بسم الله الرحمن الرحیم

مقدمه ای بر ویروسها
و
برنامه های مخرب

منبع:

Ostad Online
training on the web

مقدمه

باز هم مانند همیشه لذت به نتیجه رسیدن، را فقط مدیون لطف و مرحمت او مي‌دانم. لذت كاري كه با علاقه آن را آغاز نمودم و تا پایان مصمم پیش رفته‌ام . از اینكه همراه من بودي و تنهایم نگذاشتي، از تو سپاسگذارم. موفقیتهاي كوچك و بزرگم را فقط مدیون لطف و بزرگواري تو مي دانم.

امیدوارم مطالعه این دوره آموزشی برای خوانندگان عزیز خالی از لطف نباشد.

آرش رضاپورخان

فصل اول

اهداف

در این دوره آموزشی تنها به ارائه ی کلیات مطالب پرداخته شده است . مباحث شامل سه فصل از مطالب کلی و نیز آشنایی با برنامه های مخرب می باشد . در فصولی که متعاقبا جهت تکمیل دروس این دوره ارائه خواهد گردید به مباحث گوناگونی از جمله : شرح کامل چند ویروس معروف ، نحوه مقابله و پاکسازي آنها ، تجزیه و تحلیل کد سورس بعضي از ویروسهاي قدیمي که هنوز هم در بعضي سیستمها دیده مي‌شوند و نیز اطلاعات و نتایج به دست آمده از مراکز و گروههاي مختلف تحقیقاتي کامپیوتري ، پرداخته خواهد شد .

ویروس کامپیوتری چیست؟

ویروس کامپیوتر برنامه‌اي است که مي‌تواند نسخه‌هاي اجرایي خود را در برنامه‌هاي دیگر قرار دهد. هر برنامه آلوده مي‌تواند به نوبه خود نسخه‌هاي دیگري از ویروس را در برنامه‌هاي دیگر قرار دهد. برنامه‌اي را برنامه ویروس می نامیم که همه ویژگیهاي زیر را داراباشد:
۱) تغییر نرم افزارهایي که به برنامه ویروس متعلق نیستند با چسباندن قسمتهایي از این برنامه به برنامه‌هاي دیگر
۲) قابلیت انجام تغییر در بعضي از برنامه‌ها.
۳) قابلیت تشخیص این نکته که برنامه قبلاً دچار تغییر شده است یا خیر.
۴) قابلیت جلوگیري از تغییر بیشتر یك برنامه در صورت تغییراتی در آن بواسطه ی ویروس .
۵) نرم افزارهاي تغییر یافته ویژگیهاي ۱ الي ۴ را دارا هستند . اگر برنامه‌اي فاقد یك یا چند ویژگی از ویژگیهای فوق باشد، نمی توان به طور قاطع آنرا ویروس نامید .

آشنایی با انواع مختلف برنامه‌های مخرب

E-mail virus

ویروسهایي که از طریق E-mail وارد سیستم مي‌شوند معمولاً به صورت مخفیانه درون یك فایل ضمیمه شده قرار دارند که با گشودن یك صفحه ی HTML یا یك فایل قابل اجراي برنامه‌اي (یك فایل کد شده قابل اجرا) و یا یك word document می توانند فعال شوند.

Marco virus

این نوع ویروسها معمولاً به شکل ماکرو در فایلهایي قرار می گیرند که حاوي صفحات متني (word document) نظیر فایلهاي برنامه‌هاي Ms office (همچون word microsoft و Excel)هستند .

توضيح ماكرو: نرم افزارهايي مانند microsoft word و Excel اين امكان را براى كاربر بوجود مى آورند كه در صفحه متن خود ماكرويي ايجاد نمايد،اين ماكرو حاوي يكسري دستور العملها، عمليات و يا keystroke ها است كه تماماً توسط خود كاربر تعيين ميگردند.
ماكرو ويروسها معمولاً طوري تنظيم شده‌اند كه به راحتي خود را در همه صفحات متني ساخته شده با همان نرم افزار (Excel , ms word) جاي مي‌دهند.

اسب تروآ:

اين برنامه حداقل به اندازه خود اسب تروآي اصلي قدمت دارد . عملكرد اين برنامه‌ها ساده و در عين حال خطرناك است.
در حاليكه كاربر متوجه نيست و با تصاوير گرافيكى زيبا و شايد همراه با موسيقى محسور شده ، برنامه عمليات مخرب خود را آغاز مى كند.
براي مثال به خيال خودتان بازي جديد و مهيجي را از اينترنت Download كرده‌ايد ولي وقتي آنرا اجرا مي‌كنيد متوجه خواهيد شد كه تمامى فايلهاي روي هارد ديسك پاك شده و يا به طور كلي فرمت گرديده است.

كرمها (worm)

برنامه كرم برنامه‌اي است كه با كپي كردن خود توليد مثل مي‌كند. تفاوت اساسي ميان كرم و ويروس اين است كه كرمها براي توليد مثل نياز به برنامة ميزبان ندارند. كرمها بدون استفاده از يك برنامة حامل به تمامي سطوح سيستم كامپيوتري «خزيده» و نفوذ مي‌كنند. راجع به اينگونه برنامه ها در فصل سوم مفصلا بحث خواهد شد.

ويروسهاي بوت سكتور و پارتيشن

Boot sector قسمتى از ديسك سخت و فلاپي ديسك است كه هنگام راه اندازى سيستم از روي آن به وسيله كامپيوتر خوانده مي‌شود. Boot Sector يا ديسك سيستم ، شامل كدي است كه براي بار كردن فايلهاي سيستم ضروري است. اين ديسكها داده هايى در خود دارند و همچنين حاوي كدي هستند كه براي نمايش پيغام راه اندازى شدن كامپيوتر بوسيله ى آن لازم است .
سكتور پارتيشن اولين بخش يك ديسك سخت است كه پس از راه‌اندازي سيستم خوانده مي‌شود. اين سكتور راجع به ديسک اطلاعاتي نظير تعداد سكتورها در هر پارتيشن و نيز موقعيت همه ى پارتيشن‌ها را در خود دارد.
سكتور پارتيشن، ركورد اصلي راه‌اندازي يا Master Boot Record -MBR نيز ناميده مي‌شود.
بسياري ازكامپيوترها به گونه اى پيكربندي شده‌اند كه ابتدا از روي درايو: A راه‌اندازي ميشوند. (اين قسمت در بخش Setup سيستم قابل تغيير و دسترسي است) اگر بوت سكتور يك فلاپي ديسك آلوده باشد، و شما سيستم را از روي آن راه‌اندازي كنيد، ويروس نيز اجرا شده و ديسك سخت را آلوده مي‌كند.
اگر ديسكى حاوي فايلهاي سيستمي هم نبوده باشد ولي به يك ويروس بوت سكتوري آلوده باشد وقتى اشتباهاً ديسكت را درون فلاپي درايو قرار دهيد و كامپيوتر را دوباره راه‌اندازي كنيد پيغام زير مشاهده مي‌شود. ولي به هر حال ويروس بوت سكتوري پيش از اين اجرا شده و ممكن است كامپيوتر شما را نيز آلوده كرده باشد.
Non-system disk or disk error
Replace and press any key when ready

