امنیت اطلاعات

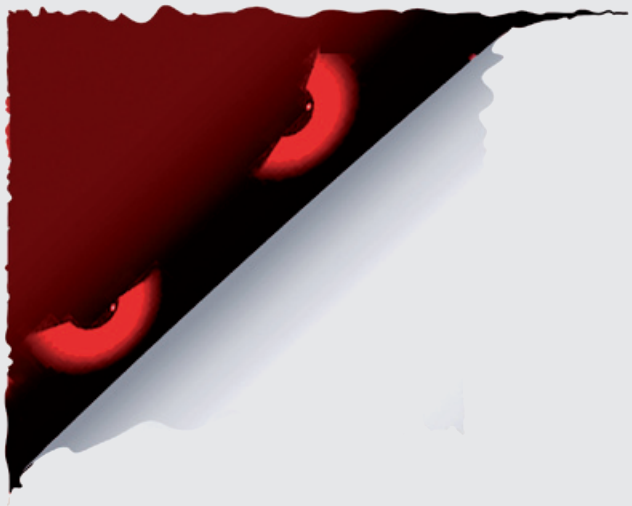
بولتن تحلیلی ■ شماره ششم ■ پاییز ۱۳۹۳

شرکت نرم افزاری
امن پرداز

به بهانه رسیدن پاییز...

برگ‌های پاییزی
سرشار از شعورِ درخت اند
و خاطراتِ سه فصل را بر دوش می کشند
آرام قدم بگذار ....
بر چهره‌ی تکیده‌ی آن ها
این برگ‌ها حُرمت دارند...
دردِ پاییز، دردِ " دانستن " است

در این شماره خواهید خواند:
نکورس، بدافزاری زیرک در پنهان سازی
مراقب باج‌گیر اینترنتی Cryptowall باشید!
آزمون نفوذپذیری- به خطر انداختن سیستم و افزایش حق دسترسی، بخش ششم
پیغام جعلی مبنی بر شناسایی شدن ویروس DSVX در اکانت ایمیل یاهو
سرقت ۸۳ هزار دلار از mining poolهای Bitcoin
خطای Blue Screen of Death به دلیل به روزرسانی ماه آگوست شرکت مایکروسافت
تبلیغات اجباری از طریق یک بدافزار!



نکورس، بدافزاری زیرک در پنهان سازی

بدافزار نکورس درحالت‌های متفاوتی مثل دانلودر، دراپر و روت‌کیت ظاهر می‌شود، ومی‌توان ماژول روت‌کیت آن را قوی‌ترین و کاربردی‌ترین بخش از خانواده نکورس نامید. روت‌کیت نکورس با فراهم آوردن گزینه‌های متفاوت توانسته است خود را به عنوان ابزاری کارآمد در پنهان سازی ماژول‌های بدافزاری و جلوگیری از اجرای ابزارهای امنیتی مطرح کند. علاوه بر این به دلیل استفاده از تکنیک‌های بقا و پنهان سازی قوی، نکورس در دسته‌ی بدافزارهای دشوار برای پاکسازی قرار می‌گیرد.

شروع کار در این بدافزار با اجرای ماژول دانلودر همراه است. این ماژول در آغاز، فایل درایور خود را با نامی تصادفی ایجاد کرده و آن را اجرا می‌کند. سپس در صورتی که بتواند به سرورهای خود متصل شود اقدام به دانلود فایل‌های جدیدتر و اجرای آن‌ها در سیستم قربانی می‌کند.

بعد از اجرای ماژول دانلودر ادامه‌ی روند از ماژول دراپر آغاز می‌شود. این ماژول نقش یک سرویس با نام "syshost32" را ایفا می‌کند که در دو حالت اجرایی متفاوت قابل اجرا می‌باشد.

حالت ابتدایی آن وقتی است که سرویس در سیستم قربانی راه اندازی نشده است ولی فایل آن در یکی از دو مسیر %APPDATA% و یا %Windir%\Installer موجود است. در این صورت دایرکتوری‌ای با نام تصادفی در این مسیر ساخته شده و فایل مورد نظر با نام syshost.exe در یکی از دو مسیر گفته شده کپی و با ورودی "Service\" راه اندازی می‌شود.

