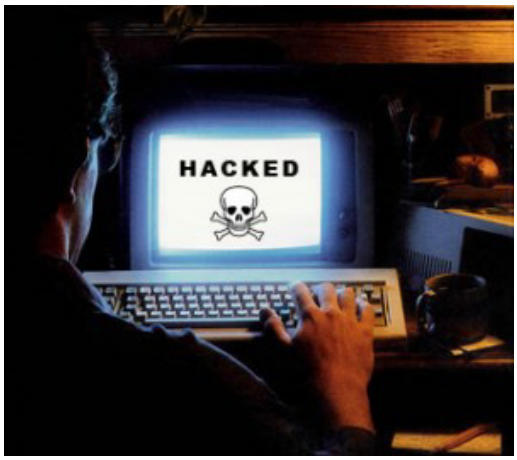
پـس از انتخابـات ایـران صـورت گرفـت: حملـه هکرهـا بـه سـایت هـای خبـری

بعد از انتخابات باشکوه ۴۰ میلیونی در ۲۲ خرداد ۱۳۸۸ و اغتشاشات صورت گرفته پس از آن، فضای اینترنـت نیـز از یورش حمله کنندگان اینترنتی (هکرها) در امان نماند و این امر باعث شد برخی سایت های خبری از کار افتاده و عملاً جریان اطلاعات کند شود. گفتنی است نداشـتن یـک سیاسـت امنیتی جامع در اکثر سایت های خبری و نیز وجـود ضـعفهای امنیتی در آنها، اثربخشی این حملات را دو چندان کرده اسـت. از همین رهگذر می توان به این نکته پی برد که اگر مدیران و دست اندرکاران سایت ها، به راهکارها و سیاست های امنیتـی مناسب پایبند باشند، در مواقع بحرانی می توانند سرویس هـای خود را از گزند اختلالات ناخواسته محافظت نمـوده و خـدمات مطلوب و قابل قبولی به کاربران و مشتریان ارائه نمایند. در حال حاضر در سایت های معمولی، هزینه های امنیتی ۱۲ درصد کل هزینه ها را به خود اختصاص می دهد. این میزان در سایت هایی که به نقل و انتقالات مالی می پردازند تا ۲۰ درصد و در حوزه نظامی نیز تا ۳۰ درصد از بودجه را در بر می گیرد. *(منبع: مهران رایانه)*



با این بدافزارها آشـنا شـوید

W32/AutoRun.ea و W32/Fraud.er.ch دو کـرم اینترنتی هستند که به تازگی به پایگاه داده ضدویروس ایمن افزوده شده است. بـر اسـاس گـزارش هـای آزمایـشگاه تحقیقات ویروس‌های رایانه‌ای ایمن، بدافزارهای یادشده علاوه بر ایجاد تعدادی فایل بر سیستم قربانی، رجیـستری را نیز دستکاری می کنند. تغییر IP کاربران شبکه، یکی دیگر از اختلالاتی اسـت کـه کـرم W32/AutoRun.ea بـه وجود می آورد. برای بر طرف سازی اثرات تخریبی این کـرم در رجیـستری، مـی توانیـد برنامـه RegRepair را از آدرس http://www.imenantivirus.com/RegRepair.zip دانلود و اجـرا نماییـد. اطلاعـات تکمیلـی را در http/ www.imenantivirus.com/encycf/encycf.htm پیگیر شوید.

راهنمای آزمایش امنیت شبکه (قسمت چهل و نهم – مقایسه تطبیقی ، بخش سوم)

سومین قسمت موضوع «مقایسه تطبیقی بین تکنیک های مختلف تست شبکه» را پی می گیریم:

۴. شکستن کلمه عبور (Password cracking)

مزایا:
- سریعاً کلمات عبور ضعیف را شناسایی می کند.
- تصویر واضحی از ضعف و قوت کلمات عبور ارائه می کند.
- به راحتی اجرا می شود.
- کم هزینه است.

ضعف ها:
- بالقوه می تواند مورد سو استفاده قرار گیرد.
- یک سری محدودیت های خاصی برای سازمان بوجود می آورد.

۵. تکنیک بازبینی فایل های ثبت شده (Log reviews)

مزیت:
- با استفاده از آن می توان اطلاعات جالب و خوبی تهیه کرد.

ضعف ها:
- مرور فایل ها به طور دستی، کاری سخت و طاقت فرساست.
- ابزارهای خودکار نمی توانند به طور کامل اطلاعات مهم را فیلتر کنند.

