*** ۱۰ مشکل شبکه و روشهای مقابله با آنها ***

هرچه را که روی اینترنت می‌خوانید باور کنید، اینترنت جای خطرناکی است، پر از هکر که می‌توانند در عرض چند ثانیه به PC شما حمله کنند، ویروسهایی که می‌توانند سیستم شما را از پای درآورند. این جملات را تا به حال چند دفعه شنیده‌اید؟ مردم دیگر گوششان پر از این جمله‌های رعب‌آور و وحشت انگیز شده است ولی واقعیت چیز دیگری است. چند وقت پیش در یک گروه خبری نوشته بود". آیا می‌دانید که هر کلیک روی ویندوز ۹۸ و منوی Start شما بطور دائم و بصورت مخفی در یک بانک اطلاعاتی ذخیره می‌شود؟" و حتی می‌توانند هر صفحه وبی که سالهای سال پیش دیده‌اید را هم به شما نشان دهند و می‌توانند بفهمند که کدام سایتها را دیده‌اید؟ شاید این خبرها تا حدی درست باشد ولی کمی هم اغراق آمیز هستند.

لذا ما تصمیم گرفتیم که به جای این حرفها کمی فنی‌تر با قضیه برخورد کنیم و راههای حمله و مقابله را در کنار هم به شما آموزش دهیم. پس با ما باشید:

۱ – Spyware

سایت http://www.whatis.techarget.com به ما گفت که Spyware برنامه‌ای است که بصورت پنهانی روی سیستم شخصی می‌نشیند و اطلاعات خاصی را به سمت مشخصی می‌فرستد. بسیاری از این برنامه‌ها با کلیک شما روی یک تبلیغ در یک سایت وارد سیستمتان می‌شوند. برای درک بهتر این مسئله ما آخرین نسخه Go!zilla (که ادعا شده آن یک Spyware است) را روی یک ماشین نصب کردیم. در حین نصب، صریحاً ذکر شد که این برنامه در Background اجرا می‌شود و اطلاعاتی را جمع‌آوری می‌نماید و به سمت سایتهای تبلیغ کننده می‌فرستد. پس از نصب، قسمت تبلیغات برنامه (Radiate) منوی Start > Programs خود را دارد و شما می‌توانید مطالب بیشتری را در مورد آن یا حذف کامل آن در اینجا بخوانید.

آقای Steve Gibson سایت وبی دارد که در آدرس http://www.grc.com قرار دارد و توجه مردم را بیشتر به Spywareها جلب کرده است (به قسمت grc.com/00/spyware.htm مراجعه کنید).

اگر بخواهیم در مورد Spyware توصیه‌ای کرده باشیم باید خدمتتان عرض کنیم که هیچ برنامه تبلیغی را روی سیستم خود نصب نکنید و اگر هم این کار را انجام دادید، حتماً licence را بخوانید، فقط روی Ok کلیک نکنید و ادامه دهید.

شـاید چنـد تـا از ایـن بسـته‌هـای نـرم افـزاری هـم اکنـون روی سیسـتم شـما نصـب باشـند، سـایت http://www.lavasoft.de به شما در حذف آنها کمک می‌کند ولی راحت باشید زیـرا حـذف برخـی از قسمتهای تبلیغاتی برنامه‌ها می‌تواند کلاً باعث از کار افتادن برنامه‌ها شود.

درجه خطر: ۲
http://www.spychecker.com یک بانک اطلاعاتی بزرگ از spywareها است.

۲ – برنامه‌های ستیزه جو

هر کاری روی اینترنت یک کار خطا محسوب نمی‌شود و گاهاً مثل یـک شـوخی یـا آزار دوسـتانه هـم تلقـی شده‌اند.

مثلاً نگاهی به مگاهرتز http://www.gohip.com بیندازید. "ارتقاء مرورگر" آنرا نصب کنید و بگذاریـد خودش پیش فرض Search شما را Set کند و تبلیغات را بصورت ثابت نمایش دهد و سایتهای دیگـر را بـا اضافه کردن آنها به Favorite شما، اعلام نماید. هیچ گزینه Uninstallای هم وجود ندارد. بـرای اینکـه متوجـه شـوید چگونـه مـی‌تـوان ایـن برنامـه را remove کـرد بـه سـایت http://www.gohip.com/remove_enhancement.html مراجعه کنید. بعضی وقت‌ها برنامه نویسی بد، کاربران را بطور جدی دچار مشکل کند.

