

Virus Protection for SAP[®] E-Recruiting

A



White Paper

E-Recruiting – latest trend in HR

Today's enterprises save significant amounts of money by employing modern e-recruiting technology in Human Resource development.

Access to a talent-warehouse and the associated talent-pool helps enterprises addressing imminent but also future staffing requirements in a very effective way.

The Human Resources area benefited from the increased acceptance of the Internet. The ever decreasing number of Job ads in print media prove this fact.

Most of today's e-recruiting systems – not only those based on SAP's e-recruiting application – allow applicants to attach files to their online-application, such as photos, certificates etc. These files that are uploaded to the portal pose a serious threat to enterprise security.

Especially because of an ever increasing number of malware, even in popular office file-formats, and because traditional anti-virus technology is unable to inspect them, these uploads are to be considered unsafe.

In this scenario, potentially malicious content passes the enterprise boundary without being inspected and are saved into the SAP database. Every user, internal or external, accessing the files from the portal will receive potentially infected an unchecked content.

Infection-vector File Attachement

Since long, malware risks are no longer limited to executable sent by email anymore. Even file formats that used to be considered safe turn out to be successful infection vectors for malware, also because unsuspecting users anticipate no harm in opening these non-executable files.

For instance, while a few years ago, one was quite save, when only deactivating macros in Microsoft Word, the same behavior today is totally sufficient to infect the machine.



Security

Alert Raised for MS Word Zero-Day Attack

By Ryan Naraine
May 19, 2006

TALKBACK
Comment on this article
2 comments posted
Add your opinion



News

Report of 05.02.2007 13:49

Zero day vulnerability found in Excel

You are a guest
Login | Register

Adobe's Portable Document Format (PDF), often even used by government authorities and propagated as a save format for the exchange of data can host malware (eg "peachy virus")

Even the simple viewing of a picture, for example using the popular JPEG-format, may activate a malicious function if malware is embedded into the picture ("perrun" virus), if the security patch closing this security hole has not been applied to your system.

Security Publications	Alerts and Tips	Related Resources	About Us	Search US-CERT:
Information For	National Cyber Alert System			
Technical	Technical Cyber Security Alert TA04-260A			
Non-Technical	Microsoft Windows JPEG component buffer overflow			
Government				

<http://www.us-cert.gov/cas/techalerts/TA04-260A.html>

But other graphics file-formats, such as the Microsoft proprietary Windows Metafile Format (WMF) have also been used to spread malware in the past.

Vulnerability Notes Database	Vulnerability Note VU#181038
Search	Microsoft Windows Metafile handler SETABORTPROC GDI Escape vulnerability

<http://www.kb.cert.org/vuls/id/181038>

Virus protection for SAP-Portals

Built-in functionality of NetWeaver:

Since NetWeaver04 SPS9, SAP's application server platform contains an interface to secure uploads and downloads. This interface proprietary (NW-VSI) may be used to pass content to a virus scanner.

BowBridge AntiVirus Bridge:

The patent-pending AntiVirus Bridge technology developed by BowBridge allows fast and cost-efficient integration of existing, off-the-shelf antivirus products with SAP NetWeaver.

In most cases, enterprises already have licensed products that can be combined with the BowBridge adapter.

Having successfully passed the thorough certification process, SAP attests to the solution's interoperability with your e-recruiting application or any other ABAP or Java based application and ensures support from the overall solution

For further information, please visit:

<http://www.bowbridge.net/en/index.html>

or contact us via email: info@bowbridge.net

Test your SAP e-recruiting portal.

In the following, we will describe steps to verify whether your SAP e-recruiting portal is secured against malware uploads, using an imaginary ACMA corporation. The EICAR test-file is to be used to determine whether malware is detected. The EICAR test file is a 68-byte string detected by all virus scanners, although it poses no threat to any system. You may get the EICAR test file from <http://www.eicar.org>



BowBridge denies any liability from running these tests. They are performed to your sole responsibility.

Choose a Job posting on your portal:

Search for Jobs

Are you looking for an interesting new job?

We are constantly looking for talented and motivated new employees who can contribute to the success of our company. Take a look at our vacancies now!

Full Text Search

Search for

Search Method

Search Criteria for Employment Opportunities

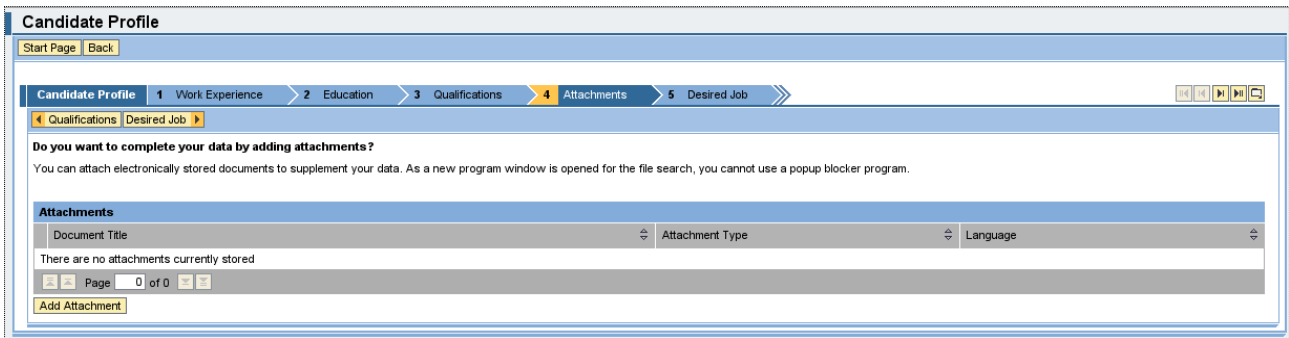
Functional Area
Business Area
Country
Branch

