Mail2000
Social Engineering Scanner
Release Notes

網擎資訊軟體股份有限公司 謹呈

Openfind Information Technology, Inc.

目錄

What's New

Mail2000 Social Engineering Scanner（以下簡稱 SES）是專門針對 Mail2000 V4.0 以上的版本所設計的社交工程安全掃描工具，可以協助 Mail2000 的管理者對郵件系統進行安全掃描，針對不正常的系統檔案提出警示，並能統一調整全系統內使用者的相關郵件閱讀安全設定(如使用者的信件閱讀安全設定、密碼複雜度設定)，以主動防護的積極態度，協助組織的使用者遠離社交工程的威脅，預防系統發生相關的郵件安全性問題。

管理者可使用 SES 工具，進行以下的功能：

- 進行全系統檔案的安全掃描
  (可防止系統遭受竄改或者洩密攻擊)
  - 將掃瞄 Mail2000 系統的全部檔案，將不屬於系統本身，或者系統檔案內容遭到竄改、有資訊安全威脅的檔案，作移除動作 (會保留備份)。
- 統一更新系統及所有網域的密碼原則設定 (僅支援 v4.5SP2 以上的 Mail2000 版本)
  (可防範帳號、密碼過於簡單，導致使用者帳號被盜用)
  - 密碼最小長度：至少大於 6 個字元
  - 密碼複雜性限制：勾選 英文字元 及 數字字元
- 統一調整系統預設「使用環境」設定值和全系統使用者「使用環境」設定
  (可防範使用者在一開啟信件時，便直接遭遇到社交工程攻擊)
  - 個人設定 > 使用環境 > 進階功能設定 > 將刪信返回設定為信件列表
  - 個人設定 > 使用環境 > 進階功能設定 > 其他讀信設定– 去除 JavaScript
- 新增系統安全性功能
  (可警示使用者定期檢視自己的「自動轉寄」名單，避免機密信件外洩)
  - 使用者設定自動轉寄時，系統會寫 log (/webmail/log/account.log)
  - 信箱資訊頁面新增「轉寄資訊」區塊 (僅支援 v4.5SP3 以上的 Mail2000 版本)
  - 讓全系統使用者皆在信箱資訊頁面加入「轉寄資訊」區塊 (僅支援 v4.5SP3 以上的 Mail2000 版本)

System Requirement

- 支援版本：
  一台正常運行中的 Mail2000 V4.0 或 Mail2000 V4.5 以上的標準版，若有其他客製版本的使用需求，請洽 Openfind 技術人員。

- 硬碟空間：
  請檢視您安裝 Mail2000 系統目錄(預設為 /webmail)的 Partition，確認至少有 **50MB** 以上的磁碟空間。

- 作業系統：
  FreeBSD 5.x、FreeBSD 6.x
  - m2kV45ss_MLP_FreeBSD.090806.tgz
  - m2kV45ms_MLP_FreeBSD.090806.tgz

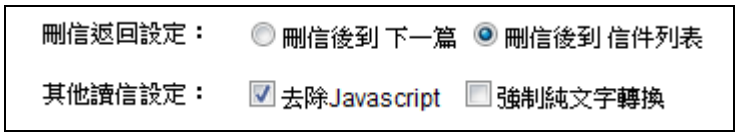
  Red Hat Enterprise AS/ES/WS5、CentOS 5
  - m2kV45ss_MLP_Linux.090806.tgz
  - m2kV45ms_MLP_Linux.090806.tgz

  Solaris 8、9、10 for Sparc
  - m2kV45ss_MLP_Solaris.090806.tgz
  - m2kV45ms_MLP_Solaris.090806.tgz

