



## eSecurity Advisory: Blackmal Email Worm

A new variant of an old worm is scheduled to be released this Friday, February 3. The W32.Blackmal.E worm, initially released on Jan. 17, is programmed to implement a very destructive routine that repeats on the third day of each month. The worm, which is scheduled to begin this malicious activity on Friday, Feb. 3, replaces the contents of files such as Word documents, Excel spreadsheets, PowerPoint presentations, and Access databases. It uses subject lines such as "**Photos**", "**\*Hot Movie\***", and "**Miss Lebanon 2006**" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected.

The State's anti-virus definition files are up to date and our gateway is well protected, but additional variants of the worm are anticipated. We ordinarily do not release advisories about individual worms, but because of the destructive nature of this worm, we wanted to bring this to your attention to protect both your work computer and your home computer.

### What can you do?

Do you have any Word, Excel, or PowerPoint files on your local C: drive? If so, we strongly recommend taking precautionary measures and saving these files to a server that is backed up regularly. This is a good time to get out of the habit of keeping important files only on your C: drive.

**Do you preview your inbox looking for suspicious emails before opening them?**

If not, *start now!*

Listed below is more information that may helpful to users to protect their work and home computers.

---

### SUBJECT:

Blackmal Email Worm destroys files on the third day of each month

### OVERVIEW:

Blackmal.E (aka Nyxem.E, MyWife.d) is a new email worm which will overwrite or destroy files on an infected system on the third day of each month. The files destroyed include Microsoft Office files including Word documents, Access database and PowerPoint files; files belonging to various Anti-Virus applications; Adobe Acrobat files and others. In addition to spreading via email, this worm can also spread through network file sharing where the file shares are not password protected or have a weak password.

Although anti-virus vendors are rating this low-medium risk, it is important to note the destructive nature of this worm. Additionally, the worm may spread via email attachments that may not normally be blocked at email gateways. Additional variants of this worm are anticipated.

**SYSTEMS AFFECTED:**

- Microsoft Windows 2003/2000/95/98/ME/NT/XP

**RISK:**

Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: **High**

**DESCRIPTION:**

W32.Blackmal.E@mm is a mass-mailing worm that relies on user intervention to spread. The worm typically arrives in a malicious email attachment, though it can also spread through file-sharing networks. The worm uses social engineering to trick users into opening unsolicited emails. Once executed, the worm scans the victim's computer for email addresses and uses its own SMTP engine to send copies of itself to these harvested addresses. Additionally, on the third day of every month, it will destroy various file types on the infected systems. The files destroyed will have the following file extensions: .doc, .xls, .ppt, .mdb, .mde, .zip, .rar, .pdf, .psd, .dmp, .pps and files belonging to Anti-Virus applications.

**REFERENCES:**

**SANS**

<http://isc.sans.org/blackworm>

<http://www.incidents.org/diary.php?storyid=1065>

**SecuriTeam Blog**

<http://blogs.securiteam.com/index.php/archives/241#more-241>

**Symantec**

<http://securityresponse.symantec.com/avcenter/venc/data/w32.blackmal.e@mm.html>

**Sophos**

<http://www.sophos.com/virusinfo/analyses/w32nyxemd.html>

**McAfee**

[http://us.mcafee.com/virusInfo/default.asp?id=description&virus\\_k=138027](http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=138027)

**Trend Micro**

[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM\\_GREW.A](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_GREW.A)

[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM\\_GREW.B](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_GREW.B)

**F-Secure**

[http://www.f-secure.com/v-descs/nyxem\\_e.shtml](http://www.f-secure.com/v-descs/nyxem_e.shtml)

**Computer Associates**

<http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=50198>