كامپيوترهاي بر پايه Intel در برابر ويروسهاي Boot Sector و Partition Table آسيب پذير هستند. تا قبل از اينكه سيستم بالا بيايد و بتواند اجرا شود صرفنظر از نوع سيستم عامل مى تواند هر كامپيوترى را آلوده سازد.

HOAX (گول زنك‌ها)

اين نوع ويروسها در قالب پيغامهاي فريب آميزي ، كاربران اينترنت را گول زده و به كام خود مي‌كشد. اين نوع ويروسها معمولاً به همراه يك نامه ضميمه شده از طريق پست الكترونيك وارد سيستم مي‌شوند. متن نامه مسلماً متن مشخصي نيست و تا حدودي به روحيات شخصي نويسنده ويروس بستگی دارد، پيغامها می توانند مضمونی تحديد آميز يا محبت آميز داشته باشند و يا در قالب هشداری ، مبنی بر شيوع يک ويروس جديد ئر اينترنت ، يا درخواستی در قبال يک مبلغ قابل توجه و يا هر موضوع وسوسه انگيز ديگر باشد . لازم به ذكر است كه همه اين نامه‌ها اصل نمي‌باشند يعني ممكن است بسياری از آنها پيغام شخص سازنده ويروس نباشند بلكه شايد پيغام ويرايش شده يا تغيير يافته از يك كاربر معمولي و يا شخص ديگري باشد كه قبلا اين نامه‌ها را دريافت كرده و بدينوسيله ويروس را با پيغامي كاملاً جديد مجدداً ارسال مي‌كند.
نحوه تغيير پيغام و ارسال مجدد آن بسيار ساده بوده ، همين امر باعث گسترش سريع Hoaxها شده، با يك دستور Forward مي‌توان ويروس و متن تغيير داده شده را براي شخص ديگري ارسال كرد. اما خود ويروس چه شكلي دارد؟ ويروسي كه در پشت اين پيغامهاي فريب آميز مخفي شده مي‌تواند به صورت يك بمب منطقي ، يك اسب تروا و يا يكي از فايلهاي سيستمي ويندوز باشد. شيوه‌اي كه ويروس Magistre-A از آن استفاده كرده و خود را منتشر مي‌كند.

SULFNBK يك ويروس، يك شوخي و يا هردو؟!

سايت خبري سافس چندي پيش خبري مبني بر شناخته شدن يك ويروس جديد منتشر كرد، ويروسي با مشخصه SULFNBK (SULFNBK.EXE)كه ممكن است نام آن اغلب برای شما آشنا باشد .

SULFNBK.EXE نام فايلي در سيستم عامل ويندوز ۹۸می باشد كه وظيفه بازيابي اسامي طولاني فايلها را به عهده دارد و در سيستم عامل ويندوز ۹۸ فايلی سودمند می باشد .
اينجاست كه می توان به مفهوم واقعی HOAX ها پی برد ، فايل SULFNBK.EXE كه معمولا از طريق پست الكترونيكی به همراه يک نامه ی فريب آميز و شايد تهديد آميز به زبان پروتكلی وارد سيستمها می شود دقيقا در جايی ساكن می شود كه فايل سالم SULFNBK.EXEدر آنجاست به بيان بهتر اينكه جايگزين آن فايل سالم می شود. فايل SULFNBK.EXE آلوده در شاخه Command ويندوز ۹۸ ساكن شده و چون به همان شكل و سايز مي‌باشد به همين منظور كاربر متوجه حضور يك ويروس جديد در سيستم خود نخواهد شد ، اينجاست كه فريب خورده، ويروس خطرناك Magistre-A كه در هسته اين فايل وجود دارد در اول ماه ژوين فعال شده و سازنده خود را به مقصودش مي‌رساند. نسخه‌اي ديگر از اين ويروس را مي‌توان يافت كه در ۲۵ ماه مي فعال می شود. تفاوتي كه اين ويروس نسخه قبلي خود دارد آنست كه روي فايل SULFNBK.EXE آلوده در درايو C ساكن مي‌شود. لازم به ذكر است اين ويروس در سيستم عامل ويندوز ۹۸فعال شده و حوزه فعاليتش در درايو C مي‌باشد.
تشخيص اينكه فايل SULFNBK.EXE واقعاً آلوده است يا خير دشوار می باشد . البته شايد بعد از ماه ژوئن ۲۰۰۲ از طريق ويروس يابهای جديد مانند Norton Mcafee بتوان آنها را تشخيص داد ، اما در صورت در سترس نبودن ويروس يابهای مذكور ، حداقل می توان SULFNBK.EXE را چه آلوده و چه غير آلوده پاک كرد ، البته از آنجايي كه فايل SULFNBK.EXE يك فايل سيستمي ويندوز به شمار مي‌رود ممكن است پاك كردن آن به سيستم عامل لطمه وارد كند، از اينرو بد نيست قبل از پاك كردن، نسخه‌اي از آن را بر روي يك فلاپي كپي كرده و نگه داريم. حقيقت آنست كه كمتر كسي ريسک می كند و اين قبيل فايلها را اجرا می كند .
پيغامي كه ضميمه اين فايل ارسال مي‌شود نيز در چندين نسخه وجود دارد. همانطور كه قبلا ذكر شد نسخه ی اصل پيغام به زبان پرتغالي است اما ترجمه ی انگليسي و اسپانيولي آن ميز يافت شده است .
به هرحال هر ويروس چه از نوع HOAX باشد و چه از انواع ديگر، مدتی چه طولانی و چه كوتاه روي بورس است و معمولاً لطمه‌هاي جبران ناپذير خود را در همان بدو تولد به جاي گذاشته و بعد

از مدتي مهار مي‌شود . نكته ی قابل توجه اينست كه با داشتن خداقل آشنايی از اين ويروسها در همان شروع كار به راحتی مي‌توان با نسخه‌هاي جديدتر آن ويروس و يا ويروسهاي مشابه مبارزه كرد.