در انتها نیز برای بقای سرویس راه اندازی شده، مطابق روش معمول نام سرویس یعنی "syshost32" در مسیر Run رجیستری قرار می‌گیرد.

در مرحله‌ی دوم سرویس به درستی راه اندازی شده است. برنامه تکه کدی کوتاه را در کلیه‌ی پردازه‌های سیستمی تزریق می‌کند. این کد فراخوانی به آدرسی با محتوای 0x00 است اجرای آن در بسیاری از پردازه‌ها باعث بروز خطا، کرش کردن و راه اندازی مجدد سیستم می‌شود.

درایور ایجاد شده که نقش روت‌کیت بدافزار را بر عهده دارد، دارای فرمتی رمز شده است. این فایل به صورت ماژولی مستقل دارای توانایی‌های بسیار متنوع و بالایی است که آن را به کاندیدی مناسب برای استفاده در بسیاری از بدافزاها و حتی برنامه‌های سالم تبدیل می‌کند.

یکی از تکنیک‌های به کار رفته، قراردادن درایور در لیست ابتدایی‌ترین سرویس‌های Load شده در سیستم است. این کار با استفاده از رجیستر کردن درایور در صدر فهرست سرویس‌های گروه Boot Bus Extender صورت می‌پذیرد. با استفاده از این تکنیک سرویس روت‌کیت نکورس حتی قبل از سرویس‌های آنتی ویروس‌ها Load خواهد شد. بنابراین به راحتی می‌تواند اجرا شدن آنها را تحت کنترل خود درآورد. از دیگر تکنیک‌های استفاده شده در این روت‌کیت می‌توان به موارد زیر اشاره کرد.

۱. جلوگیری از دسترسی پردازه‌ها و نخ‌های دیگر برنامه‌ها به سرویس روت‌کیت و کلیه‌ی پردازه‌های تحت پشتیبانی آن در سیستم، شامل ماژول‌های دیگر بدافزار. (SSDT Hooks)

۲. جلوگیری از دسترسی پردازه‌ها و نخ‌های دیگر برنامه‌ها به رجیستری مربوط به سرویس روت‌کیت در سیستم. (Registry Notify Routine)

۳. جلوگیری از دسترسی پردازه‌ها و نخ‌های دیگر برنامه‌ها به فایل مربوط به روت‌کیت به صورت فیزیکی. (FS Filter Driver)

۴. جلوگیری از Load شدن سرویس‌ها و پردازه‌های قرار گرفته در لیست سیاه روت‌کیت. (Load Image Notify Routine)

همان طور که مشاهده شد تکنیک‌ها شامل جلوگیری از اجرای برخی سرویس‌ها در سیستم و اجازه به دیگر سرویس‌ها برای اجرا است. برای انجام این کار روت‌کیت لیستی مخصوص از پردازه‌های سفید (دارای اجازه‌ی اجرا در سیستم) را تهیه و ذخیره می‌کند. این کار با ساخت و مقداردهی دو پارامتر به نام‌های DB0، DB2 در کلید رجیستری درایور صورت می‌گیرد. محتوای این دو پارامتر دو نوع Hash از سرویس‌ها و پردازه‌های سفید در سیستم است. در زمان تهیه‌ی Hashها با روشی هوشمندانه فایل‌ها و سرویس‌های مربوط به پردازه‌های امنیتی تشخیص داده شده و از آن‌ها Hash گرفته نمی‌شود. در ادامه نمونه‌ای از ده پردازه‌ی قرار گرفته در لیست ۱۳۵ تایی پردازه‌های لیست سیاه بدافزار را مشاهده می‌کنید.

