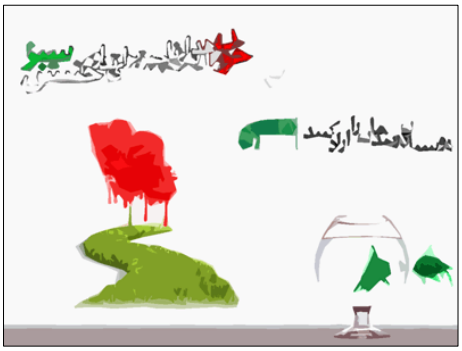
W32/Trojan.ahk؛ کرم جدید اینترنتی

Trojan.ahk نوعی کرم اینترنتی است که با حجم ۳۳۸۴۳۲ بایت، اقدامات تخریبی مختلفی بر رایانه قربانیان انجام می دهد. تغییر تصویر پس زمینه رایانه (تصویر روبرو)، ایجاد فایل inetinfo.exe و اعمال تغییراتی در رجیستری بخشی از این فعالیت های ناخوشایند است. به گزارش *آزمایشگاه تحقیقات ویروس‌های رایانه‌ای ایمن*، کاربران می توانند برای بر طرف سازی اثرات تخریبی این کرم در رجیستری، برنامه RegRepair.zip را به طور رایگان از آدرس http// www.imenantivirus.com/RegRepair .zip دانلود کرده و مورد استفاده قرار دهند.



مشکل کاربران با کرم جدید Palevo

از آغاز اسفند ماه کاربران ضدویروس ایمن با کرم جدیدی دست و پنجه نرم می کنند که ضدویروس ایمن آن را به نام Palevo شناسایی و پاکسازی می کند. این کرم در پوشه های Recycler و System، فایل های logon.exe، Isass.exe، firewall.exe و explorer.exe را ایجاد می نماید. بر اساس این گزارش، در هفته اخیر بخش پشتیبانی فنی شرکت مهران رایانه تماس های بسیاری در ارتباط با این کرم و آلودگی های ناشی از آن داشت. به گزارش بخش پشتیبانی فنی شرکت مهندسی مهران رایانه، اکثر گونه های این کرم در اواخر هفته گذشته به ضد ویروس ایمن اضافه شده و اکنون توسط آن قابل پاکسازی است.

مایکروسافت بات نت Waledac را فلج کرد

مایکروسافت طی عملیاتی موفق، یکی از بزرگترین بات نت های جهان را از کار انداخت. واحد Digital Crimes مایکروسافت توانست با ممانعت از دسترسی بزهکاران سایبری به صدها هزار رایانه آلوده در سراسر جهان، بات نت والداک (Waledac) را از کار بیاندازد. مایکروسافت با همکاری برخی شرکت های امنیتی و مراکز قانونگذاری، طرح موسوم به عملیات b49 را

آدرس: تهران- انتهای بلوار آفریقا – خ شهید طاهری – ایثار۳ – ایثار۲ – شماره ۱۷ – ساختمان مهران | تلفن: ۲۲۰۵۰۷۸۰ – ۲۶۲۰۲۴۹۳ | نمابر: ۲۲۰۵۳۹۲۷

اجرا نمود و با استفاده از دستور قضایی، ۲۷۷ دامنه دات کام آلوده را که توسط صاحبان والداک مورد سوءاستفاده قرار گرفته بوده، بست. بر اساس این گزارش، والداک یکی از ۱۰ بات نت بزرگ در آمریکا به شمار می رود که مسئول ارسال میلیاردها هرزنامه در سراسر جهان است. مایکروسافت می گوید که این شبکه خرابکار، صدها هزار رایانه را در سراسر جهان آلوده ساخته و گمان می رود از قابلیت ارسال روزانه ۱/۵ میلیارد هرزنامه در روز برخوردار باشد. *(منبع: sgnec.net)*

افزایش محبوبیت مرورگر کروم در فوریه ۲۰۱۰

کروم گوگل تنها مرورگر اینترنتی است که طی ماه گذشته موفق شد سهم بیشتری از بازار را به خود اختصاص دهد و از رقبای سرسختی چون Internet Explorer، فایرفاکس و Safari پیشی بگیرد. به گفته شرکت تحقیقاتی Net Applications، سهم کروم از بازار مرورگرهای اینترنتی در ماه گذشته با رشد ۰/۴ درصدی به ۵/۶ درصد رسید. محبوبیت این مرورگر طی ۱۶ ماهی که از عرضه آن می‌گذرد سیر صعودی را دنبال کرده و ظرف ۶ ماه گذشته سهم آن از بازار جهانی مرورگرهای اینترنتی دو برابر شده است. در ماه گذشته میزان استفاده از Internet Explorer مایکروسافت با کاهش ۰/۵ درصدی به ۶۱/۲ درصد رسید که البته این رقم کمترین افت IE در سال جاری بود. فایرفاکس نیز در این دوره زمانی با کاهش محبوبیت ۰/۲ درصدی، حدود ۲۴/۲ درصد از بازار جهانی را تصاحب کرد. دو مرورگر برتر دنیا یعنی IE و فایرفاکس در ماه ژانویه نیز با کاهش محبوبیت خود نزد کاربران مواجه شدند. در ماه فوریه سهم Safari اپل از بازار جهانی مرورگرها با ۰/۱ درصد کاهش به ۴/۴ درصد رسید و باعث تعجب کارشناسان شد. مرورگر کروم برای نخستین بار در دسامبر گذشته از Safari اپل بیشتر شد و کارشناسان پیش‌بینی می‌کنند که این روند در آینده نیز به همین صورت دنبال شود. مرورگر اینترنتی گوگل در ماه‌های گذشته قابلیت‌های جدیدی را در اختیار کاربران قرار داده و احتمالا همین مسئله باعث افزایش محبوبیت آن شده است. *(منبع: systemgroup.net)*