برنامه‌های زیادی که احتیاج به کار بصورت تنگاتنگ با مرورگر را دارند (مثلاً یک شتابدهنده مرورگـر) خـود را همچون یک Proxy روی سیستمتان نصب می‌کنند و این بدان معنی است که کنترل اتصال اینترنت شما را به دست می‌گیرد. اگر بعد از Uninstall کردن به درستی فایلهای این برنامه‌هـا remove نشـود مرورگـر شما صفحات وب را دیگر نشان نخواهد داد. پاک کردن تنظیمات Proxy تنها راه رفع مشکل است. Tools > Internet Options > Connections > LAN Settings را انتخاب کنید و علامت Use a proxy server را پاک کنید.

عملاً راهی برای رهایی از این برنامه‌ها وجود ندارد ولی یک راه جالب برای رفع این مشکل این است که وقتی شما برنامه‌ای این چنین را نصب می‌کنید، هرگـز از قسـمت Conditions نخوانـده رد نشـوید (بـه سـایت http://www.gohip.com/freevideo مراجعه کنید تا دقیقاً علت ایـن کـار را متوجـه شـوید). روی برنامه‌ای مثل (http://www.roxio.com) سرمایه گذاری کنید که بوسیله آن می‌توانید اشتباهات خـود را Undo کنید. و در ضمن یک سری هم به سایت http://groups.google.com برای توصـیه‌هـای بیشتر بزنید.

درجه خطر: ۳
به سایت GoHip برای دریافت اطلاعات مراجعه کنید.

۳ – حملات DoS

بچه‌های اسکریپت کوچکترین فرم حمله‌ها محسوب می‌شوند. به خاطر کمبود توانایی تکنولوژی در انجام انواع حملات کاغذی، آنها با استفاده از برنامه‌های خاصی که نوشته‌اند باعث آزار و اذیت افراد دیگر می‌شوند (DoS = Denial of Service به زبان ساده یعنی روشی برای از کار انداختن PC شخص دیگری).

شاید برایتان جالب باشد که بدانید انجام اینکار خیلی ساده‌تر از آن است که بتوانید تصور کنید. مثلاً اگر یک برنامه بتواند مجموعه داده‌هایی را به سمت یک PC با سیستم عاملی که Update نشده بفرستد، در آن صورت آن PC، هنگ خواهد کرد و ارتباط اینترنت خود را از دست خواهدداد یا صفحه آبی رنگ ویندوز که به صفحه مرگ آن معروف است ظاهر خواهد شد. تمام اسکریپت نویسهای این نوع حملات باید آدرس IP شما را بدانند واگر مثلاً شما در یک IRC باشید یا در حال استفاده از یک برنامه پیام رسان مثل ICQ باشید، بدست آوردن IP شما مثل آب خوردن است.

اما خبر خوب در مورد حملات DoS این است که آنها رو به زوال می‌روند و دیگر آنقدرها هم خطرناک نیستند حتی اگر باعث Crash شدن سیستم شما شوند یک reboot همه چیز را به حالت نرمال باز خواهد گرداند.

اما خبر بد اینکه، محافظت در برابر آنها سخت است. بهترین روش، به روز نگهداشتن ویندوز خود (http://www.windowsupdate.com) و دیدن سایتهای جالبی مثل IRCHelp(http://www.irchelp.org/irchelp/nuke) می‌باشد.

درجه خطر: ۲
مطالبی بیشتری را در مورد انواع روش حمله و کتابخانه‌های آن پیدا کنید. سایت http://www.antionline.com/cgibin/anticode/anticode.pl را ببینید.

