پنجشنبه 08 مهر 1389 - 08:12

روش مقابله با کرم جاسوس اطلاعات

کرم Stuxnet بدافزاري است که چنان در استفاده از آسيب پذيري هاي اصلاح نشده ماهر است...

کرم Stuxnet بدافزاري است که چنان در استفاده از آسيب پذيري هاي اصلاح نشده ماهر است و چنان در کار خود پيچيده عمل مي کند که آن دسته از متخصصان امنيتي که در مورد آن تحقيق کرده اند، معتقدند که ممکن است اين بدافزار کار متخصصاني با پشتوانه قوي و با انگيزه خاص باشد.
به گزارش مهر، نسخه ابتدايي استاکس نت نخستين بار يک و نيم سال پيش از سوي يک شرکت کوچک امنيتي در بلاروس گزارش شد و يک ماه بعد از آن نيز تاييد شد که اين کرم در حال هدف قرار دادن سيستم هاي ويندوز در مديريت سيستم هاي کنترل صعنتي بزرگ است اما شرکت هاي معروف دنيا که عليه بدافزارها کار مي کنند در مورد اين بدافزار که آن زمان از آسيب پذيري هاي ساده تري استفاده مي کرد در مورد آن اطلاع رساني عمومي نکرده و اقدامي خاصي در اين باره انجام ندادند.
سيستم هاي کنترل صنعتي اغلب با عنوان اسکادا شناخته مي شوند و هر چيزي را از سايت هاي نيروگاهي گرفته تا خطوط انتقال نفت کنترل مي کنند و طبق اعلام رسمي، ايران جدي ترين هدف اين کرم بوده و براساس اولين آمار ارائه شده در دو ماه پيش نزديک به 60 درصد از تمامي سيستم هاي آلوده به اين ويروس در ايران قرار داشتند.
به همين دليل به نظر مي رسد اين ويروس با اهدافي خاص نيروگاههاي اتمي ايران را مورد هدف قرار داده است. استاکس مي تواند به طور همزمان از چهار آسيب پذيري براي دسترسي به شبکه هاي رايانه اي استفاده کند و به اعتقاد کارشناسان پيش از اين ديده نشده که يک بدافزار به طور همزمان از چهار آسيب پذيري اصلاح نشده استفاده کند.
ساماندهي و پيچيدگي اين بدافزار به حدي قابل توجه و اعجاب انگيزاست که محققان معتقدند که کساني که پشت اين بدافزار قرار دارند، قصد دارند به تمام دارايي هاي شرکت يا شرکت هاي هدف خود دست يابد. همچنين محققان امنيتي براين باورند که تيمي متشکل از افرادي با انواع تخصص ها و پيش زمينه هاي صنعتي و IT اين بدافزار را ايجاد کرده و هدايت مي کنند.
کارشناسان معتقدند که سطح بالايي از تخصص صنعتي در نوشتن اين ويروس مورد استفاده قرار گرفته است و به همين دليل انگيزه عادي يا کسب درآمد در نوشتن آن مطرح نبوده است. به همين دليل است که گفته مي شود يک سازمان يا يک دولت متخاصم عليه ايران ممکن است دست به اين اقدام سايبري زده باشد.
به اعتقاد کارشناسان استاکس نت بسيار پيچيده و در سطح بالايي از تکنولوژي قرار دارد که در نوع خود بي نظير است. شايد به تعبيري اين کرم جاسوسي اولين نمونه ويروسي باشد که به صنعت حمله کرده و خاص صنعت طراحي شده و قويترين بدافزار تاريخ است.
اما با اين وجود مسئولان شرکت فناوري اطلاعات کشور معتقدند که اين کرم جاسوسي نه تنها تهديدي براي سيستم هاي صنعتي کشور محسوب مي شود بلکه تهديدي براي بيش از يک سوم جمعيت کشور که کاربران اينترنت را تشکيل مي دهند نيز است.