CELLSAVER يك اسب تروا

a.k.a CellSaver- Celcom Screen Saver نير ويروسي از نوع HOAX مي‌باشد و عليرغم مدت زيادی كه از اولين انتشار آن می گذرد كاربران زيادی را دچار مشكل ساخته است . اين ويروس برای كاربران اينترنت ارسال شده است . نسخه نخست آن در سال ۱۹۹۸ و نسخه جديدتر آن كمي بعد در آوريل ۱۹۹۹ به همراه يك پيغام دروغين منتشر شد.
هرگاه نامه‌اي با عنوان CELLSAVER.EXE به همراه فايلي با همين نام دريافت كرديد سريعا آنرا پاك كرده و از Forward كردن براي شخصی ديگر بپرهيزبد ،اينكار هيچ گونه لذتي نداشته ، فقط به انتشار و بقای بيشتر آن كمك می كند .
اين فايل يك اسب تروا كامل مي‌باشد ، يك فايل Screen Saver زيبا براي ويندوز كه به محض اجرا شدن هر كسي را مجذوب و مسحور مي‌گرداند.
احتياط كنيد! CELLSAVER.EXE به محض اجرا شدن ، يك گوشي تلفن بي‌سيم Nokia را بصورت يک Screen Saver بر روی صفحه نمايش نشان مي دهد . در صفحه نمايش اين گوشي، می توان زمان و پيغامهارا ديد. بعد از يكبار اجرا شدن، ويروس فعال شده و شما خيلي زود متوجه خواهيد شد كه سيستم بسيار كند عمل كرده ، قادر به بوت شدن نخواهد بود و اطلاعات رود هارد ديسك نيز پاكسازي مي‌شوند .در نتيجه مجبور به نصب مجددكليه برنامه‌ها خواهيد بود.
در آخر باز هم يادآور مي‌شويم كه هرگز نامه های دريافتي كه كمي ناشناخته و مشكوك به نظر مي‌رسند را باز نكنيد.

ويروسهاي چند جزئي Multipartite virus

بعضي از ويروسها، تركيبي از تكنيكها را براي انتشار استفاده كرده ، فايلهاي اجرائي، بوت سكتور و پارتيشن را آلوده می سازند. اينگونه ويروسها معمولاً تحت windows 98يا Win.Nt انتشار نمي‌يابند.

فصل دوم

چگونه ویروسها گسترش می‌یابند؟

زماني كه يك كد برنامة آلوده به ويروس را اجرا مي‌كنيد، كد ويروس هم پس از اجرا به همراه كد برنامه اصلي ، در وهله اول تلاش مي‌كند برنامه‌هاي ديگر را آلوده كند. اين برنامه ممكن است روي همان كامپيوتر ميزان يا برنامه‌اي بر روي كامپيوتر ديگر واقع در يك شبكه باشد. حال برنامه تازه آلوده شده نيز پس از اجرا دقيقاً عمليات مشابه قبل را به اجرا درمي‌اورد. هنگاميكه بصورت اشتراکی یک کپی از فایل آلوده را در دسترس کاربران دیگر کامپیوترها قرار می دهید ، با اجراي فايل كامپيوترهاي ديگر نيز آلوده خواهند شد. همچنين طبيعي است با اجراي هرچه بيشتر فايلهاي آلوده فايلهاي بيشتري آلوده خواهند شد.

اگر كامپيوتري آلوده به يك ويروس بوت سكتور باشد، ويروس تلاش مي‌كند در فضاهاي سيستمي فلاپي ديسكها و هارد ديسك از خود كپی هایی بجا بگذارد . سپس فلاپي آلوده مي‌تواند كامپيوترهايي را كه از روي‌آن بوت مي‌شوند و نيز يك نسخه از ويروسي كه قبلاً روي فضاي بوت يك هارد ديسك نوشته شده نيز مي‌تواند فلاپي‌هاي جديد ديگري را نيز آلوده نمايد.
به ويروسهايي كه هم قادر به آلوده كردن فايلها و هم آلوده نمودن فضاهاي بوت مي‌باشند اصطلاحاً ويروسهاي چند جزئي (multipartite) می گویند.

فايلهايي كه به توزيع ويروسها كمك مي‌كنند حاوي يك نوع عامل بالقوه مي‌باشند كه می توانند هر نوع كد اجرائي را آلوده كنند. براي مثال بعضي ويروسها كدهاي را آلوده مي‌كنند كه در بوت سكتور فلاپي ديسكها و فضای سيستمي هارد ديسكها وجود دارند.

نوع ديگر اين ويروس ها كه به ويروسهاي ماكرو شناخته می شوند ، مي‌توانند عمليات پردازش كلمه‌اي (word processing) يا صفحه‌هاي حاوي متن را كه از اين ماكروها استفاده مي‌كنند ، آلوده می کنند. اين امر براي صفحه‌هايي با فرمت HTMl نيز صادق است.

از آنجائيكه يك كد ويروس بايد حتماً قابل اجرا شدن باشد تا اثري از خود به جاي بگذارد از اينرو فايلهايي كه كامپيوتر به عنوان داده‌هاي خالص و تميز با آنها سرو كار دارد امن هستند.

فايلهاي گرافيكي و صدا مانند فايلهايي با پسوند . gif، jpg، mp3، wav،...هستند .

براي مثال زماني كه يك فايل با فرمت picture را تماشا مي‌كنيد كامپيوتر شما آلوده نخواهد شد.

يك كد ويروس مجبور است كه در قالب يك فرم خاص مانند يك فايل برنامه‌اي .exe يا يك فايل متني doc كه كامپيوتر واقعاً آن را اجرا مي‌كند ، قرار گيرد .

عمليات مخفيانه ويروس در كامپيوتر

همانطور كه مي‌دانيد ويروسها برنامه‌هاي نرم افزاري هستند .آنها مي‌توانند مشابه برنامه‌هايي باشند كه به صورت عمومي در يك كامپيوتر اجرا می گردند .