٤ – ویروسها

ویروسها برنامه‌های مشکوکی هستند که خودشان را به یک میزبان می‌چسبانند. در حالی که اولین ویروس در یک کد اجرایی پیدا شد (معمولاً به دنبال فایلهای .EXE و .Com می‌آمدند) ولی با آمدن زبانهای اسکریپتینگ ویندوز، حوزه فعالیت آنها به e-mail، ورد و اکسل و بسیاری از برنامه‌های دیگر هم کشید.

هرچند بسیاری از ویروسها تنها برای تکثیر خود ساخته شده‌اند ولی برخی هم حاوی داده‌هایی هستنند. حذف یا رونویسی فایلهای مهم از جمله کارهای بدی است که برخی از آنها انجام می‌دهند. ولی اگر بتوانید مطمئن شوید که ویروسی ندارید، احتمالاً خیلی خوشحال خواهید شد.

هرگز کسی نمی‌تواند بطور کامل مطمئن باشد که عاری از ویروس است اما با استفاده از یک برنامه ضدویروس خوب که دارای پشتیبانیهای بروز است خطر وجود ویروس می‌تواند به مقدار زیادی کاهش یابد. می‌توانید برای شروع از سایتی مثل http://antivirus.cai.com یا http://housecall.antivirus.com (که بصورت online شما را اسکن می‌کند) استفاده کنید.

یادتان باشد که روی اینترنت به هیچ کسی اعتماد نکنید و تمام فایلها و e-mailهایی که می‌گیرید را اسکن کنید. و در آخر اینکه خود را با سایتهایی مثل http://www.antivirus.com/vinfo به روز نگهدارید.

درجه خطر: ۹
آخرین اخبار را در مورد ویروسها در سایتی مثل http://Packetstorm.security.com پیدا کنید.

۵ – Cookieها

شما در یک مغازه online هستید و مجموعه‌ای از سی دی‌هایی را که می‌خواهید بخرید انتخاب کرده‌اید ولی ناگهان متوجه می‌شوید که قرارتان دیر شده است. مشکلی نیست، می‌توانید مطمئن باشید که برمی‌گردید و سبد خرید هنوز حاوی دیسکهای شما خواهد بود و لازم نیست که از نو شروع به خرید کنید. این خاصیت به این دلیل وجود دارد که آن سایت یک کوکی به روی مرورگرتان می‌فرستد که حاوی اطلاعاتی درباره سفارش شما است. سایتهای دیگر نمی‌توانند این کوکی را بخوانند ولی همان سایت می‌تواند کوکی خود را بخواند. لذا وقتی برمی‌گردید می‌توانید عملیات خود را ادامه دهید.

خب تا اینجا که کوکی خوب بود اما در بعضی مواقع این تکنولوژی برای کارهای بیشتری استفاده شده است. بعضی از بنرهای تبلیغاتی از طریق کوکیها به سیستم شما یک شماره شناسایی منحصربفرد می‌دهند و تبلیغاتی را که شما دیده‌اید را ذخیره می‌کنند. این کوکیها صرفاً برای این هستند که بدانند شما چه سایتهایی را معمولاً دوست دارید ببینید و شاید هم اصلاً ندانند شما چه کسی هستید ولی گاهی باعث مزاحمت یا ارسال تبلیغات زیادی روی سیستم می‌شوند.

اگر نام و آدرس خود را وارد سایتی کنید می‌توانید انتظار داشته باشید که خیلی زود همه از آن مطلع شوند و در دنیای واقعی این آدرسها روی mailling listها خرید و فروش می‌شوند. و از همه بدتر اینکه تنظیمات کوکی مرورگر شما می‌تواند کنترل کل سیستمتان را به شخص دیگری هم بسپرد.

درجه خطر: ۱
بهترین راه فرار از کوکیها استفاده از نت اسکیپ ۶ است. کوکیها در این برنامه می‌توانند مشاهده و پاک شوند یا اینکه بلوکه شوند و براساس سایت مجاز به کار روند.

٦ – Hacking و Cracking

شاید این الفاظ را از جاهای مختلفی شنیده باشید. یک فایروال بخرید ولی باز هم سیستم شما می‌تواند بوسیله یک بچه ۱۳ ساله هک شود. درست است که اینترنت خیلی شلوغ و بی در و پیکر است ولی گاهی وقتها هکرها تنها کاری که می‌توانند بکنند این است که کنترل مرورگر شما را به دست گیرند یا نسخه ویندوزتان را بفهمند.

