امنیت نامه های الکترونیکی

«بخش دوم»

منبع : سایت www.SRCO.ir

پیشگیری سوم : تغییر فایل مرتبط و یا غیر فعال نمودن WSH

patch امنیتی ارائه شده در پیشگیری اول، باعث حفاظت سیستم در مقابل ویروس هائی نظیر ILOVEYOU ، در ۸outlook 9 و outlook 2000 می گردد . متاسفانه روش مشابهی بمنظور استفاده در outlook Express ، وجود ندارد. بمنظور حفاظت سیستم در مقابل نامه های الکترونیکی که دارای عملکردی نظیر ILOVEYOU می باشند ، می توان از روشی دیگر در outlook express استفاده کرد. بدین منظورمی توان تغییراتی را در سطح برنامه هائی که مسئول فعال نمودن فایل مورد نظر(Associations File) می باشند ، اعمال نمود. کرم ILOVEYOU ، از طریق یک فایل اسکریپت ویژوال بیسیک (vbs .) ، که توسط میزبان اسکریپت ویندوز (Windows Scripting Host :WSH) تفسیر می گردد ، فعال خواهد شد. در حقیقت WSH محیط (شرایط) لازم برای ILOVEYOU را فراهم می نماید. اعمال محدودیت در رابطه با WSH و یا تغییر در فایل پیش فرض مربوطه ای که مسئول برخورد(نمایش ، ایجاد شرایط اجراء) با فایل مورد نظر می باشد ، می تواند یک سطح مناسب امنیتی را در رابطه با ضمائم نامه های الکترونیکی که حاوی کدهای مخرب می باشند ، فراهم می نماید. در این رابطه از راهکارهای متفاوتی می توان استفاده کرد .

روش اول : یکی از روش های پیشگیری موثر در مقابل این نوع از حملات ، تغییر واکنش پیش فرض در زمانی است که کاربر باعث فعال شدن اینچنین فایل های می گردد (double click بر روی فایلی با انشعاب vbs .) .در ویندوز NT ، این عملیات از طریق Windows Explorer و بصورت زیر انجام می شود.

View | Folder Options ==>

Select VBScript Script File ==>
Click Edit ==> *Highlight* Edit ==>
Click Set Default

پس از اعمال تغییرات فوق ، در صورتیکه کاربری فایلی ضمیمه با انشعاب vbs . را فعال نماید ، فایل مورد نظر توسط WSH اجراء نخواهد شد ، در مقابل ، فایل فوق ، بدون نگرانی توسط ادیتور پیش فرض (معمولا" notepad) ، فعال و نمایش داده خواهد شد. فرآیند فوق را می توان به فایل های دیگر نیز تعمیم داد. فایل هائی که دارای یکی از انشعابات زیر باشند ، توسط WSH فعال خواهند شد . بنابراین می توان تغییرات لازم را مطابق آنچه اشاره گردید ، در رابطه با آنها نیز اعمال نمود.

WSC , WSH ,WS
,WSF,VBS,VBE,JS,JSE

روش ارائه شده در رابطه با outlook Express بخوبی کار خواهد کرد . در این راستا ، لازم است به این مسئله مهم اشاره گردد که تضمینی وجود ندارد که سرویس گیرندگان پست الکترونیکی از تنظیمات پیش فرض، زمانیکه کاربر یک فایل ضمیمه را فعال می نماید، استفاده نمایند . مثلا" زمانیکه یک فایل ضمیمه vbs. ، توسط Netscape messenger فعال می گردد ، کاربر دارای گزینه های open و یا Save خواهد بود. در صورتیکه کاربر گزینه open را انتخاب نماید ، کد مورد نظر صرفنظر از تنظیمات پیش فرض فعال خواهد شد.(نادیده گرفتن تنظیمات پیش فرض)

روش دوم : راهکار دیگری که می توان بکمک آن باعث پیشگیری از بروز چنین مسائلی گردید ، غیر فعال نمودن WSH است . برای انجام عملیات فوق (غیر فعال نمودن WSH) می بایست برنامه های ویندوز را که باعث حمایت و پشتیبانی از اجراء اسکریپت ها می گردند (برنامه های wscript.exe و csscript) را تغییر نام داد .در سیستم هائی شامل ویندوزNT ، این فایل ها در مسیر System%\System32٪ ، قرار دارند(معمولا" C:\Winnt\System32) . بمنظور تغییر نام فایل های فوق ، بهتر است از طریق خط دستور (command prompt) این کار انجام شود. در برخی از نسخه های سیستم عامل، بموازات تغییر نام فایل مرتبط با یک نوع حاص از فایل ها ، بصورت اتوماتیک برنامه مرتبط با آنان به نام جدید تغییر داده خواهد شد. بدین ترتیب تغییر اعمال شده هیچگونه تاثیر مثبتی را از لحاظ امنیتی بدنبال نخواهد داشت .