اثر واقعي يك ويروس بستگي به نويسنده آن دارد. بعضي از ويروسها با هدف خاص ضربه زدن به فايلها طراحي مى شوند و يا اينكه در عمليات مختلف كامپيوتر دخالت كرده و ايجاد مشكل مي‌كنند.

ويروسها براحتي بدون آنكه متوجه شويد خود را تكثير كرده ، گسترش مي‌يابند ، در حين گسترش يافتن به فايلها صدمه رسانده و يا ممكن است باعث مشكلات ديگرى شوند. نكته: ويروسها قادر نيستند به سخت افزار كامپيوتر صدمه اى وارد كنند . مثلاً نمى توانند باعث ذوب شدن CPU ، سوختن هارد ديسک و يا انفجار مانيتور و غيره شوند .

ويروسها و E-mail

شما صرفا با خواندن يك متن سادة e-mail يا استفاده از netpost ، ويروسي دريافت نخواهيد كرد. بلكه بايد مراقب پيغامهاي رمز دار حاوي كدهاي اجرائي و يا پيغامهايى بود كه حاوي فايل اجرائي ضميمه شده (يك فايل برنامه‌اي كد شده و يا يك word document كه حاوي ماكروهايي باشد) مى باشند. از اين رو براي به كار افتادن يك ويروس يا يك برنامه اسب تروا ، كامپيوتر مجبور به اجراى كدهايى است مي‌توانند يك برنامه ضميمه شده به e-mail ، يك word document دانلود شده از اينترنت و يا حتي مواردى از روي يك فلاپي ديسك باشند.

فصل سوم

نکاتی جهت جلوگیری از آلوده شدن سیستم

اول از هرچيزي به خاطر داشته باشيد اگر برنامه ای درست کار نکند يا کلا کامپيوتر در بعضی از عمليات سريع نباشد بدان معنا نيست که به ويروس آلوده شده است .

اگر از يك نرم افزار آنتي ويروس شناخته شده و جديد استفاده نمي‌کنيد در قدم اول ابتدا اين نرم افزار را به همراه کليه امکاناتش بر روي سيستم نصب کرده و سعي کنيد آنرا به روز نگه داريد.

اگر فکر مي‌کنيد سيستمتان آلوده است سعي کنيد قبل از انجام هر کاري از برنامه آنتي ويروس خود استفاده کنيد.(البته اگر قبل از استفاده از آن، آنرا بروز کرده باشيد بهتر است). سعي کنيد بيشتر نرم افزارهاي آنتي ويروس را محك زده و مطمئن ترين آنها را برگزينيد.

البته بعضي وقتها اگر از نرم افزارهاي آنتي ويروس قديمي هم استفاده کنيد، بد نيست. زيرا تجربه ثابت کرده که ویروس یابهای قدیمی بهتر می توانند ویروسهایی را که برای مدتی فعال بوده و به مرور زمان بدست فراموشی سپرده شده اند را شناسایی و پاکسازی کنند .

ولي اگر جزء افرادي هستيد که به صورت مداوم با اينترنت سروکار داريد حتماً به يك آنتي ويروس جديد و به روز شده نياز خواهيد داشت .

براي درك بهتر و داشتن آمادگي در هر لحظه براي مقابله با نفوذ ویروسها به نکات ساده ی زیر توجه کنید :

۱- همانطور که در بالا ذکر شد از يك کمپاني مشهور و شناخته شده بر روي سيستم تان یک نرم افزار آنتی ویروس نصب کرده و سعي کنيد هميشه آنرا به روز نگه داريد.

۲- هميشه احتمال ورود ويروسهاي جديد به سيستم وجود دارد . پس يك برنامه آنتي ويروس که چند ماه به روز نشده نمي‌تواند در مقابل جريان ويروسها مقابله کند.

۳-توصيه می شود براي آنکه سيستم امنيتي کامپيوتر از نظم و سازماندهي برخوردار باشد برنامه a.v (آنتي ويروس) خود را سازماندهي نمائيد ، مثلاً قسمت configuration نرم افزار a.v. خود را طوري تنظيم کنيد که به صورت اتوماتيك هر دفعه که سيستم بوت مي‌شود آن را چك نمايد، اين امر باعث مي‌شود سيستم شما در هر لحظه در مقابل ورود ويروس و يا هنگام اجراي يك فايل اجرائي ايمن شود.

۴- برنامه‌هاي آنتي ويروس در يافتن برنامه‌هاي اسب تروآ خيلي خوب عمل نمي‌کنند از اين رو در باز کردن فايلهاي باينري و فايلهاي برنامه‌هاي excel و Word که از منابع ناشناخته و احياناً مشکوك مي‌باشند محتاط عمل کنيد.

۵-اگر براي ايميل و يا اخبار اينترنتي بر روي سيستم خود نرم افزار کمکي خاصي داريد که قادر است به صورت اتوماتيك صفحات Java script و word macro ها و يا هر گونه کد اجرائي موجود و يا ضميمه شده به يك پيغام را اجرا نمايد توصيه مي‌شود اين گزينه را غير فعال (disable) نمائيد.

۶-از باز کردن فایلهایی که از طریق چت برایتان فرستاده می شوند ، پرهیز کنید.

۷- اگر احياناً بر روي هارد ديسك خوداطلاعات مهمي داريد حتماً از همه آنها نسخه پشتيبان تهيه كنيد تا اگر اطلاعات شما آلوده شده اند يا از بين رفتند بتوانيد جايگزين كنيد.

نكاتی برای جلوگيری از ورود كرمها به سيستم

از آنجائيكه اين نوع برنامه‌ها (worms) امروزه گسترش بيشتري يافته و بايد بيشتر از ساير برنامه‌هاي مخرب از آنها دوري كنيم، از اين رو به اين نوع برنامه هاي مخرب بيشتر مي‌پردازيم.

كرمها برنامه‌هاي كوچكي هستند كه با رفتاري بسيار موذيانه به درون سيستم رسوخ كرده، بدون واسطه خود را تكثير كرده و خيلي زود سراسر سيستم را فرا مي‌گيرند. در زير نكاتي براي جلوگيري از ورود كرمها آورده شده است.

۱) بيشتر كرمهايي كه از طريق E-mail گسترش پيدا مي‌كنند از طريق نرم افزارهاي microsoft outlook و يا express look out وارد سيستم مي‌شوند. اگر شما از اين نرم افزار استفاده مي‌كنيد پيشنهاد مي شود هميشه آخرين نسخه security patch اين نرم افزار را از سايت microsoft دريافت و به روز كنيد.