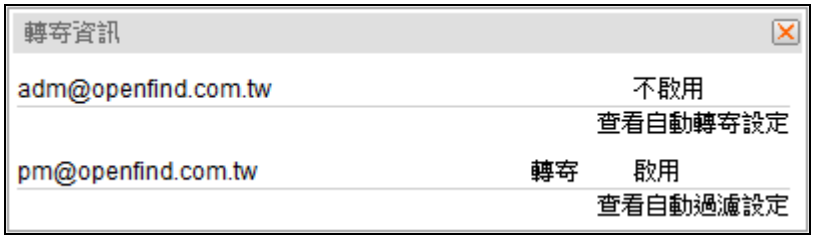
New Graphic Interface

■ A. 管理者介面：帳號管理 > 密碼原則設定

■ B. 使用者介面：個人設定 > 個人化設定 > 使用環境 > 進階功能設定



■ C. 使用者介面：登入資訊頁



Installation

- 以下安裝以 Mail2000 Multi Domain Single Server 版本，Linux 系統為例說明，其他版本除相關檔案名稱和目錄不同外，其餘流程相同。
- 請先取得由 Openfind 所提供的社交工程掃描工具（SES, Social Engineering Scanner ） 安裝套件：m2kpatch_ses.101111.tgz
- 安裝時，請將 SES 的 tgz 檔複製至 /home/webmail/ 目錄中，或其他位於系統的目錄中，在此以 /home/webmail 目錄為範例，複製完成後需確認 tgz 檔的 owner 及 group 權限皆為 webmail，用 tar 指令解開後，再執行安裝程序。

(1) 切換到 webmail 帳號：

```
# su webmail
```

(2) 確認 owner 及 group 皆為 webmail：

```
# cd /home/webmail
# ls -l ./m2kpatch_ses.101111.tgz
 -rw-r--r-- 1 webmail webmail 6264322 11??12 16:28 ./m2kpatch_ses.101111.tgz
```

(3) 解開檔案內容：

```
# /bin/tar vxzpf m2kpatch_ses.101111.tgz
```

(4) 切換至解壓縮的目錄，開始進行安裝：

```
# cd /home/webmail/m2kpatch_ses
# ./ses_scanner_main.pl
```

(5) 開始執行掃描程式：

```
Mail2000 Social Engineering Scanner v1.1
Copyright (C) Openfind Information Technology INC.

Installed system version: m2kv45 linux build6296173950
In order to increase system security, this process will scan and remove useless files in the system.
Please confirm the following questions before starting this process:

Do you want to backup these useless files before removing them? (Y/n)
請問您刪除前是否需要備份這些無用檔案？(Y/n)
Do you want to keep the scan log? (Y/n)
請問您是否需要保留掃描記錄檔？(Y/n)
```

Do you want to change the system default security value as below?
請問是否要將系統預設值變更為以下的安全設定建議值？

1) Minimum Password Length: 6 characters (only V45SP2+) (Y/n)
   密碼最小長度：6 個字元 (需為 v45 SP2 以上) (Y/n)
2) Password Rule: English Characters and Digital Characters (only V45SP2+) (Y/n)
   密碼複雜性限制：英文字元 及 數字字元 (需為 v45 SP2 以上) (Y/n)
3) Set "Display mail list after delete" as default value in "Preferences > Configuration > Advanced Settings". (Y/n)
   將個人設定>使用環境>進階功能設定中的「刪信返回」，預設為返回信件列表 (Y/n)
4) Set "Remove JavaScript while reading mail" as default value in "Preferences > Configuration > Advanced Settings" (Y/n)
   將個人設定>使用環境>進階功能設定中的「其他讀信設定」，預設為啟用去除 JavaScript (Y/n)

Do you want to set "Display mail list after delete" for all system users in "Preferences > Configuration" ? (Y/n)
請問您是否要將現有全系統使用者，個人設定>使用環境中的「刪信返回」設定變更為返回信件列表？ (Y/n)

Do you want to enable the setting of "Remove JavaScript while reading mail" for all system users in "Preferences > Configuration" ? (Y/n)
請問您是否要將現有全系統使用者，個人設定>使用環境中的「其他讀信設定」的「去除 Java Script」項目啟用？ (Y/n)

Do you want to add a "forward list" info on the page of "Mailbox info" ? (Y/n)
請問您是否要新增「轉寄資訊」到信箱資訊頁面？(Y/n)

* Backup useless files before remove: yes
* Keep scan log: yes

* Modify system default value: "Minimum Password Length": yes
* Modify system default value: "Password Rule :English Characters and Digital Characters": yes
* Modify system default value: "Display mail list after delete": yes