نقد ایمیل ملی

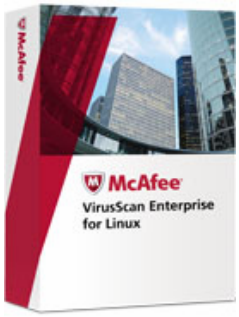
پست الکترونیکی و یا لغت جدید و زیبای «رایانامه» موضوعی است که تقریبا تمامی کاربران اینترنت اعم از برخط و یا غیر برخط به آن توجه ویژه ای دارند و همواره مانند آدرس منزل و محل کار به آن اهمیت می دهند زیرا رسمیت مکاتبات الکترونیکی ضرورتی است که نقش آن در محیط مجازی پذیرفته شده است. در حال حاضر اکثر کاربران اعم از ایرانی و خارجی از سرویس های رایانامه رایگان مانند Gmail، Yahoo و ... استفاده می کنند که انصافاً خدمات خوبی ارائه می دهند و کاربران داخل کشور نیازی نمی بینند که در صورت راه اندازی، از رایانامه ملی استفاده نمایند. اهم دلایل این عدم احساس نیاز عبارت است از: **۱.** نداشتن امنیت (در حال حاضر کاربر ایرانی نگران لو رفتن اطلاعات خویش توسط خارجی ها نیست و یا کمتر از حالتی است که اطلاعاتش دست افراد فارسی زبان بیافتد)؛ **۲.** داشتن هزینه (معمولاً کاربر ایرانی تجربه خوبی از گرفتن سرویس های داخلی بصورت رایگان نداشته و در مقام مقایسه، سرویس های رایگان خارجی را معتبر تر می داند)؛ **۳.** احتمال تحریم (کاربر ایرانی همواره نگران بحث تحریم می باشد و بخاطر اینکه در روند جاری به مشکلی برنخورد، سعی می کند در مکان های بین المللی آدرس داشته باشد تا مکان های ملی که توسط کشورهای غربی همواره مورد تهدید قرار دارد).

بنابر این وقتی موضوع رایانامه ملی مطرح می گردد اینطور تصور می شود که قرار است پروژه ای در سطح ملی اجرا شده و مبالغی هزینه گردد و بعدش هم به دست فراموشی سپرده شود. حال می توان در اهداف رایانامه ملی فرصت هائی را قرار داد تا علاوه بر رفع نگرانی کاربر ایرانی باعث شود کاربر علاقمند گردد از فرصت ایجاد شده استفاده کند و در نهایت موفقیت طرح ملی را بدینصورت تضمین کرد. موضوع اول توان و ظرفیت رایانامه ملی است که باید برای ۷۳ میلیون نفر ایرانی (فضای رایگان هشت گیگا بایتی برای هر کاربر) ایجاد گردد. موضوع دوم بحث رایگان بودن آن تا حد مشخصی است که کاربران بدانند بابت ظرفیت های بیشتر چه مقدار هزینه باید پرداخت نمایند. موضوع سوم اینکه به کاربر آموزش داده شود که در وضعیت صد در صد تحریم و یا قطع اینترنت خارج از کشور می تواند از رایانامه خود استفاده نماید (میزان زیادی از رایانامه ها داخلی هستند و وابسته به ارتباطات خارجی نیستند). موضوع چهارم نیز متقاعد کردن کاربر به حفظ حریم شخصی وی است تا کاربر نگران بهره برداری از اطلاعات خود توسط دیگران نباشد. این امر

آدرس: تهران- انتهای بلوار آفریقا - خ شهید طاهری - ایثار۳ - ایثار۲ - شماره ۱۷ - ساختمان مهران | تلفن: ۲۲۰۵۰۷۸۰ - ۲۶۲۰۲۴۹۳ | نمابر: ۲۲۰۵۳۹۲۷

نیاز به فرهنگ سازی و اداله قانونی دارد که کاربر حقوق خود را شناخته و بداند که احدی حق تعرض به آن را ندارد. قطعاً در یک فضای صمیمی می توان توانمندی داخلی را در رقابت با سرویس خارجی ارائه نمود و تعداد کاربران عضو می تواند بیانگر میزان موفقیت طرح باشد و گرنه با فیلتر کردن سرویس های بین المللی علاوه بر اینکه نمی توان برای توانمندی داخلی ظرفیت سازی نمود، بلکه این امر باعث می شود که میوه منع شده شیرین تر به نظر آید و انواع و اقسام فیلترشکن ها در محیط مجازی کاربران ایرانی حضور پیدا کنند که این به نوبه خود به بروز رسانی یک تهدید دیگر در فضای مجازی کشور منجر می گردد. (شرکت مهندسی مهران رایانه .)

