شنبه 10 دی 1390 - 08:20

حلقه گمشده امنيت در دنياي ديجيتال

جام جم آنلاين: در دنياي امروز استفاده از فناوري‌هاي جديد روز به روز در حال گسترش است.

هكرها مي‌توانند از چاپگر شما يك بمب ساعتي بسازند
حلقه گمشده امنيت در دنياي ديجيتال
جام جم آنلاين: در دنياي امروز استفاده از فناوري‌هاي جديد روز به روز در حال گسترش است.

اگرچه پيش از اين مي‌توانستيم با قرار دادن اسناد و مدارك شخصي و محرمانه در مكاني امن و مطمئن امنيت شخصي را در حريم اختصاصي خود تضمين كنيم، اما متاسفانه فناوري‌هاي ديجيتال كه به يكي از نيازهاي ضروري زندگي ما مبدل شده‌اند كم‌كم به بلاي جانمان تبديل مي‌شوند، چرا كه اين فناوري‌ها دسترسي به اطلاعات شخصي و محرمانه‌اي را كه اين روزها به شيوه‌اي جديد و امروزي و در قالب مجموعه‌اي از كدهاي ديجيتالي صفر و يك ذخيره و نگهداري مي‌كنيم، تسهيل مي‌كنند و مراقبت از اطلاعات محرمانه در برابر حمله هكرها به معضلي تبديل شده كه هنوز هم راهكار مناسبي براي آن ارائه نشده است.

هكرها يا به عبارتي سارقان دنياي ديجيتال كه فرسنگ‌ها دورتر از ما زندگي مي‌كنند مي‌توانند به آساني كنترل شبكه‌هاي كامپيوتري را در دست بگيرند و به آساني با دسترسي به مشخصات افراد مرتكب سرقت هويتي شوند. محققان دانشگاه كاليفرنيا بتازگي موفق به شناسايي موج جديدي از حمله هكرها به كامپيوترها و سيستم‌هاي ارتباطي كامپيوتري شده‌اند كه مي‌تواند تهديدي جدي عليه امنيت اعضاي شبكه‌هاي ارتباطي باشند و امنيت بيش از ميليون‌ها كاربر حقيقي يا حقوقي و حتي شركت‌هاي دولتي را در معرض تهديد قرار دهند. براساس خبر جديدي كه براي نخستين‌بار در وب‌سايت رسمي شركت مايكروسافت گزارش شده است، اين گروه از مجرمان كامپيوتري از طريق شبكه اينترنت و از راه دور كنترل چاپگرها را در دست مي‌گيرند و از آنها به عنوان ابزاري براي سرقت اطلاعات شخصي افراد استفاده مي‌كنند.

ارسال كدهاي مخرب امنيتي براي نفوذ به سيستم

به گفته محققان، اين جريان ضدامنيتي مي‌تواند با ارسال دستوراتي مبني بر افزايش ناگهاني دما در بخشي از چاپگر همراه باشد كه جوهر را در سطح كاغذ خشك مي‌كند و در نهايت موجب سوختن كاغذ خواهد شد. اگرچه اغلب چاپگرها مجهز به يك سوئيچ حرارتي هستند كه در صورت لزوم با خاموش كردن چاپگر مانع از سوختن كاغذ مي‌شوند، اما در حقيقت در اينجا چاپگرها مي‌توانند واسطه‌اي براي ايجاد خسارت‌هاي هنگفتي در شبكه‌هاي بزرگ ارتباطي باشند. در اغلب موارد، تنظيمات نصب و راه‌اندازي چاپگرها به گونه‌اي انجام مي‌شود كه مي‌توان از طريق شبكه نيز دستور چاپ اسناد يا اطلاعات خاصي را اجرا كرد و به اين ترتيب مي‌توان همزمان يك ويروس كامپيوتري را نيز با ارسال اين پيام وارد سيستم كرد. به عبارت ديگر، به كمك اين روش اين امكان وجود خواهد داشت كه بتوان از راه دور و بدون اين‌كه هرگونه اختلالي در سيستم ايجاد شود، يك سيستم كامپيوتري يا حتي يك شبكه را تحت كنترل قرار داد و به اطلاعات آن دسترسي داشت. در حقيقت مي‌توان فناوري‌هاي ديجيتالي را شبيه به خودروهايي دانست كه مالكان آنها به دليل در دست نداشتن كليد قفل آنها نمي‌توانند استفاده از آن را به انحصار خود درآورند. به اين ترتيب چنين روشي، روش امن و مطمئني براي حفاظت از اسناد و اطلاعات محرمانه نخواهد بود.