* Modify system default value: "Remove JavaScript while reading mail": yes

* Modify user setting: "Display after delete": yes
* Modify user setting: "Remove JavaScript while reading mail": yes

* Do you want to add a "forward list" info on "Mailbox info" page of all system users ?yes

Are you sure to start the process and remove these useless files permanently? (y/n)
請問您是否確定開始執行此程式，並移除這些無用的系統檔案？
[INFO] Mail2000 System V4.5 detected: m2kv45 linux build6296173950
[INFO] [SES_SCANNER]: scanner: scanner/m2k_ses_scanner_linux
[INFO] [SES_SCANNER]: output to /webmail/backup/ses_scanner/ses_scanner_log.101114_1316.log
[INFO] [SES_SCANNER]: backup files to /webmail/backup/ses_scanner/backup.101114_1316
[INFO] [PASSWD_POLICY]: TODO> minlen: 1
[INFO] [PASSWD_POLICY]: TODO> charset: 1
[INFO] [PASSWD_POLICY]: checking /webmail/etc/passwd_policy.conf
[INFO] [PASSWD_POLICY]: ==> modify min_len: 4 => 6.
[INFO] [PASSWD_POLICY]: ==> modify char_set_alpha: 0 => 1
[INFO] [PASSWD_POLICY]: ==> modify char_set_number: 0 => 1
[INFO] [PASSWD_POLICY]: /webmail/usr/C/pm.oec.openfind.com.tw/passwd_policy.conf does not exist.
[INFO] [UPDATE_DEF_PREF]: TODO> delback: 1
[INFO] [UPDATE_DEF_PREF]: TODO> rmjs: 1
[INFO] [UPDATE_DEF_PREF]: rmjs: 1 => 1
[INFO] [UPDATE_DEF_PREF]: delback: 0 => 1
[INFO] [UPDATE_DEF_PREF]: reload ini shared memory.
[INFO] [UPDATE_USER_PREF]: TODO> change_delback: 1
[INFO] [UPDATE_USER_PREF]: TODO> change_rmjs: 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/0/4B/user04
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/2/C5/user01
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/3/47/user02

```
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/3/C9/user03
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/7/14/icy_jan
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/C/B2/kappa
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/E/19/kappa-lin
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [UPDATE_USER_PREF]: SUB: process: /webmail/usr/C/pm.oec.openfind.com.tw/F/D0/admin
[INFO] [UPDATE_USER_PREF]: SUB: --> DelBack: 0 => 1
[INFO] [PATCH] apply patch for Mail2000 V4.5
[INFO] [CHECK_SP3]: current=1248278400, v45sp3=1217260800, ret=1
[INFO] [PATCH] system type: m2kv45sp3+
[INFO] [PATCH] apply patch for Mail2000 V4.5
[INFO] [PATCH] apply patch: /home/webmail/m2kpatch_ses/patch_v45sp3/m2kpatchV45ms_Linux.101108.tgz
[INFO] [PATCH] extract into tmp-dir: /home/webmail/m2kpatch_ses/extra_patch_v45.tmp.13448
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/etc/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/message/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/m2kpatch.pl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/do_backup.pl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/check_daemons.pl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/merge_conf.pl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/oml_var.tmpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/m2kpkg.lst
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/patch_backup.lst
```

```
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/message/s_cht/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/message/s_cht/portal_addpanel.msg
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/message/s_cht/portal_panel.msg
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/message/s_cht/portal_forward_xml.msg
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/standard/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/simple/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/simple/portal_panel.tpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/simple/portal_addpanel.tpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/simple/portal_forward_xml.tpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/simple/default.oml
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/standard/portal.tpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/standard/portal_forward_xml.tpl
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/template/standard/default.oml
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/etc/def_portal
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/cgi-bin/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/j45/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/chs/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/cht/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/en/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/en/portal.xml
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/en/j45/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/en/j45/msgtw.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/en/j45/submenu.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/cht/portal.xml
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/cht/j45/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/cht/j45/msgtw.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/cht/j45/submenu.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/chs/portal.xml
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/chs/j45/
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/chs/j45/msgtw.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/chs/j45/submenu.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/data/j45/PortalModule.js
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/cgi-bin/auto_forward
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/cgi-bin/portal
```

```
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/cgi-bin/portal_modules
[INFO] [PATCH] extract> m2kpatchV45ms_Linux/httpd/cgi-bin/naportal
[INFO] [PATCH] patch tarball extracted.
[INFO] [PATCH] patch installer processed.
[INFO] [PATCH] inst> Mail2000 patch program v1.2
[INFO] [PATCH] inst> Checking Permissions...done.
[INFO] [PATCH] inst> Checking User/Group...done.
[INFO] [PATCH] inst> Checking patch info file...done.
[INFO] [PATCH] inst> ================================================
[INFO] [PATCH] inst> Patch for Mail2000 v4.5 (1011080954)
[INFO] [PATCH] inst> ================================================
[INFO] [PATCH] inst> Making backup...
[INFO] [PATCH] inst> backup dir: /webmail/backup
[INFO] [PATCH] inst> backup file: /webmail/backup/m2kpatchV45_1011080954.bak.tar.gz (17 files)
[INFO] [PATCH] inst> updating config files...
[INFO] [PATCH] inst> Copying files...
[INFO] [PATCH] inst> ====================================
[INFO] [PATCH] inst> patch successful.
[INFO] [PATCH] inst> ====================================
[INFO] [PATCH] patch installed.
[INFO] [PATCH] clean-up: /home/webmail/m2kpatch_ses/extra_patch_v45.tmp.13448
[INFO] [CHECK_SP3]: current=1248278400, v45sp3=1217260800, ret=1
[INFO] [UPDATE_USER_PORTAL]: TODO> change_portal: 1
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/0/4B/user04: no portal config-file, skipped.
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/2/C5/user01: no portal config-file, skipped.
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/3/47/user02: no portal config-file, skipped.
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/3/C9/user03: no portal config-file, skipped.
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/7/14/icy_jan
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/C/B2/kappa: no portal config-file, skipped.
```

```
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/E/19/kappa-lin: no portal config-file, skipped.
[INFO] [UPDATE_USER_PORTAL]: SUB: process:
/webmail/usr/C/pm.oec.openfind.com.tw/F/D0/admin
[INFO] [JS_VER] change js_ver in oml_var.
[INFO] [JS_VER]: change js_ver from 090901 to 101114

Scan completed, scan logs and backup files were located in /webmail/backup/ses_scanner.
```