ولی اگر روی سیستمتان، فولدرهایی را بصورت Share داشته باشید و از طرفی سیستمتان هم روی اینترنت باشد و آن فولدرها هم اسم رمزی برای دسترسی نداشته باشند و تازه file and print sharing هم نصب باشد باید مطمئن باشید که بدست آوردن فایلهای روی سیستمتان مثل آب خوردن است. ولی اگر این چنین نیست هکرها نمی‌توانند به راحتی به سیستم شما وارد شوند (به قسمت Trojanها در همین مقاله مراجعه کنید). به سایت http://grc.com/It/hometouse.htm برای اطلاعات بیشتر مراجعه کنید.

اگر سیستم شما عضوی از یک شبکه مایکروسافت نیست file and printer sharing را از روی سیستم خود حذف کنید (به Control panel بروید و آیکن Network را دوباره کلیک کنید و اگر دیدید که در لیست آنرا دارید می‌توانید آنرا remove کنید). در ضمن فولدرهای share شده بی خودی را هم حذف کنید یا حداقل روی آنها یک اسم رمز ۱۰ حرفی بگذارید.

درجه خطر: ۵
file and printer sharing را روی ویندوز خود بی خودی نصب نکنید. به سایت http://www.doshelp.com/sharing.htm مراجعه کنید.

Trojans – ۷

در دنیای PC یک Trojan هر برنامه‌ای است که می‌تواند اهداف امنیتی داشته باشد و اغلب هم مشکوک می‌آید و می‌رود و از دید ما مخفی است وقتی یکی از آنها روی سیستم شما نصب باشد از طریق اینترنت دائماً با نویسنده خود تماس می‌گیرد. گاهی هم می‌تواند همچون یک Server ایفای نقش کند و بدین ترتیب کنترل سیستم شما دست سازنده Trojan می‌افتد. اولین کاری که این برنامه می‌کند این است که اسم رمزهای شما را به سمت سازنده خود می‌فرستد. معروفترین آنها Subseven است (http://www.sub7files.com) که می‌توانید جزئیات آنرا در سایت مذکور بخوانید. یک فایروال شخصی مثل ZoneAlarm (http://www.zoneAlarm.com) می‌تواند جلوی یک Trojan را بگیرد ولی یادتان باشد که این برنامه هم نمی‌تواند همه چیز را صددرصد تضمین کند. هیچ فایروالی کامل نیست و بعضی از آنها می‌توانند به راحتی دور زده شوند. ولی حواستان به برنامه‌های اینچنینی باشد. هر e-mailای که به سمت شما می‌آید می‌تواند حاوی یک Trojan باشد و برنامه‌های Shareware از یک منبع معروف مثل http://www.tucows.com هم می‌توانند حاوی Trojan باشد،هیچ مهم نیست که برنامه را از کجا Download می‌کنید.هر فایلی را که می‌گیرید اسکن کنید. cleaner (http://www.moosoft.com) برنامه خوبی برای اسکن کردن Trojanها است و ابزارهای رایگانی مثل آنچه که در سایت http://www.diamondcs.com.au است هم به دردتان خواهد خورد. با آخرین اخبار Trojanها به روز باشید (http://www.dark-e.com) و مطمئن باشید که در امان خواهید بود.

درجه خطر: ۹

فایروالهایی مثل (http://www.zonelabs.com) مقاومت خوبی در مقابل Trojanها دارند.

کتابخانه‌هایی مثل http://www.multimania.com/cdcorg/trojans.html روش خوبی برای پیداکردن روش کار اسبهای تراوا هستنند. هیچ چیزی را Download نکنید مگر اینکه دقیقاً بدانید چگونه کار می‌کند و سیستم شما را آلوده نمی‌نماید.