همچنين بهتر است علاوه بر به روز كردن اين قسمت از نرم افزار outlook سعي كنيد ساير نرم افزارها و حتي سيستم عامل خود را نيز در صورت امكان هميشه به روز نگه داريد، و يا حداقل بعضي از تكه‌هاي آنها را كه به صورت بروز درآمده قابل دسترسي است.

اگر از روي اينترنت بروز مي‌كنيد و يا از cd ها و بسته‌هاي نرم افزاري آماده در بازار ،از اصل بودن آنها اطمينان حاصل كنيد.

۲) تا جاي ممكن در مورد e-mail attachment ها محتاط باشيد. چه در دريافت e-mail و چه در ارسال آنها.

۳) هميشه ويندوز خود را در حالت show file extensions قرار دهيد.

اين گزينه در منوي Tools/folder option/view با عنوان " Hide file extensions for known file Types" قرار داردكه به صورت پيش فرض اين گزينه تيك خورده است، تيك آنرا برداريد.

۴) فايلهاي attach شده با پسوندهاي SHS و VBS و يا PIF را هرگز باز نكنيد. اين نوع فايلها در اكثر موارد نرمال نيستند و ممكن است حامل يك ويروس و يا كرم باشند.

۵) هرگز ضمائم دو پسوندي را باز نكنيد.

email attachment هايي با پسوندهايی مانند Neme.BMP.EXE و يا Name.TxT.VBS و ...

۶) پوشه‌هاي موجود بر روي سيستم خود رابجز در مواقع ضروري با ديگر كاربران به اشتراك نگذاريد . اگر مجبور به اين كار هستيد، اطمينان حاصل كنيد كه كل درايو و يا شاخه ويندوز خود را به اشتراك نگذاشته ايد.

۷) زماني كه از كامپيوتر استفاده نمي‌كنيد كابل شبكه و يا مودم را جدا كرده و يا آنها را خاموش كنيد.

۸) اگر از دوستي كه به نظر مـی رسـد ناشـناس اسـت ايميلـی دريافـت كرديـد قبـل از بـاز كـردن ضمائم آن حتماً متن را چند بار خوانده و زماني كه مطمئن شديد از طرف يك دوست است ، آنگـاه سراغ ضمائم آن برويد.

۹)توصيه می شود فايلهاي ضميمه شده به ايميل‌هاي تبليغاتي و يا احيانـاً weblink هـاي موجـود در آن‌ها را حتي الامكان باز نكنيد.

۱۰) از فايلهاي ضميمه شده‌اي كـه بـه هـر نحـوي از طريـق تصـاوير و يـا عنـاوين خـاص، بـه تبليـغ مسائل جنسـي و ماننـد آن مـی پردازنـد ، دوري كنيـد. عنـاويني ماننـد porno.exe و يـا pamela-Nude.VBS كه باعث گول خوردن كاربران مي‌شود.

۱۱) به آيكون فايلهاي ضميمه شده نيز به هيچ عنوان اعتماد نكنيد. چرا كه ممكن است كرمهايي در قالب فايل عكس و يا يک فايل متني فرستاده شود ولي در حقيقت اين فايل يـك فايـل اجرائـي بوده و باعث فريب خوردن كاربر مي‌شود.

۱۲)در massenger هـايي ماننـد IRC، ICQ و يـا AOL بـه هـيچ عنـوان فايلهـاي ارسـالي از جانـب كاربران ناشناس on-line درchat system ها را قبول (accept) نكنيد.

۱۳) از Download كردن فايل از گـروه‌هـاي خبـري همگـاني نيـز پرهيـز كنيـد.(usenet news) زيـرا اغلب گروه‌هاي خبري خود يكي از علل پخش ويروس می باشند .

CODERED يک نوع کرم اينترنتی

حال به شرح حال مختصري از خصوصيات يك كرم معروف كه هنوز هم وجود خواب آلوده خـود را بـر روي هزاران وب سرور افكنده و كارشناسان امنيتي را به تكاپو واداشته اسـت، مـي‌پـردازيم. راجـع به واژه خواب آلود متن زير را مطالعه كنيد.

CODERED يك نوع كرم اينترنتي

مركز تطبيق و هماهنگي Cert در پتيسبورگ كه مركزي براي بررسـي اطلاعـات سـري كـامپيوتري است، اذعان مي‌دارد كه ويروس CODERED احتمالاً به درون بيش از ۲۸۰۰۰۰ دسـتگاه متصـل بـه اينترنت كه از سيستم عاملهاي NT4.0 و ويندوز ۲۰۰۰ استفاده مي‌كننـد نفـوذ كـرده اسـت. حـال آنكه اين سيستم عاملها ، داراي مزيت محافظتی به وسـيلة نـرم افزارهـاي خطايـاب IIS5 و IIS4 می باشند .

هنگامي كه هر دو گونه ايـن ويـروس (نسـخه‌هـاي A.۲۹ و codered II) تـلاش مـي‌كننـد تـا روي سرورهايي كه به وسيله سرويس‌هاي شاخص نرم افزارهاييكـه IIS از لحـاظ ضـعفهاي عبـوري يـا مقاومت در برابـر ويروسـهاي جديـد اصـلاح نشـده‌انـد ، نفـوذ و منتشـر شـوند، يكـي از دو نسـخه قـديمي ايـن ويـروس طـوري تنظـيم شـده اسـت كـه صـفحات اوليـه اتصـال اينترنتـي معـروف بـه Homepage و يا start page مربوط به وب سرور آلوده شده را از حالت طبيعي خارج سازد.

اين ويروس طوري تنظيم شده است كه تا بيستمين روز ماه منتشر مي‌شود ،آنگاه بـا حـالتي كـه cert آن را مرحله ويرانگر ناميده است، چنان عمل مي‌كند كه خود سرويس محافظ شخصـي را بـر عليـه آدرس اينترنتـي داده شـده وادار بـه خرابكـاري مـي‌كنـد. جالـب اسـت بدانيـد اولـين آدرس اينترنتي داده شده به ويروس وب سرور كاخ سفيد بوده است.

به نظر می رسد که این ویروس در آخرین ساعت بیست و هفتیمن روز ماه، بمباران و انتشارهاي خود را متوقف کرده ، وارد مرحله خواب موقتي شده و خود را غير فعال مي‌کند. حال آيا ويروس قدرت اين را دارد که در اولين روز ماه بعد ، خود را براي فعاليتي دوباره بيدار کند.

