ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

بدفزار TSPY_SKIMER.A

تنظیم کننده:

سمانه غنی- سعیده نکوخیز

ویرایش: ۱

شماره سند: V-89/5-7

www.ircert.cc

ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: V-89/57

نام محصول آسیب پذیر: TSPY_SKIMER.A

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

کشف توسط: شرکت Trendmicro

تاریخ کشف: Jun 10 2009

سطح خطر: کم

شرح:

بدافزار چندین فایل مخرب را وارد دستگاه می کند. این جاسوس افزار برای سرقت اطلاعات طراحی شده است و از فرآیند تجزیه داده های خاصی به عنوان علامتی برای نمایش رابط گرافیکی خود استفاده می کند. این رابط گرافیکی به کاربر مخرب کمک می کند که ۱۰ فرمان را با وارد کردن شماره بر روی صفحه کلید دستگاه خودپرداز اجراکند.

در شکل زیر می توانید دیدگاه جامعی از رفتار این جاسوس افزار را مشاهده نمایید.

این جاسوس افزار فایل زیر را اضافه می کند:

Windows%\lsass.exe

%Windows% در واقع پوشه ویندوز است که معمولا در مسیر C:\Windows یا C:\WINNT قرار دارد.

سپس فایل های زیر را کپی می کند:

Windows%\trl2%

Windows%\kl%

در صورتی که دستگاه خودپرداز از سیستم فایل NTFS استفاده کند جریان های داده زیر را ایجاد می کند:

Windows%\greenstone.bmp:redstone.bmp %

Windows%\greenstone.bmp:bluestone.bmp %

در غیر اینصورت فایل های زیر را ایجاد می کند:

Windows%\redstone.bmp %

Windows%\bluestone.bmp %

مرکز آپای دانشگاه شیراز

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 به آن ها می دهد.

مرحله اول: بازگرداندن فایل های پشتیبان

فقط فایل های مرتبط با ماکروسافت قابل بازگردانی می باشند. در صورتی که این جاسوس افزار باعث حذف فایل های مرتبط با برنامه هایی شده است که متعلق به ماکروسافت نمی باشند می بایست مجدداً این برنامه ها روی سیستم نصب کنید.

مرحله دوم: کامپیوتر خود را با برنامه های ضد بدافزار شرکت ترندماکرو اسکن نمایید و فایل های مخرب شناسایی شده به عنوان بدافزارTSPY_SKIMER.A را از سیستم کامپیوتر خود حذف نمایید.

مرحله سوم: راه اندازی مجدد سیستم و انتخاب حالت Safe Mode

*روش رفتن به حالت Safe Mode برای کاربران ویندوز ۹۸ و Windows ME

Restart your computer

Press the CTRL key until the startup menu appears

Choose the Safe Mode option then press Enter

* برای کاربران Windows NT (VGA mode)

Click Start>Settings>Control Panel

Double-click the System icon

Click the Startup/Shutdown tab

Set the Show List field to 10 seconds and click OK to save this change

Shut down and restart your computer

Select VGA mode from the startup menu

* برای کاربران Windows 2000

Restart your computer

Press the F8 key, when you see the Starting Windows bar at the bottom of the screen

Choose the Safe Mode option from the Windows Advanced Options Menu then press Enter

* برای کاربران Windows XP

Restart your computer

Press F8 after the Power-On Self Test (POST) is done. If the Windows Advanced Options Menu does not appear, try restarting and then pressing F8 several times after the POST screen

Choose the Safe Mode option from the Windows Advanced Options Menu then press Enter

* برای کاربران Windows Server 2003

مرکز آیای دانشگاه شیراز

Restart your computer

Press F8 after Windows starts up. If the Windows Advanced Options Menu does not appear, try restarting again and then pressing F8 several times after restarting

On the Windows Advanced Option menu, use the arrow keys to select Safe Mode, and then press Enter

مرحله چهارم: جستجو و حذف فایل های زیر

Windows%\bluestone.bmp %

Windows%\greenstone.bmp:bluestone.bmp %

Windows%\greenstone.bmp:redstone.bmp %

Windows%\redstone.bmp %

pwrstr.dll

مرحله پنجم: جستجو و حذف فایل های آشکار شده تحت عنوان TSPY_SKIMER.A

مرکز ایمنی دانشگاه شیراز

منابع:

http://threatinfo.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY%5FSKIMER%2EA

http://www.snpx.com/securitynews2009/index.php?section=Trend_Micro_Antivirus

http://www.networks-by-design.com/New_Hyde_Park-Nassau_County-NY-Virus_Spyware_Adware_Removal.htm

مرکز آپای دانشگاه شیراز