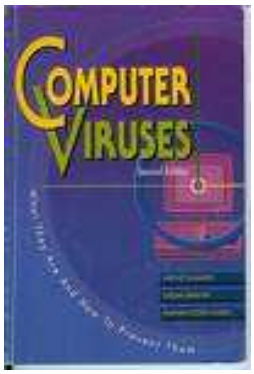
انجمن علمی مهندسی کامپیوتر - نرم افزار
دانشگاه قم
Computer Engineering Scientific Assosiation
Software
برنامه نویسی
گرافیک و انیمیشن
دروس دانشگاه
و ...

ويروس‌ها زيرك شده‌اند

اشاره :

مطالعات جديد نشان مي‌دهد ويروس‌ها و كرم‌هاي كامپيوتري، خشن‌تر شده‌اند و بيش از پيش به شكلي هدفمند، داده‌ها را به منظور كلاهبرداري درو مي‌كنند. آيا زماني را به ياد داريد كه ويروس‌ها و كرم‌هاي كامپيوتري ميليون‌ها كامپيوتر را مبتلا مي‌كردند و شبكه‌ها را به زانو درمي‌آوردند؟ اغلب اين ويروس‌ها و كرم‌ها را افراد نوجوان يا جوانان باهوش، اما ضداجتماع، مي‌نوشتند. شايد آن روزها، روزگار خوش كامپيوترها بوده‌اند.



برخلاف گذشته كه جواناني به منظور چيره شدن بر احساس پوچي در زندگي خود، آن كدها را براي حمله به سيستم‌هاي عامل مي‌نوشتند، امروزه حملات ويروسي با گسترش كمتر، اما به صورتي هدفمند، توسط جنايتكاراني اجرا مي‌شوند كه قصدشان سرقت اطلاعات، چه به صورت داده‌هاي شركتي و چه به شكل اطلاعات مربوط به حساب كاربران، به منظور كلاهبرداري است.

اين نتيجه‌گيري از بررسي‌هاي جديدي كه انستيتوي SANS و دو آژانس امنيتي دولتي، به‌نام‌هاي US-CERT در دانشگاه Carnegie Mellon شهر بيتزبورگ و National Infrustructure Security Coordinating Centre در بريتانيا، درباره بيشترين آسيب‌پذيري‌ها در سال ۲۰۰۵ انجام داده‌اند به دست آمده است.

موقعيت‌هاي خطرناك

يكي از نتايج نگران كننده به دست آمده نشان مي‌دهد كه خود نرم‌افزارهاي طراحي شده براي محافظت از داده‌ها، هدف ويروس‌ها قرار گرفته‌اند. روهيت دامانكار، مهندس امنيت در TippingPoint بخش امنيتي (Com۳) و همكار گروه ارزيابي در SANS مي‌گويد: "ما شاهد آلودگي‌اي هستيم كه نه

انجمن علمی مهندسی کامپیوتر - نرم افزار
دانشگاه قم
Computer Engineering Scientific Assosiation
Software
برنامه نویسی
گرافیک و انیمیشن
دروس دانشگاه
و ...

تنها ويندوز مايكروسافت، بلكه برنامه‌هاي ساير توليدكنندگان را نيز كه روي سيستم‌هاي متعدد نصب شده‌اند دربرمي‌گيرد."

او در ادامه مي‌گويد: "اين برنامه‌ها شامل نرم‌افزارهاي پشتيبان‌گيري، ضدويروس، بانك‌هاي اطلاعاتي و حتي پخش‌كننده‌ها مي‌شود. حفره‌هاي موجود در اين برنامه‌ها، منابع شركت‌هاي مهم را در معرض خطر قرار مي‌دهند و مي‌توانند در تمام شبكه فعاليت كنند."

اين حملات اثرات متعدد بر ايمني كامپيوترهاي خانگي، دفترهاي كاري كوچك و يا شركت‌هاي بزرگ دارند. از جمله اين اثرات، تهديد مالي جدي‌اي است كه ويروس‌ها، كرم‌ها و نظاير آن‌ها، علاوه‌بر آزار مشتريان، به وجود مي‌آورند. ديويد كول، مدير كنترل محصول در واحد عكس‌العمل امنيتي در شركت سيمانتك مي‌گويد: "اين حملات بيشتر به منظور سرقت اطلاعات مشتريان انجام مي‌شوند."