يك مرکز تحقيقات تخصصي که در اوهايو ايالات کلمبيا شرکتي مشاوره‌اي و فني است، به بررسي و تست ويروس Codered پرداخته و به اين نتيجه رسيده است که اين مزاحم خواب آلود مي‌تواند دوباره خود را فعال کرده و فرآيند جستجوی ميزبانان جديد را از سر بگيرد.

بررسيها و نتايج به دست آمده نشان مي دهند که codered براي شروع فعاليت مجدد، فايل مخصوصي را جستجو کرده و تا زمان پيدا کردن آن فايل و ساختن درايو مجازي خاصي به نام تروآ (Trojan) در حالت خواب باقي مي‌ماند.

کارشناسان فني بر اين عقيده‌اند که اين ويروس مجبور نيست خود را بيدار و فعال کند تا برای سيستمها تحديدی جدي به حساب آيد. در حال حاضر سيستم‌هاي آلوده ی بسياری وجود دارند که ناخودآگاه براي انتشار و سرايت ويروس به سيستم‌هاي ديگر تلاش مي‌کنند. يکي از کارشناسان SARC يکي از مراکز تحقيقاتي مي‌گويد : از آنجا که کامپيوترهاي زيادي هستند که ساعتها درست تنظيم نشده ، شاهد انتشار مجدد اين ويروس خواهيم بود. تنها يکي از سيستم‌هاي آلوده، براي انتشار موج جديدي از اختلالات کافي خواهد بود.

محاسبات مرکز تطبيق و هماهنگي CERT نشان مي‌دهد که ويروس Codered 250000 ، سرور ويندوزهايي که در خلال ۹ ساعت اول فعاليت زود هنگام خود، سرور ويندوزهایی که آسيب پذير بوده اند را آلوده ساخته است. بولتن خبري CERT تخمين مي‌زند که با شروع فعاليت ويروس از يك ميزبان آلوده، زمان لازم براي آلوده شدن تمام سيستم‌هايي که عليرغم استفاده از نرم افزارهاي IIS (البته نسخه‌هاي قديمي آن) همچنان آسيب پذير مانده‌اند، کمتر از ۱۸ ساعت است! اين رخدادها، اين سوال را تداعی می کنند که چه تعداد از کامپيوترهاي آلوده شده قبلي، تاکنون اصلاح و پاکسازي شده‌اند؟ اگرچه سرور کاخ سفيد، هدف اصلي حملات خرابکارانه Codered بوده است، با اين حال اين کرم کينه جو هنوز مشکلات بسياری را براي ميزبانان به وجود مي‌آورد.

حمله به سيستم های Linux

ويروس معروف و بسيار گستردة Slapper ، براي اولين بار در تاريخ ۱۴ سپتامبر ۲۰۰۲ کشف شد.
Slapper يك کرم شبکه
Slapper طي مدت کوتاهي به سرعت هزاران وب سرور در سراسر دنيا را آلوده کرد. يکي از جالب‌ترين خصوصيات slapper توانايي‌آن در ايجاد يك شبکه نظير به نظير است که برای نويسنده امکان کنترل تمامی شبکه های آلوده شده را بوجود می آورد .

پيوست

كوتاه و مختصر

هـــدف اصـــلي ايـــن كـــرم اينترنتـــي ضـــربه زدن بـــه مايكروســـافت و ســـايت اينترنتـــي Windowsupdate.comاين كمپاني مي باشد . نويسنده اين كرم بـا ايـن عمـل مـي خواهـد بـراي كاربراني كه مـي خواهنـد سيسـتم عامـل ويـندوز خـود را از ايـن طريـق در برابـر هجـوم ايـن كـرم محافظت كنند مشكل ايجاد نمايد . اين كرم در كدهاي خود حاوي رشته پيغام زير مي باشد :

I Just want to say LOVE YOU SAN!! Billy Gates why do you make this possible? Stop making money and fix your software .

البته اين پيغام در نسخه جديدتر اين كرم (W32/Blaster-B) تغيير كرده است .
كرم Blaster از طريق ايميل گسترش پيدا نمي كند ، بلكه از طريق يافتن نسخه هاي آسيب پـذير ويندوز گسترش مي يابد و ايـن كـار را از طريـق سـرويس (Remote Procedure Call) RPC وينـدوز انجام مي دهد . بنابراين برنامه هاي محافظ ايميل قادر به شناسايي اين كرم نيستند .
شركتها و مديران شبكه ها مي بايست نرم افزارهاي محافظ مخصـوص ايـن كـرم را از روي سـايت مايكروسافت دريافت و نيز از صحيح نصب شـدن Firewall هـا بـروي سيسـتمها و سـرورهاي خـود اطمينان حاصل كرده و نيز مهمتر از همه آنتي ويروس بروز شده را فراموش نكنند .

شرح و بررسی W32/Blaster-A

نامهاي مستعار :

W32/Lovsan.worm , W32.Blaster.worm , WORM_MSBLAST.A , win32.Poza , Worm/Lovsan.A

نوع :

win32 worm
W32/Blaster-A كرمي است كه از طريـق اينترنـت و بـا اسـتفاده از خطـاي آسـيب پـذيري DCOM موجود در سرويس Remote Procedure Call- RPC سيستم عاملهاي ويندوز براي اولين بار توسط كمپاني مايكروسافت در اواسط ماه جولاي ۲۰۰۳ فاش و منتشر مي شود . لازم به ذكر است اين كرم برخلاف اغلب كرمهاي ديگر از طريق ايميل گسترش نمي يابد .
سيستم عاملهايي كه در معرض هجوم اين كرم مي باشند بشرح زير هستند :
Windows NT 4.0
Windows NT 4.0 Terminal Services Edition
Windows 2000
Windows XP
Windows Server 2003
در نسخه هاي ويندوز xp كه به اين كرم آلـوده مـی شـوند ، بطـور متـوالي سـرويس RPC متوقـف ميشود و پيغامي مبني بر خاموش شدن سيستم ظاهر ميشـود " System ShutDown" و بعـد از حدود يك دقيقه سيستم حاوي ويندوز ، XP دوباره راه اندازی مي شود .