استاکس نت در کمين رايانه هاي شخصي
معاون شرکت فناوري اطلاعات ايران با تاکيد بر اينکه ويروس رايانه اي استاکس نت که چندي است رايانه هاي ايراني را مورد حمله قرار داد تنها محيط صنعتي را تهديد نمي کند ، گفت: اين ويروس نقاط ضعفي را در کامپيوترهاي آلوده ايجاد مي کند که امکان دسترسي به اطلاعات رايانه کاربران را از راه دور فراهم مي سازد.
حميد عليپور اظهار داشت: کرم جاسوسي استاکس نت بسيار خطرناک است و به رغم اينکه محيط هاي صنعتي را مورد حمله قرار مي دهد ، کاربراني که در منزل از رايانه استفاده مي کنند و يا شرکت هاي دولتي و خصوصي نيز در معرض تهديد اين ويروس قرار دارند.
وي با تاکيد بر اينکه معمولا مهاجمين به اطلاعات اجازه دسترسي به راههاي نفودي که در رايانه ها باز کرده اند را به ديگران نمي دهند و با سرورهاي مياني و روش هاي کد شده سعي مي کنند اين راه هاي نفوذ را حفاظت کرده و تنها خود از اين کامپيوترهاي آلوده استفاده کنند، اضافه کرد: اما آنچه که در اين ويروس تعجب آور است اين است که راههاي نفوذ در دسترس است و هر فردي که کوچکترين اطلاعاتي از هک و جاسوسي الکترونيک داشته باشد مي تواند از کامپيوتر آلوده سوء استفاده کند.
معاون شرکت فناوري اطلاعات گفت: اين به اين معنا است که دري روي رايانه هاي آلوده باز شده که از طريق اينترنت امکان حمله به رايانه توسط گروهي به جز مهاجمين استاکس نت را فراهم کرده است.
عليپور گفت: با بيان اينکه اگرچه تهديد اوليه اين ويروس در ايران بوده اما با توجه به رشد و نفوذي که در سطح دنيا داشته اين بدافزار از کنترل خارج شده و در جاهاي ديگر دنيا هم در حال توسعه يافتن است.

نحوه عملکرد ويروس استاکس نت
معاون شرکت فناوري اطلاعات در پاسخ به اين سئوال که اين جاسوس رايانه اي چه اطلاعاتي از کاربران خانگي را به سرقت خواهد برد ، گفـت: به نظر نمي رسد هدف اوليه نويسنده اين بدافزار سرقت اطلاعات کارت هاي اعتباري کاربران خانگي بوده باشد اما اين

امكان به وجود آمده كه هر كامپيوتر آلوده به اين ويروس نه تنها از سوي نويسنده اين بدافزار بلكه توسط هر فردي كه اطلاعات آن را در اينترنت خوانده و نحوه استفاده از آن را ياد گرفته باشد مورد سوء استفاده قرار گيرد.
وي تصريح كرد: جزئيات فعلي اين بدافزار در وب سايت ماهر «مركز مديريت امداد و هماهنگي عمليات رخداد رايانه‌اي» به نشاني www.certcc.ir آمده و مجموعه اي از اخبار و اطلاعات و مقالات در بخش توصيه هاي امنيتي اين سايت خاص اين ويروس گذاشته شده است.
عليپور با تاكيد بر اينكه نحوه پاكسازي رايانه ها در سايت ماهر توضيح داده شده و تمامي اطلاعات بروزرساني مي شود تا كاربران عام در جريان قرار گيرند ، افزود: در زمان حاضر اكثر نرم افزارهاي ضد بدافزار و ويروس كش هاي مختلف قابليت پاكسازي ويروس استاكس نت را دارند و اگر كاربران از نرم افزارهاي بروز شده ضد ويروس كه قابليت شناسايي داشته باشد استفاده مي كنند مي توانند با اين بدافزار مقابله كنند.
وي با بيان اينكه ليست بدافزارهايي كه قابليت شناسايي آنها وجود دارد روي سايت مركز ماهر قرار دارد به مهر گفت: برخي از نرم افزارهاي ويروس كش براي كاربران خانگي قابل دانلود و رايگان است.
معاون شركت فناوري اطلاعات با اشاره به ديگر نكات لازم براي رعايت كاربران خاطرنشان كرد: كاربران سعي كنند با حداقل سطح دسترسي وارد كامپيوترشان شوند. كساني كه با سيستم عامل لينوكس كار مي كنند اين موضوع را رعايت مي كنند اما كاربراني كه از سيستم عامل ويندوز استفاده مي كنند بايد اين موارد را بيشتر رعايت كنند.
وي افزود: متاسفانه كاربران ويندوز كه اكثر كاربران كشور ما را تشكيل مي دهند عادت دارند كه يا به اسم مدير سيستم وارد كامپيوتر مي شوند و يا به كلمه عبوري كه براي خود ايجاد كرده اند اختيارات مدير سيستم را مي دهند كه اين موضوع بسيار خطرناك است. به همين دليل به كاربران توصيه مي شود دو كلمه عبور براي سيستم خود ايجاد كنند كه به يكي از آنها اختيارات سطح بالاي دسترسي و مدير سيستم را بدهند و به كلمه عبور ديگر اين اختيار را ندهند.