1."eeCtrl.sys"	2."eraser.sys"
3."SRTSP.sys"	4."SRTSPIT.sys"
5."SRTSP64.SYS"	6."a2gffx86.sys"
7."a2gffx64.sys"	8."a2gffi64.sys"
9."a2acc.sys"	10."a2acc64.sys"

روت‌کیت نکورس قابلیت‌های زیادی برای پاسخگویی به درخواست‌های پردازه‌های خود دارد. علاوه بر این نکورس مشخصه‌ی پردازه‌ها و نخ‌های مربوط به بدافزار را در خود نگه داری کرده و این توانایی را دارد که هر تعداد پردازه و نخ را که در حین اجرا به این دسته اضافه شود به لیست اشاره شده بیافزاید. استفاده‌ای که از این لیست می‌شود در هنگام درخواست‌های دسترسی به منابع بدافزار است. به این صورت که شناسه‌ی پردازه و یا نخ درخواست کننده با لیست اشاره شده مقایسه شده و تنها در صورت توافق و موجود بودن در لیست به آن اجازه‌ی دسترسی به منابع داده می‌شود.

روت‌کیت‌ها و ضدروت‌کیت پادویش

روت‌کیت‌ها گونه‌ای از بدافزارها هستند که به منظور نفوذ پنهانی، سوء استفاده و در بعضی مواقع اختلال در سیستم طراحی شده اند. ویژگی بارز این نوع بدافزارها طرز عملکرد مخفیانه آنها می‌باشد که به شکلی کاملا نامحسوس کنترل سیستم آلوده را به دست گرفته و مقاصد خود را دنبال می‌کنند.

این گونه از بدافزارها در بسیاری از موارد کارکرد خود را با جعل عملکرد توابع سیستم عامل انجام داده و با مخفی‌سازی حضور خود در بخش‌های مختلف سیستم ازجمله فایل‌ها، کلیدهای رجیستری، پردازه‌ها و حافظه، به بقا ادامه خواهند داد. به علت قابلیت پنهان‌سازی قوی اینگونه برنامه‌ها، شناسایی آن‌ها یا برنامه‌هایی که توسط آنها پنهان گردیده اغلب مشکل بوده و این امر می‌تواند مشکلاتی را برای کاربران بوجود آورد.

یک روت‌کیت می تواند شامل جاسوس‌افزار و برنامه‌های مخرب دیگری مانند مانیتورینگ ترافیک شبکه یا KEYSTROKEها باشد. روت‌کیت‌ها با ایجاد درب پشتی بر روی سیستم برای استفاده هکرها، تغییر فایل‌های گزارش، حمله به ماشین‌های دیگر بر روی شبکه و تغییر ابزارهای موجود روی سیستم برای دور زدن شناسایی، موجب اختلال در سیستم می‌شوند.

راه‌اندازی روت‌کیت‌ها بصورت خودکار و یا از طریق مهاجم با کسب دسترسی ویژه صورت می‌گیرد. اخذ این دسترسی، نتیجه حمله مستقیم به سیستم (برای مثال سواستفاده از یک آسیب‌پذیری شناخته شده) و یا کسب کلمه عبور (برای مثال از طریق مهندسی اجتماعی) می باشد. با یک بار نصب روت‌کیت، پنهان‌سازی نفوذ و حفظ دسترسی ویژه امکان‌پذیر می شود. روت کیت‌ها با این دسترسی کنترل کامل بر روی سیستم خواهند داشت و این بدان معنی می‌باشد که روت کیت‌ها قابلیت تغییر نرم‌افزارهای موجود بر روی سیستم از جمله نرم‌افزارهای شناسایی و مقابله با بدافزارها را خواهند داشت. برای شناسایی روت‌کیت‌ها روش‌هایی از جمله استفاده از سیستم عامل‌های جایگزین و امن، روش‌های مبتنی بر رفتار، پویش امضا، تحلیل DUMP حافظه معرفی شده‌اند.

به دلیل قابلیت پنهان‌سازی و عملکرد این نوع از بدافزارها، شناسایی و پاکسازی کامل آنها توسط ضدویروس‌ها به تنهایی کافی نمی‌باشد؛ بدین منظور، از ابزار ضدروت‌کیت استفاده می‌شود.