ويندوزهاي ۹۵ ، ۹۸ ، ME كه از سرويس RPC استفاده نمي كنند از اين بابت در خطر حمله ی اين كرم نيستند .
در مسير يافتن سيستمهاي آسيب پذير ، كرم سيستم راه دور (كامپيوتر آسيب پذير) را وادار به دريافت فايلي از طريق پروتكل دريافت فايل TFTP با عنوان msblast.exe ويا penis32.exe مي نمايد .
اين فايل در شاخه ويندوز كپي مي شود .
همچنين دستور زير را در رجيستري ويندوز اضافه مي كند :

HKLM/Software/microsoft/windows/currentVersion/Run/windows auto update = "msblast.exe"

و نيز رشته كاراكتر زير در كدهاي اين ويروس ديده شده كه البته واضح نيست :

I Just want to say LOVE YOU SAN!! Billy Gates why do you make this possible? Stop making money and fix your software.

نحوه مقابله و پاكسازی:

Blaster از طريق شبكه اينترنت سايت ها را جستجو كرده و سيستمهايي كه داراي خطاي آسيب پذيري سرويس محافظتي DCOM RPC هستند را يافته و به درون آنها نفوذ مي كند.

تمهیداتی برای مدیران شبکه ها

مديران شبكه (Adminstrators) براي مقابله با نفوذ اين كرم به درون سيستمها و خنثي كردن آن بهتر است كه به روش زير عمل كنند :
- در مرحله ی اول اگر آنتی ويروس بر روی سيستم شما نصب بود آنرا به روز كنيد در غير اينصورت از يكی از سايتهای مشهور و قابل اطمينان نظير سايتهای Symantec و يا Mcafee به نصب آنتی ويروس مناسب بپردازيد .
- در مرحله ی بعدی Patch مربوط به عمليات خنثی سازی Blaster را از سايت Microsoft دريافت كرده و بر روی تک تک سيستمها و سرورها نصب كنيد .
- فايل ftp.exe (كه يكی از فايلهای برنامه ی ويندوز مي باشد) فايلی است كه Blaster می تواند از طريق آن به مقاصد خود برسد . پس بهتر است آنرا به فايل ftp.exe.old تغيير نام داد و عمليات Blaster را خنثی كنيد .

نكته :

از حذف فايل مذكو بپرهيزيد چرا كه ممكن است نرم افزارهای ما بدان محتاج شوند .
-در آخر توصيه مي شود حتي الامكان ترافيك موجود در پورت هاي زير را در نرم افزار Firewall مسدود نمائيد .

- TCP/69 -used by Tftp process
- TCP/135-RPC remote access
- TCP/4444-used by this worm to connect

راهنمایی برای کاربران خانگی

افرادي كه از نسخه هاي ويندوز NT4 , 2000 , XP , server 2003 استفاده مي كنند می توانند جهت محافظت سیستم خود و حتي پاكسازي آن از آلودگي به نكات زير توجه كنند .

نکته اول :

نرم افزار Firewall در محافظت از كامپيوتر به شما كمك می نمايد .راه اندازي نرم افزار Firewall مي تواند عمليات مخفيانه كرمها در سيستم را محدود سازد .
در نسخه های Windows XP و Server 2003 ، نرم افزار Firewall موجود می باشد . قبل از راه اندازی این نرم افزار، اگر سیستم مدام Reboot شد ، ابتدا ارتباط اینترنتی را قطع کرده و سپس Firewall را فعال کنید .

۱- کاربران XP :

براي راه اندازي Firewall ويندوز XP به ترتيب مراحل زير را انجام دهيد :
- Network connection را باز كنيد .
(startmenu/setting/controlPanel/Network & Internet connection)
- سپس روي گزينه Network connection كليك كنيد .
- برروي يكي از Internet connection هايي كه مايليد محافظت بر روی آن انجام شود ، كليك كنيد .
سپس در سمت چپ و در قسمت Network tasks برروي settings of this connections كليك كرده و يا برروي يكي از connection ها كليك راست كرده و گزينه ی Properties را بزنيد .
- در قسمت Advanced Tab اگر گزينه "Protect my computer network" تيك داشته باشد ، Firewall نيز و اگر تيك آن برداشته شود ، غير فعال خواهد بود.
براي دريافت اطلاعات بيشتر راجع به اين قسمت ميتوانيد به آدرس زير مراجعه كنيد :
www.microsoft.com/security/incident/blast.asp

۲- کاربران ویندوز server 2003

براي فعال كردن Firewall ويندوز می توان به آدرس زير مراجعه كرد :
www.microsoft.com/technet/treeview/default.asp

نکته دوم:

دريافت security patch از سايت مايكروسافت است .
/http://windowsupdate.microsoft.com

نکته سوم:

نصب يك آنتي ويروس Uptodate بر روی سیستم می باشد .

نکته چهارم:

پاكسازي كرم از روي سيستم است . كه برای انجام این کار هم می توان از ندم افزار آنتی ویروس Uptodate شده استفاده کرد و هم اینکه جهت اطمینان بیشتر بصورت دستی اقدام کرد

که ابتدا باید کرم موجود در سیستم و در نرم افزار آنتی ویروس را شناسایی کرده و سپس اقدام به پاکسازی آن کنید .

پاکسازی دستی Blaster-A از روی سیستم

۱ : ابتدا که security patch مخصوص را از سایت مایکروسافت دریافت کرده و برروي سیستم نصب نمایید.

۲ : کلیدهاي Ctrl+Alt+Del را بطور همزمان با هم فشار دهید.

۳ : پس از ظاهر شدن پنجره Task manager برروي گزینه ی Processes Tab کلیك کنید .

۴ : فایل msblast.exe را در لیست جستجو کنید .

۵ : پس از یافتن فایل بروي آن کلیك کرده ، آنرا highlight نموده ، بروي End process کلیك کرده و Task manager را ببندید .

۶ : توسط موتور جستجوگر ویندوز سه فایل msblast.exe , Penis32.exe , Teekids.exe را (Start /search) جستجو کنید .

احتمالاً به همراه فایلهاي اجرائي فوق ، فایلهایي با پسوند .Pif یافت میشوند . پس از اتمام عملیات جستجو کلیه فایلهاي یافته شده با مشخصات بالا را پاك نمائید . این فایلها همگي در شاخه ویندوز یافت می شوند .

