



Sober Blast – CME-681
infectionvectors.com
November 2005

Overview

After a long and successful run, the Sober worm adds another feather to its cap with an incarnation promising racy pictures and more information about why the CIA is investigating you. Sober.X, released in late November 2005 became the largest worm outbreak of the year.

CME-681/Sober.X

As was the case with previous variants, Sober.X sends itself in English or in German (dependant upon the TLD it is sending its message to). The worm is received as an attachment to a message such as:

```
From: Admin@hotmail.com
To: Z-Account2501@earthlink.net
Date: Wed, 23 Nov 2005 19:17:11 UTC
Subject: Paris Hilton & Nicole Richie
Attachment: downloadm.zip
Importance: Normal
X-Priority: 3 (Normal)
Message-ID: <1bb8.09923caa400@hotmail.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="====184f41ee9ae.d615baa"
```

The Simple Life:

View Paris Hilton & Nicole Richie video clips , pictures & more ;)
Download is free until Jan, 2006!

Please use our Download manager

```
From: scott@ofallonchamber.org
To: address@earthlink.net
Date: Wed, 23 Nov 2005 18:14:07 GMT
Subject: hi, ive a new mail address
Attachment: mailtext.zip
Importance: Normal
X-Priority: 3 (Normal)
Message-ID: <alfacd9.a55b9d9ff@ofallonchamber.org>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="aedb3ca7b.fbcf86c6b4b1e0"
```

hey its me, my old address dont work at time. i dont know why?!
in the last days ive got some mails. i' think thaz your mails but im
not sure!

plz read and check ...
cyaaaaaaaa

Inside each ZIP file (no matter the name of the archive), is a copy of the worm named "File-packed_datInfo.exe). Upon execution (which requires the user to open the contents of the compressed archive), Sober.X kicks off the following:

Initially, the worm displays a fake warning message, similar to other worms. This is an attempt to mask what the malware is doing in the background by making the user think the file was not successfully opened.



To insure that the worm starts with the machine, Sober.X sets the following Registry value:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
Windows: "C:\WINDOWS\WinSecurity\services.exe"

[Note: "WINDOWS" is replaced by the %Windir% value for the respective operating system.]

To complement the installation, CME-681 creates a new folder in the %Windir% directory, inaccurately named "WinSecurity." The folder contains a number of copies of the worm.



Like previous versions of Sober, the worm attempts to kill Microsoft's Malicious Software Removal Tool, by ending the process mrt.exe. In addition, it attempts to stop processes named: asw*.tmp. Sober.X tries to end previous incarnations of itself by adding multiple empty files to the Windows system directory.

To ensure it is working with a "live" system, Sober.X verifies that the host is connected to the Internet by attempting to reach one of 41 hard-coded NTP servers. Once that is complete, the worm begins connecting to mail servers hosting addresses harvested from the infected host:

```
From: Service@lists.tislabs.com
To: omstudio@hotmail.de
Date: Thu, 24 Nov 2005 01:47:14 GMT
Subject: Mailzustellung wurde unterbrochen
Importance: Normal
X-Priority: 3 (Normal)
Message-ID: <13aae.620a14b4d3b@lists.tislabs.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="===3e2ea0d0f59c2.8bdeb8d9"
Content-Transfer-Encoding: 7bit
```

This is a multi-part message in MIME format.
-----3e2ea0d0f59c2.8bdeb8d9

This is an automatically generated Delivery Status Notification.
SMTP_Error []
I'm afraid I wasn't able to deliver your message.

This is a permanent error; I've given up. Sorry it didn't work out.

The full mail-text and header is attached!

-----3e2ea0d0f59c2.8bdeb8d9

Content-Type: application/octet-stream; name=Email_text.zip

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename="Email_text.zip"

UESDBAoAAAAAACQdjPMYus3XtgAAF7YAAAYAAAAARmlsZS1wYWNRZWRfZGF0YUluZm8uZXh
lTVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAyAAAAA4fug4AtAnNlbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSB5dW4ga
W4gRE9TIGlvZGUuDQ0KJAAAAAAAAABd+8faGZqpiRmaqYkZmqmJmoaniRiaqYlwhaCJHJqp
iQmFpIkYmqmJUmljaBmaqYkA[worm payload clipped here]

Scheme

The success of this version of Sober is a familiar story: a well-crafted con. Social engineering is correctly credited with the overwhelming explosion of Sober.X messages on the Internet in late November 2005.

The US FBI has posted an alert indicating that the message is in fact spoofed and not from their agency. <http://www.fbi.gov/pressrel/pressrel05/emailscheme112205.htm>