گروه ضدویروس پادویش از شرکت نرم افزاری امن‌پرداز با توجه به اهمیت شناسایی و مقابله با روت کیت‌ها محصول ضدروت‌کیت خود را تولید و منتشر نموده است و به طور رایگان برای استفاده همگان در سایت پادویش قرار داده است. لازم به ذکر است که در حال حاضر ضدویروس پادویش قادر به شناسایی روت‌کیت‌ها می‌باشد، اما در مواردی که قبل از نصب آنتی ویروس سیستم آلوده به روت‌کیت شده باشد استفاده از ضدروت‌کیت لازم می‌شود. ضدروت‌کیت پادویش ابزاری است که علاوه بر شناسایی و پاکسازی روت‌کیت‌های شناخته شده، قابلیت شناسایی رفتارهای مشکوک سیستم شما را نیز خواهد داشت. با اجرای این برنامه، سیستم شما در مدت زمانی کوتاه پویش شده و در صورت یافتن روت‌کیت(ها) توسط این ابزار، به طور کامل پاکسازی خواهد شد.

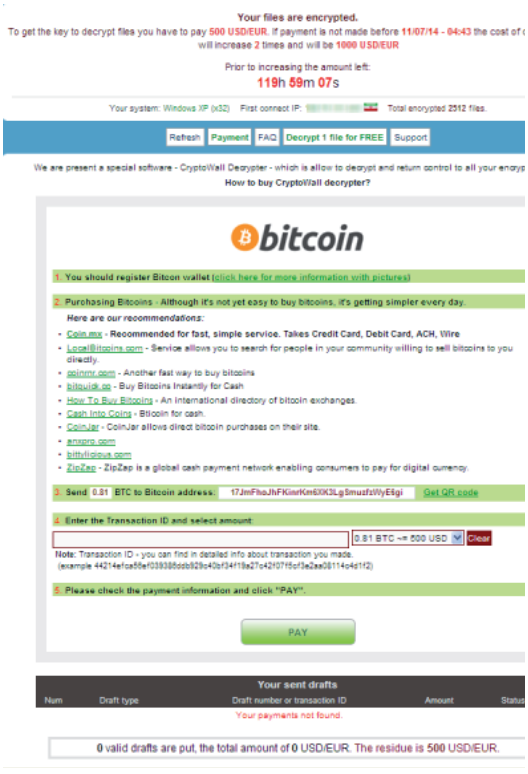
برای دانلود ضدروت‌کیت پادویش از لینک زیر استفاده کنید:

www.padvish.com/contents.php?cntid=107

مراقب باج‌گیر اینترنتی Cryptowall باشید!

تصور کنید یک روز کامپیوتر را روشن می‌کنید و دیگر نمی‌توانید فایل‌های مهم و مورد نیاز خود را ببینید. صفحه‌ای بالا آمده و از شما برای دیدن این اطلاعات پول درخواست می‌کند. شما احتمالا به یک Ransomware دچار شده‌اید.

Ransomwareها گونه ای از بدافزارها با نام باج‌گیر هستند که ابتدا فایل‌ها و پوشه‌ها در سیستم قربانی را رمزگذاری می‌کنند و از این راه وی نمی‌تواند اطلاعات خود را در دسترس داشته باشد. سپس با نمایش یک پیغام برای در اختیار گذاشتن فایل‌ها یا رمزگشایی آنها، از کاربر سیستم درخواست پول می‌کنند و از وی می‌خواهد در یک مهلت مقرر پول را پرداخت نماید و در غیر اینصورت فایل‌های او غیر قابل بازگشت خواهند بود. در این شرایط به احتمال قوی فرد قربانی راهی جز پرداخت پول برای بازگرداندن اطلاعات مهم خود را ندارد!