۷ : حال مي بایست دستوری که توسط کرم به رجیستری داده می شود را بیابیم و از بین ببریم.
البته عملیات فوق را مي توان با استفاده از دستور دیگري هم انجام داد :
- در پنجره Run دستور زیر را تایپ کنید .
Services.msc /s
-در پنجره ظاهر شده بروي گزینه "Services and Application" دوبار کلیك کرده ، همانطور که مشاهده مي شود لیستي از سرویسها ظاهر مي شود .
- در قسمت راست پنجره سرویس RPC -Remote Procedure Call را جستجو کنید .
- برروي آن کلیك راست کرده و Properties را انتخاب کنید .
- بروي Recovery TAB کلیك کنید .
- لیستهاي کرکره اي موجود (Subsequent failures , Second failure , First failure) را روي گزینه " Restart the Service " تغییر دهید .
- Apply کرده و سپس OK را بزنید.
با انجام این عملیات و به هنگام اتصال به اینترنت ، Blaster دیگر قادر به Reboot کردن سیستم نخواهد بود .

غیر فعال کردن System Restore در ویندوز XP

به منظور احتیاط ، سرویس بازیابي خودکار ویندوز XP یعني System Restore را موقتاً غیر فعل می نمائیم .
چرا که این قسمت از ویندوز XP بصورت پیش فرض فعال بوده و ممکن است ویندوز فایلهاي آسیب دیده ، ویروس ها ، کرم ها و برنامه هاي اسب تروآ يي که احیاناً قبلاً بروي سیستم بوده اند را بازگرداند. براي غیر فعال کردن این قسمت در ویندوز xp به آدرس زیر مراجعه کنید :

Startmenu / setting / controlPanel / Performance and maintennance /system / system restore(tab)

و سپس گزينه زير را فعال می کنيم:

"Turn of system Restore on all Drives"

انواع ديگر BLASTER

W32/Blaster-A با نامهاي مستعار Lovsan , MSBLAST , Poza گسترش يافته است .
هنوز چند هفته اي از شيوع اين کرم نمي گذرد که انواع جديدتر آن نيز ديده شده است .

W32/Blaster-B ، عملکرد اين نسخه از Blaster نيز مانند نسخه پيشين است با اين تفاوت فايلي را که در پوشه ويندوز ايجاد مي کند ديگر msblast.exe نمي باشدو فايلي با نام teekids.exe مي باشد ، همچنين دستوري که در رجيستري ويندوز اضافه مي کندآن دستور قبلي نمي باشد بلکه اين بار حاوي يک رشته کاراکترهايي اهانت آورعليه Bill Gates و کمپاني مايکروسافت و سازندگان آنتي ويروسها مي باشد.
نسخه ديگر اين کرم با نام W32/Blaster-C نيز موجود است که نام فايل ايجاد کرده در شاخه ويندوز آن penis32.exe مي باشد .

نکته: در کليه نسخه هاي اين کرم همراه فايلهاي exe ايي که اين کرم در شاخه ويندوز کپي مي کند يك فايل با پسوند .pifو با همان نام در شاخه ويندوز مي توان يافت .

خبر مسدود نمودن سايت windowsupdate.com ، توسط کمپاني مايکروسافت

W32/Blaster-A روز دوشنبه ، ۱۱ آگوست ۲۰۰۳ براي اولين بار ديده شد .
براساس خبرهاي گزارش شده ، کمپاني مايکروسافت تصميم گرفته است آدرس URL، windowsupdate.com اين کمپاني را بطور کلي از بين ببرد .اين همان وب سايتی است که به بوسيله ی اين کرم در تاريخ شانزدهم آگوست تمام کامپيوترها در سراسر دنيا را آلوده کرده است .
طبق اعلام مايکروسافت : کاربران مي توانند با مراجعه به آدرس http://windowsupdate.microsoft.com و يا صفحه اصلي مايکروسافت سيستمهاي خود را update نموده و نيز از اطلاعات و patch هاي محافظ موجود ، استفاده کنند .

اسب تروآ "GrayBird" ، چهره ديگر Blaster

آزمايشگاه تحقيقاتي sophos چند روز قبل برروي وب سايت اختصاصي خود اعلام کرد که نرم افزار آنتي ويروس خود را بار ديگر update نمود ، چرا که متخصصان اين مرکز به يك نوع نرم افزار مخرب اسب تروآ ی جديد با نام "Graybird" Trojan برخورد نموده اند .
اين اسب تروآ جديد که به منظور بدنام کردن مايکروسافت و شايد جوابي عليه تمهيدات اين کمپاني در مبارزه با کرم جديد Blaster بصورت عمدي بوجود آمده است که در قالب يك patch نرم افزاري محافظ عليه Blaster ، مربوط به کمپاني مايکروسافت خود را ارسال مي کند .
اين مرکز به کاربران توصيه مي کند به هيچ عنوان patch هاي محافظتي (Security patch) را هرچند که از منابع شناخته شده و مشهور از طريق ايمل ارسال می شود را باز نکنند .

صحيح ترين و قابل اطمينان ترين محل براي دريافت patch هاي محافظ ، وب سايت اختصاصي كمپاني ها و فروشنده هاي مربوطه مي باشد . همچنين از عمل كردن و يا Forward كردن پيغامهاي مشكوكي كه به هر شكلي رويدادها و پيشامدهايي را شرح و تفصيل مي كنند و به خيال خود ممكن است مفيد واقع گردد ، به همكاران و دوستان خود پرهيز كنيد .
Graybird در قالب يك patch نرم افزاري متعلق به مايكروسافت مي باشد و فقط يك حقه گمراه كننده است براي نفوذ كرم Blaster می باشد .
به گفته يكي از متخصصان اين مركز Blaster فقط و فقط يك باور و توهّم خيالي است كه با نفوذ به صدها و هزاران سيستم در سراسر دنيا تلاش مي كند تا كاربران را به ترس و وحشت گرفتار سازد .

هيچگاه كدهاي اجرائئ ارسال شده توسط ايميل را باز نكنيد .

ضمیمه

معرفی منبع – تماس با نویسنده

منابع :

-- سایت اینترنتی http://www.etvto.ir/ostadonline/www.symantec.com

-- سایت اینترنتی http://www.etvto.ir/ostadonline/www.mcafee.com

-- سایت اینترنتی http://www.etvto.ir/ostadonline/www.safos.com

منابع ویروس Blaster

۱- http://www.sophos.com

۲- http://www.symantec.com

آرش رضا پور خان

graphist-office

rezapurkhan@etvto.ir