روش سوم : گزینه سوم در خصوص غیر فعال نمودن WSH ، تغییر مجوز فایل (File Permission) در رابطه با فایل های Wscript.exe و CSscript.exe است . روش فوق ، نسبت به دو روش اشاره شده ، ترجیح داده می شود. در چنین مواردی امکان استفاده از

پتانسیل های WSH برای مدیران سیستم وجود داشته در حالیکه امکان استفاده از پتانسیل فوق از کاربران معمولی سلب می گردد .

لازم است به این نکته مهم اشاره گردد که با اینکه پیشگیری فوق ، در رابطه با کرم هائی نظیر ILOVEYOU و موارد مشابه موثرخواهد بود ، ولی نمی تواند تمام ریسک های مربوط در این خصوص و در رابطه با سایر فایل ها ئی که ممکن است شامل کدهای اسکریپت باشند را حذف نماید. در این رابطه می توان به فایل های با انشعاب exe . ، اشاره نمود. این نوع فایل ها دارای نقشی حیاتی در رابطه با انجام عملیات بر روی یک کامپیوتر بوده و نمی توان آنها را غیر فعال نمود . بدین ترتیب متجاوزان اطلاعاتی می توانند از این نوع فایل ها ، بعنوان مکانیزمی جهت توزیع کدهای مخرب ، استفاده نمایند .

پیشگیری چهارم : حفاظت ماکروهای آفیس و آموزش کاربران

ماکروسافت در رابطه با حفاظت در مقابل فایل های ضمیمه حاوی کدهای مخرب از طریق سایر برنامه های جانبی، نیز تدابیری اندیشیده است . مثلا" با اینکه patch امنیتی ارائه شده در پیشگیری اول ، بصورت پیش فرض در رابطه با ماکروهای word موثر واقع نمی شود ، ولی در بطن این نوع نرم افزارها امکانات خاصی قرار گرفته شده است که می توان بکمک آنان ، یک سطح امنیتی اولیه در رابطه با فعال شدن ماکروها را اعمال نمود. مثلا" آفیس ۹۷ ، گزینه اختیاری حفاظت ماکرو را ارائه که می توان بکمک آن یک لایه حفاظتی را در رابطه با عملکرد ماکروها ، ایجاد نمود. در چنین مواردی به کاربران پیامی ارائه و کاربران می توانند قبل از فعال شدن ماکرو در رابطه با آن تصمیم گیری نمایند (ارائه پاسخ مناسب توسط کاربران) . لازم است در این خصوص به کاربران آموزش های ضروری و مستمر در رابطه با خطرات احتمالی عدم رعایت اصول اولیه امنیتی خصوصا" در رابطه با دریافت نامه های الکترونیکی از منابع غیرمطمئن داده شود . گزینه فوق را می توان از طریق Tools|options|General| Enable macro virus protection ، فعال نمود. آفیس ۲۰۰۰ و XP وضعیت فوق را بهبود و می توان تنظیمات لازم در خصوص اجرای ماکروهای دریافتی از یک منبع موثق و همراه با امضاء دیجیتالی را انجام داد . در Excel. word , Powerpoint می توان ، گزینه فوق را از طریق Tools|macro|Security ، استفاده و تنظیمات لازم را انجام داد. با انتخاب گزینه High ، حداکثر میزان حفاظت ، در نظر گرفته خواهد شد.

پیشگیری پنجم : نمایش و انشعاب فایل

یکی از روش متداول بمنظور ایجاد مصونیت در مقابل فایل های حاوی کدهای مخرب ، تبدیل فایل فوق به فایلی بی خاصیت (عدم امکان اجراء) است . بدین منظور می توان از یک انشعاب

فایل اضافه استفاده نمود .(مثلا" فایل : ILOVYOU.TXT.VBS) . در صورتیکه ویندوز برای نمایش این نوع فایل ها (با در نظر گرفتن انشعاب فایل ها) ، پیکربندی نشده باشد ، فایل فوق بصورت یک فایل متن تفسیر خواهد شد. (ILOVEYOU.TXT) . بمنظور پیاده سازی روش فوق می بایست دو فاز عملیاتی را دنبال نمود : در اولین مرحله می بایست به ویندوز اعلام گردد که انشعاب فایل ها را از طریق Windows Explorer ، نمایش دهد . (انتخاب Options|View و غیر فعال نمودن Hide file extensions for known file types) . متاسفانه برای برخی فایل های خاص که می توانند شامل عناصر اجرائی و یا اشاره گری به آنان باشند ، تنظیم فوق ، تاثیری را بدنبال نداشته و در این رابطه لازم است کلید های ریجستری زیر ، بمنظور پیکربندی ویندوز برای نمایش انشعاب این نوع از فایل ها ، حذف گردد (مرحله دوم).