پس از Cryptolocker که توانست حدود ۲۵۰،۰۰۰ رایانه در جهان را آلوده کند وتقریبا یک میلیون دلار (حدود £۶۰۰،۰۰۰) به جیب بزند[1]، نوع جدیدی از بدافزارهای باج‌گیر یا Ransomware با نام Trojan.Win32.Cryptowall.B در حال شیوع می‌باشد که کاربران اینترنت می‌بایست از خطرات آنها آگاهی داشته باشند. عملکرد این بدافزار بسیار پیچیده می‌باشد وتاکنون هیچ راهی برای یافتن کلید رمزگشایی یا شکستن رمز آن کشف نشده است و قربانیان راهی به جز پرداخت پول ندارند.

عامل اصلی انتشار بدافزار Cryptowall ، یک بسته نفوذ (exploit kit) به نام RIG می باشد که با قرار گرفتن بر روی وب سایت ها، اقدام به آلوده کردن سیستم بازدید کنندگان می‌کند. این بسته در سیستم قربانی به دنباله نسخه‌های به‌روز نشده از نرم‌افزارهایی چون Java، Flash و multimedia می‌گردد و از حفره‌های امنیتی موجود در آنها به منظور نصب خود در سیستم استفاده می‌نماید. Cryptowall به منظور جلوگیری از ردیابی و شناسایی از bitcoin در تراکنش مالی خود استفاده می‌کند.

برای ایمنی از آسیب احتمالی این بدافزار نکات زیر را مورد توجه قرار دهید:

- اولین و مهمترین نکته تهیه نسخه پشتیبان از اطلاعات خود به طور منظم و دوره‌ای که در صورت آلوده شدن به هر گونه بدافزار باج‌گیر بتوانید به اطلاعات خود دسترسی داشته باشید.
- از به‌روز بودن تمامی برنامه‌های نصب شده بر روی سیستم خود، اطمینان حاصل کنید.
- مراقب آگهی‌های تبلیغاتی و نامه‌های الکترونیک مشکوک باشید و به طور کل هر درخواست کلیک را بدون اطمینان پاسخ ندهید.
- ضدویروس خود را به طور دائم به‌روز نگه دارید.
- از ابزارهای خاص مقابله با این این نوع بدافزارها مانند Padvish CryptoProtect استفاده نمایید.

برای دانلود ابزار Padvish CryptoProtect از لینک زیر اقدام نمایید:
www.padvish.com/contents.php?cntid=93

1. http://www.theinquirer.net/inquirer/news/2320452/cryptolocker-ransomware-has-infected-quarter-of-a-million-systems-since-september

آزمون نفوذپذیری

به خطر انداختن سیستم و افزایش حق دسترسی

بخش ششم

در زمانیکه فرد آزمون کننده‌ی آزمون نفوذ به یک سیستم از طریق کدهای مخرب[1] دسترسی پیدا می‌کند، ممکن است بتواند از آن به منظور جمع آوری اطلاعات حساسی، همچون اطلاعات مالی، نحوه‌ی پیکربندی اطلاعات، فایل‌های شخصی و یا اسناد سازمان‌ها استفاده نماید. اگر آزمون کننده بتواند به اینگونه اطلاعات حساس دسترسی پیدا نماید، می‌توان اینگونه در نظر گرفت که آزمون نفوذ با موفقیت انجام شده است. اما در آزمون نفوذ تنها یک مورد وجود دارد که می‌توان گفت که از دسترسی به اطلاعات حساس، بهتر و باارزشتر است و آن هم، بدست آوردن دسترسی ادمین در سیستم می‌باشد. این موضوع که یک کاربر نامعتبر بتواند دسترسی ادمین بر روی یک سرور مهم و حیاتی بدست آورد، کابوس ادمین‌های سیستم‌ها می‌باشد. بدین منظور جهت افزایش دسترسی، روش‌های متفاوتی وجود دارد که به شرح زیر است:

- اولین روش در افزایش حق دسترسی، جستجوی آسیب پذیری‌های بیشتر در سیستم می‌باشد. اگر آزمون کننده بتواند هرگونه دسترسی به سیستم پیدا نماید، حتی اگر دسترسی بسیار محدود باشد، ممکن است بتواند از آسیب پذیری‌هایی که فقط از طریق وارد شدن به حساب کاربری امکان پذیر است، سوء استفاده نماید. زیرا معمولا کنترل‌های داخلی ضعیف‌تر از کنترل‌های خارجی می‌باشد در نتیجه در صورت ایجاد دسترسی محدود به یک سیستم، امکان به خطر انداختن سیستم از داخل آن امکان پذیر می‌باشد.
- دومین روش، شنود شبکه به منظور دست یافتن به اطلاعات حساسی از جمله نام کاربری و رمز عبور می‌باشد. اگر آزمون کننده بتواند تمام ترافیک ورودی و خروجی سیستم هدف را استراق سمع نماید، دسترسی به اطلاعات حساس که به آزمون کننده اجازه دسترسی به سیستم با سطح دسترسی بالا را می‌دهد، امکان پذیر می‌شود.
- سومین و کارآمدترین روش، مهندسی اجتماعی می‌باشد. این روش نسبت به روش‌هایی همچون استفاده از اکسپلویت‌های گوناگون، سریعتر و راحت‌تر است. مهندسی اجتماعی شامل روش‌هایی همچون استفاده از فایل‌های ضمیمه شده پست‌های الکترونیکی و دسترسی فیزیکی به سرور و فیشینگ می‌باشد.

هدف از اجرای این فاز از تست نفوذ این نیست که آزمون کننده سیستم و یا شبکه هدف را دچار خطر نماید، بلکه هدف شناسایی نقاط قوت و ضعف آن‌ها و گزارش آن به کارفرما می‌باشد.

در این شماره، به روش‌های افزایش دسترسی و به خطر انداختن سیستم و یا شبکه هدف اشاره گردید. در شماره‌های پیش رو به بررسی چگونگی نگه‌داری و حفظ دسترسی ایجاد شده در این فصل پرداخته خواهد شد.

1. Exploit

پیغام جعلی مبنی بر شناسایی شدن ویروس DSVX در اکانت ایمیل یاهو

اگر پیغامی مبنی بر اینکه ویروسی در ایمیل یاهوتان کشف شده است، دریافت نمودید آنرا حذف نمایید. این روشی است که اخیرا مهاجمان به منظور فریب کاربران استفاده می‌نمایند. مهاجم ایمیل نامعتبری را که نشان دهنده این است که از طرف شرکت یاهو ارسال شده است، ارسال می‌نماید که در آن ذکر شده است که ویروسی به نام DSVX در اکانت ایمیل شما کشف شده و شما برای رفع آن باید اکانت خود را به‌روزرسانی نمایید. این ایمیل همچنین اعلام می‌نماید که با به‌روزرسانی اکانت خود به آخرین حفاظت کننده هرزنامه، ارسال ایمیل سریع‌تر شده و به فضای نامحدود دست خواهید یافت. بدین منظور، این پیغام از کاربران نام کاربری، شناسه ایمیل، رمزعبور، سوال امنیتی ایمیل و پاسخ آن، نام کشور، شماره تلفن و تاریخ تولد را درخواست می‌نماید.

لازم به ذکر است که شرکت یاهو و یا هر سازمان دیگری هرگز درخواست ارسال نام کاربری و رمزعبور و یا سایر اطلاعات حساس را از طریق یک ایمیل ناامن، نمی‌نماید.

سرقت ۸۳ هزار دلار از mining poolهای Bitcoin

تا کنون خبرهایی در مورد هک شدن کیف‌های الکترونیکی Bitcoin و یا وب سایت‌های Bitcoin گزارش شده است؛ اما اکنون هکرها توانستند با سرقت پول رمزنگاری شده از mining poolها، ۸۳ هزار دلار به سرقت ببرند.

