



US-CERT Critical Infrastructure Information Notice CIIN-08-074-01 March 14, 2008

Spear Phishing Campaign Directed at USG Employees (U//FOUO)

Overview (U//FOUO)

US-CERT has received reports of spear phishing campaign currently underway that may be directed towards US defense contractors and government employees. US-CERT is issuing this report to provide early notification of this activity and prevent further compromises from occurring. US-CERT will continue to investigate this activity and provide updates as needed.

Details (U//FOUO)

US-CERT has received information that a phishing email containing a .zip file or link to a .zip file has been circulating. The emails are believed to have been first sent on March 13, 2008.

The senders address appears as `grace[dot]a[dot]harris@gmail[dot]com`, however it is likely that the address was spoofed and could change.

The subject of the email is "**Project Data Summary Report**" and the email contains either a link to, or a .zip attachment named "**project080312.zip**". This file contains the file and link to the hosted file located at `hxxp://www[dot]Telebeam[dot]com/private/project080312[dot]zip`.

Contained within this ZIP file are two files:

080312.doc
data source.db

The file "data source.db" is a Microsoft Access Database that is designed to exploit a stack buffer overflow in the Microsoft Jet Engine. Details of the vulnerability can be found at <http://seclists.org/bugtraq/2007/Nov/0235.html>.

When the "080312.doc" file is opened, MS Word uses the Jet Engine to open the "data source.db" file. This triggers a stack buffer overflow in MS Word.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

This causes MS Word to disappear (crash) and then re-open, displaying the document contents. When MS Word crashes, the following processes occur:

- A file called SVCH0ST.EXE (note the zero instead of an "O") is written to c:\ and executed
- A file called WINWORD.EXE is created in the users's "Application Data" directory and executed
- A service called "Portable Media Serial Number Service" is installed, which is provided by c:\windows\system32\wmdmsvc32.dll

SVCH0ST.EXE and the extra WINWORD.EXE files are only temporary. The only remaining symptoms of a system that has been compromised is the presence of wmdmsvc32.dll. The details for the file are as follows:

wmdmsvc32.dll
MD5: 194593AC12B65C0D487F3F522D67B483
SHA1: 61C05DD2197FF4345AD67639061F89AD7C39958A

Note that there is a legitimate service called "Portable Media Serial Number Service" that is installed by some multimedia applications. However, the legitimate version of the service is provided by WmdmPmsn.exe, rather than wmdmsvc32.dll.

The malicious "Portable Media Serial Number Service," which is provided by wmdmsvc32.dll, appears to be a downloader to retrieve additional malware.

Recommendations (U//FOUO)

US-CERT recommends organizations block executable and unknown file types (.zip, .exe, .vbs) to mitigate risks against these types of attacks. More information about unsafe file types can be found at <http://support.microsoft.com/kb/925330>.

It's important to note that although this report details activity involving an attachment named "project080312.zip," the file name and type could easily change to trick new and unsuspecting users.

US-CERT also recommends that organizations remind users of the following pre-cautions when working with emails and attachments.

- Do NOT trust unsolicited email.
- Treat all email attachments with caution.
- Do NOT click links in unsolicited email messages.
- Turn off the option to automatically download attachments
- Employ the use of a spam filter.

To educate users about social engineering and phishing attacks, review US-CERT Cyber Security Tip ST04-014, "[Avoiding Social Engineering and Phishing Attacks](#)."



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

To educate users about handling malicious attachments, review US-CERT Cyber Security Tip ST04-010, "Using Caution with Email Attachments."

Report to US-CERT (U//FOUO)

Please report any validated incidents involving this activity to US-CERT for further correlation, analysis, and assistance.

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

WARNING: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of the US-CERT Operations Center at 1-888-282-0870. No portion of this report should be furnished to the media, either in written or verbal form.