following table is from
http://vil.mcafee.com/dispVirus.asp?virus_k=10567, which shows the rate of infection as of January 31, 2001, as documented by mcafee.com.

[5] Jube Shiver JR, McAfee Issues Controversial Bug Advisory, Los Angeles Times, Feb, 2nd 2001

[6] Mary Landersman,
http://antivirus.about.com/compute/antivirus/library/weekly/aa020301a.htm?terms=aol, Feb, 15th 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

VIRUS FAMILY STATISTICS - Past 30 Days			
Virus Name	Infected Files	Scanned Files	% Infected Computers

Table 1- Rate of Infection

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Removing APStrojan.qa

Found during this research was several methods to remove this program from an infected system. The following is an example to accomplish this:[7]

Here's how:

1. Reboot the computer and quickly hit the F8 key before Windows starts. You should get a boot menu. Select Safe Mode and let Windows boot.
2. Double click on 'My Computer.' Select Options from the View Menu. Then click on the View tab.
3. Make sure 'Show all files' is selected and 'Hide file extensions' is not selected. Click Ok.
4. Double click on the icon for your C drive. Then find the file named msdos98.exe, right click on it and select Delete. If asked to confirm, click Yes.
5. Double click on the Windows folder. Find the file uninstallms.exe, right click on it and select Delete. If asked to confirm, click Yes.
6. Right click on the file Win.ini (not winfile.ini) and select Properties. Make sure the box for Read Only is unchecked. Click Ok.
7. Double click on Win.ini. A notepad window will open. Select Find from the Search menu. Search for the text c:windowsuninstallms.exe.
8. When you find the text c:windowsuninstallms.exe, delete it. Save the file win.ini and close it.
9. Double click on the System folder. Find the files mine.exe and readme.txt and delete them.
10. Select Run from the Start Menu and type regedit.exe in the window that pops up. Click Ok.
11. Once in the Regedit program, click the plus sign next to HKEY_LOCAL_MACHINE.
12. Then click the plus signs next to Software, Microsoft, Windows, CurrentVersion and Run in that order.
13. In the right window pain, you should see an item that says Windows and then c:msdos98.exe in the column next to it. Highlight the word Windows and hit delete. Click Yes when asked to confirm.
14. Select Exit from the Registry Menu.
15. Restart your computer.

Tips:

1. Wait until your computer beeps to hit the F8 key to get the boot menu.
2. If you hit the F8 key too late, you won't get the boot menu and you'll have to restart again.

[7] Sharon Gillson, http://aol.about.com/internet/aol/library/howto/htvirus.htm, Feb, 16th 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As you can see that it takes some effort to repair a device with this malicious code

REFERENCES

www.tlsecurity.net/sourcecodeb.html
www.zarr.net
www.cnn.com/2001/TECH/computing/02/01/aol.virus.idg/index.html
www.nitro2000.de/csource.htm
www.neworder.box
www.lockdown2000.com
www.drsolomon.com/vircen/allabout.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.