Bitcoin پول مجازی رمزنگاری شده‌ای است که در کیف‌های الکترونیکی ذخیره می‌شود و به منظور استفاده و یا انتقال پول توسط کاربران استفاده می‌گردد. رمزنگاری مورد استفاده Bitcoin از نوع رمزنگاری کلید عمومی می باشد، بدین صورت که هر دو کلید عمومی و خصوصی مورد استفاده شده‌ی bitcoin، در کیف الکترونیکی ذخیره می‌گردد. محققان توانستند مجموعه‌ای از فعالیت‌های مخرب را شناسایی نمایند. آنها متوجه شدند که روش سارقان پول‌های رمزنگاری شده، به منظور سرقت پول‌های الکترونیکی از کاربران بدین صورت بوده است که آنها از پروتکل‌های ساختگی‌ای به منظور hijack نمودن شبکه‌ی چندین شرکت فراهم کننده اینترنت استفاده کرده و با ایجاد تغییر مسیر بخشی از ترافیک آنلاین سرورهای آن‌ها، موفق به سرقت شده‌اند. با توجه به مدت زمان انجام این سرقت، محققان تخمین زده‌اند که در حدود ۸۳ هزار دلار توسط سارقان سرقت شده است.

علاوه بر Bitcoin، سارقان قادر به سرقت پول‌های رمزنگاری دیگری همچون HoboNickels، Dogecoin و WorldCoin شده اند.

محققان اعلام کردند که سرورهای mining pool ای که از پروتکل‌های رمزنگاری SSL استفاده می‌نموده‌اند، از مسیردهی مجدد به سرور دیگر و سرقت، در امان مانده اند.

خطای Blue Screen of Death به دلیل به‌روزرسانی ماه آگوست شرکت مایکروسافت

شرکت مایکروسافت اخیرا کاربران خود را مجبور به حذف آخرین به‌روزرسانی امنیتی خود نموده است. این اقدام بعد از گزارش پدید آمدن خطای نامعلوم BSoD توسط کاربران این شرکت صورت گرفت.

به‌روزرسانی امنیتی ماه آگوست شرکت مایکروسافت علاوه بر دارا بودن آسیب‌پذیری افزایش حق دسترسی، به دلیل حذف نمودن کش- فونت ویندوز سبب ایجاد خطای صفحه‌ی آبی می‌شود. این اقدام پس از اعتراض صدها کاربر به این خطای نامعلوم صورت گرفت.

به‌روزرسانی MS 14-045 ، یکی از نه به‌روزرسانی اخیر شرکت مایکروسافت است که به منظور رفع ضعف‌های امنیتی که یکی از آنها در هسته‌ی ویندوز قرار دارد، داده شده است. این به‌روزرسانی سبب شده است که کاربران به اجبار سیستم خود را راه‌اندازی مجدد نمایند. این قضیه کمی بعد از انتشار این به‌روزرسانی توسط یکی از کاربران شرکت مایکروسافت در انجمن مجازی این شرکت اعلام گردید. این خطا بعد از اجرای یکی از چهار به‌روزرسانی KB2975331 ، KB2975719 ، KB2970228 ، KB2982791 ایجاد می‌شود که پس از اجرا، پیغامی مبنی بر راه‌اندازی مجدد درخواست می‌گردد. این ضعف بیشتر توسط کاربران ویندوز ۷ نسخه ۶۴ بیت گزارش داده شده است.

براساس گفته‌ی شرکت مایکروسافت، این خطا بیشتر به دلیل نصب شدن آپدیت‌های زیر می‌باشد:

- MS14-045 2982791: به‌روزرسانی امنیتی برای درایورهای هسته – ۱۲ آگوست ۲۰۱۴-۰۸-۲۵
- 2970228: به‌روزرسانی به منظور پشتیبانی از نماد پول جدید کشور روسیه در ویندوزها
- 2975719: به‌روزرسانی ماه آگوست ۲۰۱۴ برای Windows Server 2012 R2 ، Windows 8.1 ، Windows RT 8.1
- 2975331: به‌روزرسانی ماه آگوست ۲۰۱۴ برای Windows Server 2012 ، Windows 8 ، Windows RT

تبلیغات اجباری از طریق یک بدافزار!