General Search Settings

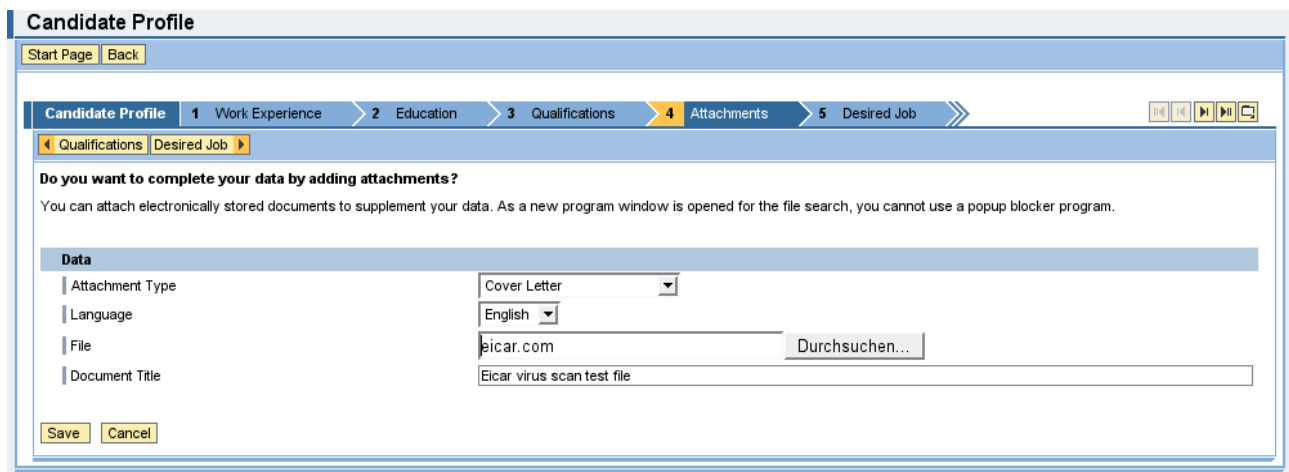
and apply to it to open the Application Wizard.

Depending on your system's configuration, you may have to register and provide personal information in the Application Wizard.

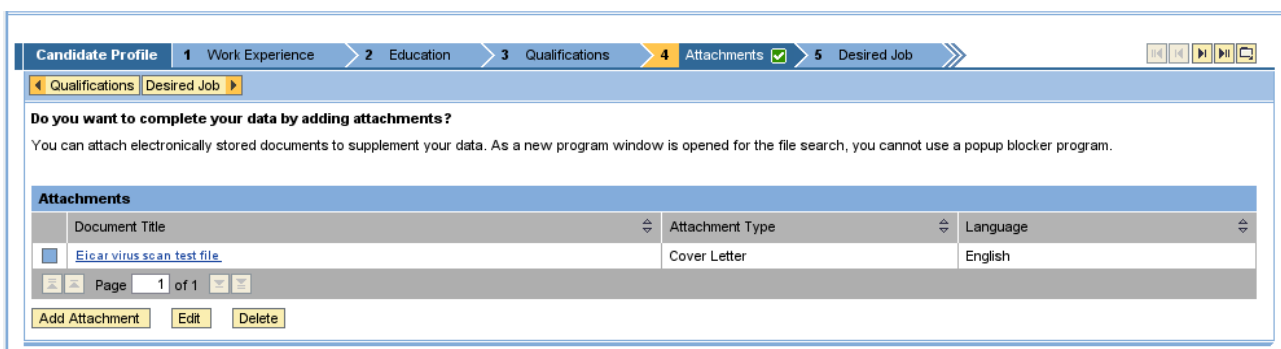
When asked to provide personal and professional data in the wizard, scroll to the right until the tab “Attachments” appears.



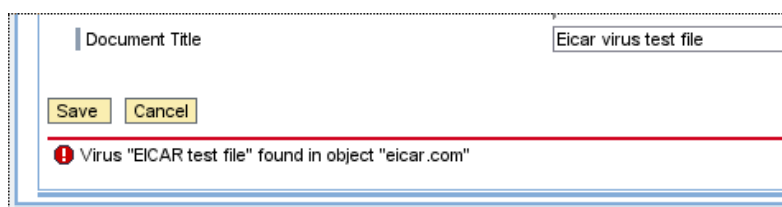
Add an attachment and specify the EICAR file. You may have to rename the EICAR file to something like “EICAR.DOC” if your portal enforces file types. Then click on “Save”.



If you succeed in uploading EICAR and you get a result similar to this, your portal is NOT PROTECTED against malicious uploads.



If virus protection is implemented and active, the upload fails and you will be displayed a message indicating it such as:





Copyright 2007, BowBridge Software Limited, Altrottstr. 31, 69190 Walldorf, Germany

SAP and NetWeaver are registered trademarks of SAP AG.

All other trademarks, even if not marked specifically, are the sole property of their respective owners