ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

بدافزار TROJ_WALEDAC.AIR

تنظیم کننده:

سمانه غنی- سعیده نکوخیز

ویرایش: ۱

شماره سند: V-89/5-6

www.ircert.cc

ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: V-89/56

نام محصول آسیب پذیر: TROJ_WALEDAC.AIR

نوع سیستم عامل: Windows 98, ME, NT, 2000, XP, Server 2003

کشف توسط: شرکت Trend micro

تاریخ کشف: 1 Aug 2010

سطح خطر: متوسط

شرح:

این تروجان با استفاده از روش های مهندسی اجتماعی ممکن است کاربران را با انجام اقدامات خاص به طور مستقیم یا غیر مستقیم فریب دهد و باعث ایجاد روال مخرب گردد.

این تروجان از طریق پیام هایی به صندوق هرزنامه به صورت فایل پیوست توسط برنامه های مخرب یا کاربر مخرب دریافت می گردد. این تروجان به وب سایت های خاص متصل می گردد و دیگر فایل های مخرب شناسایی شده توسط ترندماکرو را مطابق زیر دریافت می کند:

- http://{BLOCKED}.74.161/mrmun_sgjlgdsjrthrtwg.exe - detected as TROJ_FAKEAV.ZZS
- http://{BLOCKED}.191.111/bat.exe- detected as TROJ_BREDOLAB.WV

ذخیره فایل های دریافت شده بر روی سیستم کامپیوتر اثر می گذارد و سپس فایل های دریافت شده در سیستم اجرا می گردد. در نتیجه روال فایل های دریافت شده بر روی سیستم آسیب دیده به نمایش گذاشته می شود. فایل های دریافت شده مطابق زیر می باشد:

- %\Application Data%\{Random File Name}.exe
- %Temp%_ex-08.exe

حجم: ۲۶,۶۲۴ بایت

نحوه رفع مشکل:

کاربران Windows ME و Windows XP می بایست قبل از انجام هر عمل اسکن اطمینان حاصل کنند که برنامه System Restore در کامپیوتر شان غیرفعال است و اجازه اسکن تمام قسمت های کامپیوتر را بـه آنها می دهد.

کامپیوتر خود را با برنامه های ضد بدافزار شرکت ترندمایکرو اسکن نمایید و فایل های مخرب شناسایی شده مطابق زیر را از سیستم کامپیوتر خود حذف نمایید:

- TROJ_WALEDAC.AIR
- TROJ_FAKEAV.ZZS
- TROJ_BREDOLAB.WV

مرکز آپای دانشگاه شیراز

منابع:

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FWALEDAC%2EAIR&VSect=P

http://www.safebyte.ro/component/option,com_newsfeeds/task,view/catid,15/Itemid,49/

http://www.spyremover.optimized-webs.com/spywaredatabase.php

مرکز آپای دانشگاه شیراز