آگهی‌افزار یا بدافزار تبلیغاتی (Adware) نام گونه‌ای از بدافزار است که با هدف تبلیغات ساخته و منتشر می‌شود. این نوع بدافزارها اگرچه ممکن است خطر اساسی برای سیستم نداشته باشند اما با باز کردن پی‌درپی صفحات تبلیغاتی دردسرساز می‌شوند. به گزارش گروه تحلیل بدافزار پادویش این بار این روش ناپسند تبلیغاتی توسط بدافزار Adware.win32.adsline به کار گرفته شده است که به تبلیغ در برخی سایت‌های فارسی زبان می‌پردازد.

این بدافزار تمامی فایل‌های اجرایی سیستم را با اضافه کردن یک کاراکتر $ به انتهای نام فایل، تغییر نام داده (به جز فایل هایی که در درایو نصب ویندوز هستند) و یک رونوشت از خود را به جای آنها قرار می‌دهد. به علاوه عملیات مذکور را روی فایل‌های اجرایی موجود در usbهای متصل به سیستم انجام می‌دهد. این کار باعث می‌شود تا با اجرای هر فایل سالم، یکبار این بدافزار اجرا شود و صفحه تبلیغاتی مربوط به آن باز شود. آیکون این بدافزار به شکل  است. درصورت آلوده بودن سیستم تمامی آیکون‌های فایل‌های اجرایی در همه درایوها به جز درایو نصب ویندوز به این شکل خواهد بود.

سیستمی که به این کرم آلوده شود بلافاصله با صفحه‌ی اینترنتی با آدرسی مشخص روبرو می شود که به فروش خدمات خاصی اشاره می کند. این آدرس می تواند به هر آدرسی که هکر می‌خواهد redirect شود. آنچه که هم‌اکنون هدف این بدافزار است فروش آنتی ویروس از طریق اتصال به درگاه بانکی است. این سایت، کاربر سیستم قربانی را به خرید آنتی ویروس اصل شرکت‌های kaspersky و eset از طریق سایت خود ترغیب می کند. در کد مخرب قرار داده شده در این بدافزار هر ۲۴ ساعت صفحه‌ی مرورگر باز شده و به آن آدرس هدایت می‌شود.

بدافزار فایل‌های اجرایی که در مسیر HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run قرار دارند را با فایل خود جایگزین کرده، سبب اجرای کرم در هربار بالا آمدن سیستم می‌شوند.

نرم‌افزاری که این کرم برای پیاده سازی اهداف خود از آن استفاده کرده AutoPlay Media Studio بوده که نرم‌افزاری برای تولید فایل‌های autorun از شرکت indigorose است. یکی از ویژگی‌های این نرم‌افزار استفاده از موتور برنامه‌نویسی LUA 5.1 است. در واقع هکر با اضافه کردن اسکریپت‌های مورد نظر خود به یک پروژه‌ی عادی ساخت برنامه‌های autorun، توانسته سیستم را به هدف فروش محصولات و خدمات خود آلوده کند.

برای جلوگیری از آلوده شدن به این بدافزار و به طور کلی adwareها استفاده از یک ضدویروس به‌روز، یک راه حل منطقی می‌باشد. لازم به ذکر است ضدویروس پادویش این بدافزار را خنثی می‌کند.

پادویش

خلاق و هوشمند، در خدمت امنیت

موتور هوشمند، مقابله
با ویروس های ناشناخته

رهایی از کابوس
فلش های ویروسی

سرعت در پویش
قدرت در پاکسازی

www.padvish.com

شرکت نرم افزاری

امن پرداز

آدرس: تهران، خیابان ملاصدرا، خیابان شیخ بهایی جنوبی، گرمسار غربی، پلاک ۷۶
تلفن: ۰۲۱-۴۳۹۱۲۰۰۰ فکس: ۰۲۱-۴۳۹۱۲۸۰۰
www.amnpardaz.com
info@amnpardaz.com