- 本掃描工具備份檔案備份目錄為/webmail/backup/ses_scanner/，所有刪除的檔案將會依照原目錄結構備份於此，若有後續還原的需求，可直接進行還原。

Patch File List

- 本工具將會更新 Mail2000 系統中，以下所表列的檔案，若您所使用的版本有客製化，或者變更過這些檔案，請洽詢 Openfind 原廠技術人員確認更換細節。

  - Mail2000 v40：
    cgi-bin/auto_forward

  - Mail2000 v45：
    cgi-bin/auto_forward

  - Mail2000 v45SP3：
    httpd/cgi-bin/auto_forward
    etc/def_portal
    httpd/cgi-bin/portal
    httpd/cgi-bin/portal_modules
    httpd/cgi-bin/naportal
    httpd/data/j45/PortalModule.js
    httpd/data/chs/portal.xml
    httpd/data/cht/portal.xml
    httpd/data/en/portal.xml
    httpd/data/chs/j45/msgtw.js
    httpd/data/chs/j45/submenu.js
    httpd/data/cht/j45/msgtw.js
    httpd/data/cht/j45/submenu.js
    httpd/data/en/j45/msgtw.js
    httpd/data/en/j45/submenu.js
    template/standard/portal.tpl
    template/standard/portal_forward_xml.tpl
    template/simple/portal_panel.tpl
    template/simple/portal_addpanel.tpl
    template/simple/portal_forward_xml.tpl
    message/s_cht/portal_addpanel.msg
    message/s_cht/portal_panel.msg
    message/s_cht/portal_forward_xml.msg
    template/standard/default.oml
    template/simple/default.oml