حفره امنیتی در یکی دیگر از محصولات مکافی



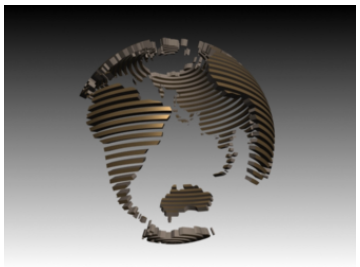
یک باگ امنیتی در ضدویروس لینوکسی مکافی به نام LinuxShield شناسایی شده است که هکرهای برون سازمانی با استفاده از آن می توانند به درستی سنجی نام های کاربری در رایانه مقصد اقدام نمایند. این باگ امنیتی توسط SecurityTracker گزارش شده است.

آشنایی با Clickjacking یا کلیک دزدی

کلیک جکینگ (کلیک دزدی) یک روش هوشمندانه است برای ترغیب یا مجبور کردن کاربران به کلیک کردن روی چیزی، بدون اینکه از آن آگاه باشند. این تکنیک به شکل های مختلفی اتفاق میفتد و ممکن است هر کاربری را فریب دهد، اما با کمی دقت و استفاده از ابزارهایی خاص، می‌توان از آسیب‌های این روش در امان ماند. برای مثال با استفاده از CSS لایه‌ای شفاف روی صفحه وب قرار می‌گیرد که باعث می‌شود تمام صفحه به یک لینک تبدیل بشود و با کلیک کردن روی قسمت‌های خالی صفحه به مکان مورد نظر هکر منتقل بشوید. *(منبع: negahbaan)*

برخی عناوین اخبار IT
به نقل از خبرگزاری ها و سایت های داخلی

- **شهروندان جامعه اطلاعاتی در معرض بمباران اطلاعاتی** – ایتنا
- **ثبت دامنه اینترنتی به خط فارسی تا یک ماه آینده** – خبرگزاری مهر
- **اینترنت ملی ۴ سال دیگر به بهره‌برداری می‌رسد** – ایتنا به نقل از ایسنا
- **وبلاگ‌نویسی؛ گونه‌ای از مسرت و رهایی** – ایسنا
- **دکتر جلالی: مخالف ایمیل ملی هستم** – هموطن سلام
- **اینترنت بدون گوگل، زندگی بدون برق!** – خبرآنلاین
- **کشف شیوه‌ی جدید انتشار ویروس در اینترنت** – ایسنا
- **یک مقام مسئول: رشد پنج درصدی پورت‌های پرسرعت واگذار شده در بهمن ماه** – ایرنا
- **مدیرکل روابط عمومی شرکت مخابرات ایران: مخابرات به دنبال کاهش هزینه است** – موبنا
- **کابوسی به نام «فیس‌بوک»** – مدیانیوز به نقل از دویچه وله
- **مدیر یک شرکت اینترنتی: مخابرات تمام مسائل مرتبط با اینترنت را انحصاری کرده است** – ایلنا
- **طرح ساماندهی بازار فناوری‌اطلاعات کشور از سال ۸۹ آغاز می‌شود** – ایلنا
- **«غفلت در صنعت فناوری اطلاعات در کشور موج می‌زند»** – ایلنا
- **سبیت ۲۰۱۰ پایان یافت** – itiran به نقل از دنیای اقتصاد
- **برترین جستجوهای یاهو در ۱۵ سال گذشته: ۱۱ سپتامبر و شبیه سازی** – خبرگزاری مهر
- **استقبال از موبایل ایرانی در نمایشگاه سبیت** – موبنا



برخی عناوین اخبار IT
به نقل از خبرگزاری ها و سایت های خارجی

- **فیشرها به دنبال لقمه های بیشتر و بزرگتر** – eSecurity Planet
- **ظهور بات نتی برای حل کردن کپچا!** – CyberInsecure به نقل از Softpedia.com News
- **گوگل DocVerse را خرید** – InternetNews.com
- **پلیس سرکرده های بات نت Mariposa را دستگیر کرد** – ZDNet Blog Security
- **چین قول داد هکرهای گوگل را تنبیه کند** – Fudzilla
- **موافقت تایلند با استرداد هکر کارت های اعتباری به ایالات متحده** – PCWorld
- **کمک سیستم قضایی به مایکروسافت برای مبارزه با Waledac** – SPAMfighter
- **مدیر FBI: هکرها علاوه بر سرقت اطلاعات، آنها را دستکاری می کنند** – PCWorld
- **IBM: افزایش حملات فیشینگ و SQL Injection در ۲۰۰۹** – SPAMfighter
- **فیشرها در ژانویه رکورد خود را بهبود بخشیدند!** – V3.co.uk

- *نظرات، انتقادات و پیشنهادهای شما برای ما ارزشمند است: support@MehranCo.com*
- *آدرس کامل 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.*