۸ – مردم

شما داده‌های مهمی را روی سیستم خود دارید لذا طبیعی است که بوسیله هکرها مورد توجه قرار گیرید. اما آیا مطمئن هستید که خطر در کنار خانه شما نیست؟ اگر شخصی به PC شما دسترسی داشته باشد می‌تواند بفهمد که چه سایتهایی را شما اخیراً دیده‌اید و با جمع آوری اطلاعاتی می‌تواند اسم رمز شما را هم پیدا کند یا اینکه برنامه‌ای را روی سیستم شما نصب کند که هر فشار کلید روی سیستمتان را log کند. هیچ شخصی

دوست ندارد که فکر کند فامیل، دوست یا اقوامش اینکار را می‌کنند ولی باور کنید که از این اتفاقها بارها رخ داده است.

یکی از راهها این است که به کسی اجازه دسترسی به سیستمتان را ندهید. مطمئن باشید که کامپیوترتان یک روز مثلاً به خاطر تعمیر می‌تواند به جای دیگری برود و در این صورت اطلاعات شما به راحتی لو خواهد رفت. اگر شماره‌های خصوصی خود مثل شماره اقوام یا شماره Credit card خود را روی سیستم داشته باشید و این اطلاعات به دست دیگری بیفتد، تمام است. بد نیست که روی برنامه‌هایی مثل (http://www.pc-magic.com) که اجازه مخفی کردن فولدرها و کدکردن محتویات آنها را می‌دهد سرمایه‌گذاری کنید. برنامه‌های مخفی سازی مثل (http://www.pgpi.org) هم می‌توانند مفید باشند.

برای حذف همیشه و نابود کردن برخی از فایلها که نمی‌خواهید اثری از آنها باقی بماند از برنامه‌ای مثل (http://www.tropsoft.com/pcsecurity) استفاده کنید.

۹ – نرم افزارهای مونیتورینگ

هرآنچه را که می‌خواهید می‌توانید روی PC خود انجام دهید ولی معلوم نیست که با سیستم شما وقتی که بالاسر آن نیستید چه می‌کنند. برنامه http://www.iopus.com/starr.htm یک مثال خوب از برنامه‌ای است که هرآنچه را که تایپ می‌کنید log می‌کند، هر سایتی را که می‌بینید، تبادلات اطلاعاتی در برنامه‌های messaging را برایتان نگه می‌دارد و هیچ کس هم متوجه وجود آن نمی شود. و هیچ ردپایی در Windows Task Manager نمی‌گذارد.

البته راه‌حلهای دفاع در برابر STARR هم در تئوری وجود دارد. مثلاً می‌توانید در Safe mode سیستم را بوت کنید و احتمالاً بسیاری از برنامه‌های شما دیگر load نخواهند شد و فایلهای اجرایی را روی دیسک خود پیدا کنید و آنها را rename یا Disable کنید.

درجه خطر: ۶

MSINFO32.EXE را اجرا کنید و Tools > System configuration utility > Startup را انتخاب نمائید. برنامه‌های مانیتورینگ را هم در لیست خواهید دید.

۱۰ – برنامه‌های استثمارکننده

بسیاری از افراد فکر می‌کنند که با نصب فایروال از شر حملات online در امان هستند ولی این طور نیست. هر برنامه‌ای که روی اینترنت از آن استفاده می‌کنید مثل مرورگر، IM و ... می‌توانند باگ داشته باشد. بیائید

به Ie5.5 به عنوان یک نمونه بپردازیم. اگر تنظیمات پیش فرض آنرا دست نزنید برای یک سایت امکان این وجود دارد که به فایلهای روی سیستم شما دست یابد. سایت http://www.guninski.com/scractx.html را برای جزئیات بیشتر ببینید. شاید جالب باشد که بدانید هر کسی می‌تواند یک HTML e-mail به سمت شما بفرستد که بطور اتوماتیک بدون هشدار برنامه‌ای را روی سیستم شما اجرا کند (اگر IE نسخه ۵/۰۱ یا ۵/۵ داشته باشید که بدتر هم است) سایتهای http://www.microsoft.com/technet/security/buletin/ms01-020.asp و http://www.icq.com/features/security و سایتهای دیگری مثل http://www.securityfocus.com را ببینید.