اين گروه از هكرها مي‌توانند چاپگرها را با ارسال يك كد مخرب ويران كنند. با ارسال اين كد ضدامنيتي و نصب يك نرم‌افزار دائمي در سيستم كه تنها 30 ثانيه زمان مي‌برد، يك ويروس كامپيوتري به شبكه راه مي‌يابد كه پس از نصب، امكان شناسايي آن وجود نخواهد داشت مگر اين‌كه تراشه يا چيپ را از سيستم خارج كرده و آن را مورد بررسي و بازبيني دقيق قرار دهيم. هيچ‌يك از انواع نرم‌افزارهاي ضدويروسي پيشرفته و جديد نيز توانايي تشخيص و از كارانداختن اين نرم‌افزار را كه در تراشه داخلي چاپگر نصب و راه‌اندازي مي‌شود نخواهند داشت. اگرچه شايد اين موضوع تا به حال كمتر مورد توجه قرار گرفته باشد، اما در حقيقت چاپگرها نيز در يك شبكه ارتباطي همانند يك سيستم كامپيوتري مجزا عمل مي‌كنند كه ممكن است با مشكلات مشابهي در سيستم‌هاي ارتباطي مواجه شده و از تاثيرات مشابهي بر عملكرد ديگر سيستم‌هاي ديجيتالي تعبيه شده در يك شبكه ارتباطي برخوردار باشند.

ميليون‌ها چاپگر در معرض خطر هستند

براساس بررسي‌هاي انجام شده از آنجا كه اين ويروس مخرب ضدامنيتي تنها مي‌تواند در عملكرد پرينترهاي ليزري اختلال ايجاد كند و اغلب كاربران خانگي از چاپگرهاي جوهرافشان براي رفع نيازهايشان استفاده مي‌كنند مي‌توان آسيب‌پذيري چاپگرها در برابر موج

جديد حمله هكرها به شبكه‌هاي ارتباطي را تنها محدود به گروه خاصي از كاربران شركت‌هاي بزرگ تجاري دانست.

نكته: هكرها يا به عبارتي سارقان دنياي ديجيتال كه فرسنگ‌ها دورتر از ما زندگي مي‌كنند مي‌توانند به آساني كنترل شبكه‌هاي كامپيوتري را در دست بگيرند و به آساني با دسترسي به مشخصات افراد مرتكب سرقت هويتي شوند
البته بايد اين نكته را نيز مد نظر قرار داد كه از سال 1984 (1363) تاكنون بيش از 100 ميليون چاپگر ليزري در سطح دنيا به فروش رفته است و به عبارتي مي‌توان گفت تعداد زيادي از كاربران در معرض خطري از جانب هكرها هستند كه شايد برايشان بسيار گران تمام شود. پس از اين كه چاپگر يك شبكه ارتباطي به اين ويروس آلوده شد با ارسال كد مخرب به كامپيوترهاي شبكه، مجموع سيستم‌هاي مرتبط در اين شبكه را تحت تاثير قرار مي‌دهد. به اين ترتيب به مجموعه‌اي از اطلاعات شخصي كاربران نظير شماره كارت شناسايي و يا اطلاعات مربوط به شماره حساب آنها دسترسي پيدا مي‌كند. اگر يك هكر تنها به دنبال اين باشد كه در عملكرد يك شبكه ارتباطي اختلال ايجاد كند، با اين روش و تنها با ارسال يك برنامه نرم‌افزاري به منظور ارتقاي سيستم مي‌تواند هزاران و يا ميليون‌ها سيستم ديجيتالي را كه در برابر نفوذ اين برنامه مخرب آسيب‌پذير هستند از كار بيندازد. جالب است بدانيد كه حتي پرينترهاي كاربران خانگي كه به طور مستقيم به شبكه اينترنت متصل نباشند هم در معرض خطر حمله اين گروه از هكرها قرار دارند. چراكه تنها ارتباط بين كامپيوتر و پرينتر براي نفوذ هكرها كافي است. محققان در يك بررسي آني و لحظه‌اي بيش از 40 هزار سيستم ارتباطي ديجيتالي را شناسايي كرده‌اند كه تنها در مدت زمان چند دقيقه مورد حمله اين ويروس ضدامنيتي قرار گرفته‌اند.

