

# [REVS] Worm Analysis – Microsoft LSASS Buffer Overflow from Exploit to Worm

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0028.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/06/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 6 Oct 2004 14:37:20 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Worm Analysis – Microsoft LSASS Buffer Overflow from Exploit to Worm

---

## SUMMARY

The document linked below provides a thorough analysis of a worm that exploits the vulnerability discussed in

<<http://www.securiteam.com/windowsntfocus/5YP0C15CKY.html>> Windows Local Security Authority Service Remote Buffer Overflow (MS04-011). The paper explains the original exploit code, how it is used by a malicious attacker, and how the worm was developed from it.

## DETAILS

Statement of Purpose:

This paper is an analysis of the vulnerability in the Microsoft Local Security Authority Service. This vulnerability has been widely exploited and at the time of this writing it has been implemented into most new worms that are released. Publicly released exploit code (released by [houseofdabus](#)) will be examined to show how it is compiled and then used against targets. We will show the attacker can use tools such as Netcat to gain access to the compromised machines. We will then review how with the use of tools such as Snort and Ethereal we can detect and monitor the attack. Lastly, we will show common utilities can be combined to create a

Securiteam: [REVS] Worm Analysis – Microsoft LSASS Buffer Overflow from Exploit to Worm

snapshot of a compromised system. Next a worm that utilizes this attack will be analyzed. For this paper we will review the Korgo.V worm. This paper reviews the 5 steps of system exploitation. These steps are Reconnaissance, Scanning, Exploiting the System, Keeping Access and Covering Tracks. Finally, the six step Incident Handling process developed by the SANS Institute to show how to contain this threat is examined. We will also review a few different ways companies can prevent this type of threat from wreaking havoc on their networks.

The whitepaper can be found at:

<[http://www.giac.org/practical/GCIH/Travis\\_Abrams\\_GCIH.pdf](http://www.giac.org/practical/GCIH/Travis_Abrams_GCIH.pdf)> Microsoft LSASS Buffer Overflow from exploit to worm

ADDITIONAL INFORMATION

The original article can be found at:

<[http://www.giac.org/practical/GCIH/Travis\\_Abrams\\_GCIH.pdf](http://www.giac.org/practical/GCIH/Travis_Abrams_GCIH.pdf)>  
[http://www.giac.org/practical/GCIH/Travis\\_Abrams\\_GCIH.pdf](http://www.giac.org/practical/GCIH/Travis_Abrams_GCIH.pdf)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.