ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

کرم P2P.Palevo.FP

تنظیم کننده:

سعیده نکوخیز - سمانه غنی

ویرایش: ۱

شماره سند: V-89/5-3

www.ircert.cc

ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری:V-89/5-3

نام محصول آسیب پذیر: Worm.P2P.Palevo.FP

نوع سیستم عامل: سیستم عامل ویندوز

کشف توسط: BitDefender

تاریخ کشف: 9 Jul 2010

سطح خطر: متوسط

شرح:

این بدافزار از طریق ارسال پیام های فوری هرز به مخاطبان گسترش می یابد.

این برنامه مخرب کپی هایی از خودش را در پوشه های سیستم عامل با نام jusched.exe ایجاد می کند که شبیه یک فایل زبان برنامه نویسی شناخته می شود. به منظور اجرای خود در هر زمان که سیستم عامل راه اندازی می شود مقادیر زیر در رجیستری ویندوز اضافه می شود:

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run with "Java developer Script Browse" which contains the path of the Trojan "%Windir%\jusched.exe"

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install Software\Microsoft\Windows\CurrentVersion\Run : "Java developer Script Browse" with the value "%Windir%\jusched.exe"

C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run : "Java developer Script Browse" with the value "%Windir%\jusched.exe"

Worm.P2P.Palevo.FP بوسیله افزودن مقادیر زیر در رجیستری خود را به عنوان یک برنامه کاربردی مجاز برای دیواره آتش سیستم اضافه می کند.

keyHKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

این بدافزار خدمات بروز رسانی ویندوز را متوقف می کند، و از انجام بروز رسانی لازم توسط کاربر جلوگیری می کند. همچنین تلاش می کند msmpsvc.exe را متوقف کند که یک سرویس حفاظت از بدافزار هاست که متعلق به شرکت مایکروسافت می باشد.

این کرم قادر به ارسال پیام ها به مخاطبان در برنامه های کاربردی ارسال پیام فوری مانند Skype، Yahoo Messenger و AIM(AOL Instant Messenger) می باشد.

علائم:

پیام های ناخواسته در برنامه های پیام رسانی فوری که به صورت زیر است. (تصویر زیر)

"foto :D [shortend_url]"

[redacted]: foto http://ow.ly/28pw7?=http://www.facebook.com/photo.php

shortend_url حاوی یک کرم است که نمادی شبیه به یک تصویر دارد تا بتواند کاربر را از طریق این تصویر که در واقع حاوی بدافزار است فریب دهد. در صورتی که کاربر این فایل را اجرا کند، یک پنجره مرورگر ظاهر خواهد شد، به دنبال آن پنجره جدیدی که حاوی لیستی از تماس هایی از وب سایت شبکه اجتماعی است ظاهر می شود. سپس این کرم خودش را بوسیله تغییر خصوصیات فایل پنهان می کند.

سیستم عامل تحت تاثیر قرار گرفته: سیستم عامل ویندوز

نام های مستعار:

Worm.Win32.Pushbot

W32.Yimfoca

حجم: ۷۰ کیلوبایت

نحوه رفع مشکل:

همواره نرم افزار ضد ویروس، سیستم کامپیوتر خود را بروز رسانی نمایید و سیستم خود را با نرم افزار های ضد ویروس به روز رسانی شده اسکن نمایید.

مرکز آپای دانشگاه شیراز

منابع:

http://www.bitdefender.com/VIRUS-1000624-en--Worm.P2P.Palevo.FP.html

http://www.malwarecity.com/site/Main/virusEnciclopedia

مرکز آپای دانشگاه شیراز