تهديدات جديد

تصور داشتن ايمني به دليل نصب آخرين وصله‌هاي سيستم عامل، تفكري خطرناك است. بايد اطمينان حاصل كنيد كه برنامه‌هاي متعلق به توليدكنندگان متعدد ديگر نيز، بروز هستند. خوشبختانه اغلب برنامه‌ها مانند Adobe Acrobat Reader و Mozilla FireFox كه هر دو در سال گذشته مورد حمله قرار گرفتند، داراي سيستم بروز رساني خودكار هستند. از آنجايي‌كه اين برنامه‌ها روي سيستم‌هاي مختلف اجرا مي‌شوند، نمي‌توانيد مطمئن باشيد كه به دليل استفاده از سيستم عامل Mac OS X يا لينوكس به‌جاي ويندوز، با خطر مواجه نيستيد.

از بيست مورد انواع آسيب‌پذيري معرفي شده در اين گزارش، نُه مورد براي حمله به سكوهاي متفاوت طراحي شده‌اند. در بين محصولات رايج، برنامه‌هاي به‌اشتراك‌گذاري فايل‌ها مانند eDonkey،kazaa، و BitTorrent از هدف‌هاي اصلي بوده‌اند. مشكل اصلي اين برنامه‌ها اين است كه فايل‌هايي كه كاربران به اشتراك گذاشته‌اند، مي‌توانند حاوي موارد خطرناك (ويروس، كرم و ...) باشند.

پخش‌كننده‌هاي آسيب‌پذير

علاوه بر پيچيدگي‌هاي موجود، برنامه‌هاي پخش رسانه، مانند Windows Media Player،RealPlayer و iTunes همگي در سال ۲۰۰۵ داراي نقاط آسيب‌پذيري بودند كه امكان نصب برنامه‌هاي مهاجم را كه براي مثال، كليدهاي صفحه كليد را مي‌خوانند و مي‌توانند كلمه عبور يا اطلاعات مربوط به حساب كاربران را به سرقت ببرند، فراهم مي‌ساخت. بنابراين اگر اين حقيقت كافي نباشد كه دريافت‌هاي غيرمجاز از اينترنت، قانوني نيست و صاحبان محتوا مي‌توانند آن را تحت پيگرد قرار دهند، خطرات ايمني دليل ديگري براي كنترل برنامه‌هاي به اشتراك گذاردن فايل‌ها محسوب مي‌شود.

سرورهاي وب

انجمن علمی مهندسی کامپیوتر - نرم افزار
دانشگاه قم
Computer Engineering Scientific Assosiation
Software
برنامه نویسی
گرافیک و انیمیشن
دروس دانشگاه
و ...

جنبه ديگر، حملات افزايش يافته از طريق سرورهاي وب است. در بدترين شكل خود، سايت‌هايي وجود خواهند داشت كه به بازديدكنندگان از طريق كشف نقاط آسيب‌پذير در مرورگرها حمله مي‌كنند. سايت‌هاي وب كه از زبان‌هاي رايج اسكريپت PHP استفاده كرده‌اند، در سال گذشته داراي بيشترين نقاط آسيب‌پذير بوده‌اند.

گذشته از سرورهاي وب، حملات بسياري از طريق ساختار بنيادي اينترنت انجام گرفته است. سه آسيب‌پذيري در بين بيست آسيب‌پذيري اصلي، مربوط به محصولات شبكه‌اي، مانند Juniper Networks، Symantec و Checkpoint Software Technologies بوده است كه براي ايمن سازي شبكه طراحي شده‌اند.

وصله كاري

درسي كه از اين گزارش گرفته مي‌شود آن است كه شايد فروشندگان اصلي سخت‌افزار و نرم‌افزار بايد از شركت‌هاي پيشرو مانند مايكروسافت و اپل پيروي كنند و سازوكاري ارائه دهند كه سيستم‌هاي آن‌ها را به طور خودكار بروزرساني كنند.

آلن پالر، مدير تحقيقات SANS مي‌گويد: "نكته نهايي اين‌كه امنيت در هيجده‌ماه گذشته، شش سال به عقب برگشته است. شش سال پيش حمله كنندگان سيستم‌هاي عامل را هدف مي‌گرفتند و توليدكنندگان، وصله‌هاي نرم‌افزاري خودكار براي آن‌ها ارائه نمي‌دادند. در اين سال‌ها پيدايش وصله‌هاي نرم‌افزاري خودكار، همگان را تحت حفاظت قرار دادند. اكنون حمله كنندگان برنامه‌هاي محبوب را مورد حمله قرار مي‌دهند. اما توليد كنندگان اين برنامه‌ها، براي آن‌ها وصله‌هاي خودكار نمي‌سازند." به‌نظر مي‌رسد توليد كنندگان، خود را به ساخت كد منبع برنامه‌ها محدود مي‌دانند.

ماهنامه شبكه

www.ComputerUnion.Blogfa.com

www.News82.Blogfa.com