۶. آزمون ویروس یاب ها (Virus Detectors)

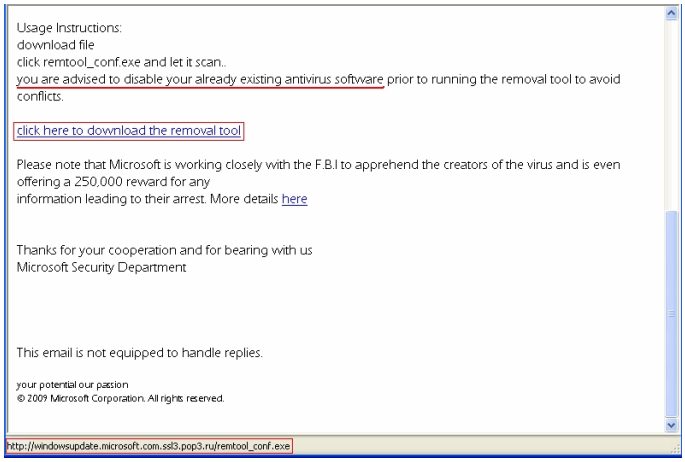
مزایا:
- روشی است عالی برای محافظت در برابر ویروس ها و حذف آنها.
- هزینه ای که در بر دارد، کم یا متوسطی است.

ضعف ها:
- برای تاثیرگذاری بهتر، نیازمند بروزرسانی است.
- توانایی آن در واکنش دهی به ویروس های جدید و آن دسته از ویروس های که به سرعت خود را کپی می کنند، اندک است.
- موقع کار با آن، بعضاً با پیغام False positive مواجه می شویم. *(منبع: مهران رایانه)*

تهیه کننده: شرکت مهندسی مهران رایانه – واحد پشتیبانی فنی
تلفن: ۲۲۰۵۰۷۸۰ – ۲۶۲۰۲۴۹۳
آدرس: تهران– انتهای بلوار آفریقا – خ شهید طاهری – ایثار۳ – ایثار۲ – شماره ۱۷ – ساختمان مهران
نمابر: ۲۲۰۵۳۹۲۷

Patch دروغین مایکروسافت

در چند روز اخیر سه بدافزار فعال در اینترنت مشاهده شـده کـه در پوشـش وصـله ترمیمـی مایکروسـافت و بـا بهـره گیـری از بـستر ایمیـل، منتـشر مـی شـوند. وصـله اول که Important Windows XP/Vista Security Update نام دارد، در ظاهر حاوی ابـزاری بـرای پاکـسازی کانفیکر (Conficker) است. وصله دوم Outlook re-configuration است که در ماه جاری به صـورت spam در فضای اینترنت مشاهده شد. مورد آخر هـم کـه عنـوان پرطمطـراق Update for Microsoft Outlook / Outlook Express (KB1072) را یـــدک می کشد، چیـزی نیـست جـز یـک تروجـان! گفتنی است این بـه اصـطلاح Conficker removal حدود یک هفته است که فعالیت خود را آغاز نموده و جالب است که نویـسندگان آن گـویی نتوانـسته انـد تفاوت بین TrojBrisvA و Conficker را دریابنـد. آنهـا مرتکـب یـک اشـتباه نوشـتاری نیـز شـده انـد و Conficker را ConFlickerz درج نموده اند! گفتنی است Conficker نوعی کـرم رایانـه‌ای اسـت کـه از اکتبـر سال ۲۰۰۸ ظاهر شده و رایانه‌هایی را که با سیستم این بدافزار به نام داونادآپ (Downadup) نیـز شـناخته مـی‌شـود. شرکت مهران رایانه در خبرنامه شـماره ۱۶۲ و ۱۶۸ موضـوع ویـروس Conficker را مـورد بحـث و بررسـی قـرار داده است. *(منبع: CyberInsecure)*


Usage Instructions:
download file
click remtool_conf.exe and let it scan..
you are advised to disable your already existing antivirus software prior to running the removal tool to avoid conflicts.

click here to download the removal tool

Please note that Microsoft is working closely with the F.B.I to apprehend the creators of the virus and is even offering a 250,000 reward for any information leading to their arrest. More details here

Thanks for your cooperation and for bearing with us
Microsoft Security Department

This email is not equipped to handle replies.

your potential our passion
© 2009 Microsoft Corporation. All rights reserved.

http://windowsupdate.microsoft.com.ssl3.pop3.ru/remtool_conf.exe

- *نظرات، انتقادات و پیشنهادهای شما برای ما ارزشمند است: support@MehranCo.com*
- *منابع اخبار و تصاویر در «پشتیبانی فنی شرکت مهندسی مهران رایانه» موجود است.*
- *وب سایت رسمی شرکت مهندسی مهران رایانه، www.MehranCo.com می باشد.*
- *استفاده از اخبار و مطالب خبرنامه «با ذکر منبع» بلامانع است.*