همان‌طور كه مي‌بينيد، هكرها اين توانايي را دارند كه در مدت زمان كوتاهي به هر ابزار الكترونيكي حمله كرده و از اطلاعات سرقت شده عليه خودتان استفاده كنند. خودروها، تلفن‌هاي همراه، سيستم‌هاي امنيتي خانگي، سيستم‌هاي موقعيت‌ياب جهاني (GPS) و حتي دوربين‌هاي ديجيتال، چاپگرها و پريزهاي برق از جمله آسيب‌پذيرترين تجهيزات در برابر حمله هكرهاي اينترنتي هستند، به‌رغم تلاش‌هاي گسترده هنوز هيچ روش مطمئني براي رفع مشكل امنيتي سيستم‌هاي الكترونيكي و ديجيتالي وجود ندارد. برخلاف آن كه به نظر مي‌رسد چاپگر ليزري روي ميز كارتان يك وسيله الكترونيكي كاربردي و ايمن باشد با نفوذ هكرها اين چاپگر ساده بي‌خطر به نظر مي‌رسد، مي‌تواند همچون يك بمب ساعتي منفجر شود. در حقيقت چاپگرها اين روزها به يك پتانسيل بالقوه براي ايجاد حريق از راه دور مبدل شده‌اند كه پس از نفوذ به مخزن اطلاعاتي و سرقت داده‌هاي ثبت شده موجب آتش‌سوزي مي‌شوند.

يكي از ويژگي‌هاي چاپگرها اين است كه همزمان با دريافت دستور چاپ از طريق شبكه يا سيستم به روزرساني مي‌شوند و متاسفانه تنها مقدار محدودي از چاپگرها اين توانايي را دارند كه بتوانند صحت برنامه به روزرساني را پيش از اجراي آن مورد بررسي قرار دهند. به اين ترتيب يك برنامه تقلبي براي به روزرساني مي‌تواند به سادگي و از طريق يك فايل مخرب امنيتي به چاپگر ارسال شود و از آنجا كه نرم‌افزارهاي امنيتي كه روي كامپيوترها نصب مي‌شوند قابليت بررسي وضعيت چاپگرها را ندارند، هكرها براي به دست گرفتن كنترل چاپگرها در مقايسه با ديگر اجزاي شبكه‌هاي اينترنتي از آزادي عمل بيشتري برخوردار خواهند بود. اگرچه اغلب چاپگرهايي كه در 2 سال اخير به بازار عرضه شده‌اند داراي امضاي ديجيتالي هستند كه تاييد آن براي نصب برنامه‌هاي به روزرساني از طريق اينترنت الزامي است، اما با اين حال امنيت چاپگرها موضوعي است كه اين روزها نگراني‌هاي بسياري را به همراه داشته است.

به نظر مي‌رسد در آينده‌اي نه‌چندان دور با پيشرفت علم پزشكي در زمينه استفاده از ابزارهايي كه واسط ميان انسان و ماشين‌آلات الكترونيكي باشند هكرها بتوانند حتي اطلاعاتي را كه در حافظه انسان‌ها ثبت شده‌اند را نيز هدف حملات خود قرار دهند. مسلم است كه در نهايت پيشرفت‌هاي به دست آمده در تكنيك‌ها و روش‌هاي هك اطلاعاتي، به ربودن مستقيم اطلاعات از مغز انسان‌ها و نفوذ به مغز آنها منتهي خواهد شد. اگرچه كنترل مغز انسان‌ها توسط تبهكاران بيشتر به داستان‌هاي علمي ـ تخيلي شباهت دارد، اما بايد پذيرفت كه در دنيا امكان هك شدن هر چيزي وجود دارد و اين همان چيزي است كه موجب بيم و هراس انسان‌ها از تاثير پيشرفت‌هاي علمي در زندگي آينده خواهد شد.

منبع: Msnbc

فرانك فراهاني‌جم / جام جم