توصيه اي براي زمان اتصال به اينترنت
وي اضافه كرد: توصيه امنيتي اين است كه كاربران در حالت عادي بخصوص وقتي مي خواهند به اينترنت وصل شوند و يا حافظه جانبي مثل فلش و كول ديسک و هارد اكسترنال به سيستم وصل كنند با حداقل سطح دسترسي لازم براي كار با كامپيوتر وارد سيستم شوند و زماني كه لازم است نرم افزاري نصب شود يا سطح دسترسي بالاتر در حد مدير سيستم باشد با كلمه عبور با احتياط بالاتر وارد سيستم شوند.
عليپور اضافه كرد : به اين ترتيب ويروس ها نمي توانند درايورهاي خود را روي سيستم نصب كنند و حداكثر اگر كامپيوتر را آلوده كرده باشند با يک خاموش روشن شدن سيستم اين ويروس پاک مي شود. چون ويروس نتوانسته خود را در نقاط كليدي سيستم كپي كند.
وي گفت: در مورد استاكس نت اگر كلمه عبور مديريت سيستم نباشد كامپيوتر اگر آلوده نشده باشد امكان آلوده شدن آن نيست. چون اين ويروس درايورهايي را روي سيستم نصب مي كند كه براي نصب آنها نياز به اختيارات مدير سيستم دارد. پس كاربران اين توصيه امنيتي را جدي بگيرند.نشانه ها و علائم مورد حمله قرارگرفتن سيستم ها روي سايت مركز ماهر موجود است و ضمن اينكه يک فايل اجرايي كوچک توسط مراكز آپاي دانشگاه شريف و اميركبير نوشته شده و روي وبسايت ماهر قابل دانلود شدن است.
معاون شركت ديتا با بيان اينكه طبق آمارهاي اعلام شده 8 هزار IP آلوده به اين ويروس در داخل ايران شناسايي شده است ، گفت: با وجودي كه سيستم هاي داخل كشور ترجمه آدرس مي شوند و از آدرسهاي خصوصي به جاي آدرس عمومي استفاده مي شود به طور قطع تعداد آلودگي بسيار بيشتر از اين رقم است.
وي با تاكيد بر اينكه در حال مشاهده ، شناسايي و كنترل كامپيوترهاي آلوده به اين بدافزار هستيم گفت: سعي داريم در برنامه ريزي انجام شده آن را كاهش دهيم.
عليپور اضافه كرد: برنامه حذف اين ويروس براي مدت دو ماه بود كه با توجه به اينكه اين ويروس در حال تغيير و تحول است و نسخه هاي جديدتر و خطرناكتر آن نيز در حال انتشار است اين زمان تغيير يافت. اما در صورتي كه ديگر شاهد تغييراتي در اين ويروس نباشيم اميدواريم بتوانيم برنامه دو ماهه را براي آن پياده سازي كنيم و آلودگي را به سطح قابل قبولي كاهش دهيم.
وي تصريح كرد: سطح آلودگي در كنترل و كاهش قرار دارد و اقداماتي براي پاكسازي آغاز شده اما بايد توجه داشت كه ويروس كار را رها نكرده و نسخه هاي جديدتري را به سمت اهداف خود مي فرستد.
به گفته اين مقام مسئول ، تمامي اقدامات در كشور براي پاكسازي و كنترل اين ويروس هماهنگ و مشترک و با مركزيت مركز ماهر به عنوان CERT هماهنگ كننده در جريان است.