توضیحات	کلید ریجستری	انشعاب فایل
Shortcut	HKEY_CLASSES_ROOT\lnkfile\NeverShowExt	.lnk
Program information file (shortcut to a DOS program)	HKEY_CLASSES_ROOT\piffile\NeverShowExt	.pif
Windows Explorer Command file	HKEY_CLASSES_ROOT\SHCmdFile\NeverShowExt	.scf
Shortcut into a document	HKEY_CLASSES_ROOT\DocShortcut\NeverShowExt	.shb
Shell Scrap Object	HKEY_CLASSES_ROOT\ShellScrap	.shs
Shortcut to an Exchange folder	HKEY_CLASSES_ROOT\xnkfile\NeverShowExt	.xnk
Internet shortcut	HKEY_CLASSES_ROOT\InternetShortcut\NeverShowExt	.url
Shortcuts to elements of an MS Access database. Most components of an Access database can containan executable component.	HKEY_CLASSES_ROOT\Access.Shortcut.DataAccessPage.1\NeverShowExt	.maw
	HKEY_CLASSES_ROOT\Access.Shortcut.Diagram.1\NeverShowExt	.mag
	HKEY_CLASSES_ROOT\Access.Shortcut.Form.1\NeverShowExt	.maf
	HKEY_CLASSES_ROOT\Access.Shortcut.Macro.1\NeverShowExt	.mam
	HKEY_CLASSES_ROOT\Access.Shortcut.Module.1\NeverShowExt	.mad
	HKEY_CLASSES_ROOT\Access.Shortcut.Query.1\NeverShowExt	.maq
	HKEY_CLASSES_ROOT\Access.Shortcut.Report.1\NeverShowExt	.mar
	HKEY_CLASSES_ROOT\Access.Shortcut.StoredProcedure.1\NeverShowExt	.mas
	HKEY_CLASSES_ROOT\Access.Shortcut.Table.1\NeverShowExt	.mat
	HKEY_CLASSES_ROOT\Access.Shortcut.View.1\NeverShowExt	.mav

پیشگیری ششم : از Patch های بهنگام شده، استفاده گردد

اغلب حملات مبتنی بر اینترنت از نقاط آسیب پذیر یکسانی بمنظور نیل به اهداف خود استفاده می نمایند . ویروس Bubbleboy ، نمونه ای مناسب در این زمینه بوده که تهیه کننده آن از نقاط آسیب پذیر شناخته شده در مرورگر اینترنت (IE) ، استفاده کرده است . ماکروسافت بمنظور حل مشکل این نوع از نقاط آسیب پذیر در محصولات خود خصوصا" برنامه مرورگر اینترنت ، patch های امنیتی خاصی را ارائه نموده است . با توجه به امکان بروز حوادث مشابه و بهره برداری از نقاط آسیب پذیر در محصولات نرم افزاری استفاده شده ، خصوصا" نرم افزارهائی که بعنوان ابزار ارتباطی در اینترنت محسوب می گردند ، پیشنهاد می گردد که patch های ارائه شده را بر روی سیستم خود نصب تا حداقل از بروز حوادث مشابه قبلی بر روی سیستم خود جلوگیری نمائیم .

پیشگیری هفتم : محصولات آنتی ویروس

اغلب محصولات تشخیص ویروس های کامپیوتری، عملیات تشخیص خود را بر اساس ویروس های شناخته شده ، انجام خواهند داد . بنابراین اینگونه محصولات همواره در مقابل حملات جدید و نامشخص ، غیرموثر خواهند بود. محصولات فوق ، قادر به برخورد و پیشگیری از تکرار مجدد ، حملات مشابه تهاجمات سابق می باشند. برخی از محصولات آنتی ویروس ، امکان بلاک نمودن ضمائم نامه های الکترونیکی را در سطح سرویس دهنده پست الکترونیکی فراهم می نمایند. پتانسیل فوق می تواند عاملی مهم بمنظور بلاک نمودن ضمائم نامه های الکترونیکی حاوی کدهای مخرب قبل از اشاعه آنان باشد .

پیشگیری هشتم : رعایت و پایبندی به اصل " کمترین امتیاز "

" کمترین امتیاز " ، یک رویکرد پایه در رابطه با اعمال امنیت در کامپیوتر است . بر این اساس توصیه می شود که به کاربران صرفا" امتیازاتی واگذار گردد که قادر به انجام عملیات خود باشند . کدهای مخرب بمنظور تحقق اهداف خود به یک محیط ، نیاز خواهند داشت . محیط فوق ، می تواند از طریق اجرای یک برنامه توسط یک کاربر خاص بصورت ناآگاهانه ایجاد گردد. در این رابطه پیشنهاد می گردد ، پس از آنالیز نوع فعالیت هائی که هر کاربر می بایست انجام دهد ، مجوزها ی لازم برای وی تعریف و از بذل و بخشش مجوز در این رابطه می بایست جدا" اجتناب ورزید.

پیشگیری نهم : امنیت سیستم عامل

حفاظت در مقابل کدهای مخرب می تواند به میزان قابل محسوسی از طریق کلیدهای اساسی سیستم ، کنترل و بهبود یابد. در این راستا از سه رویکرد خاص استفاده می گردد : حفاظت عناصر کلیدی در ریجستری سیستم ، ایمن سازی اشیاء پایه و محدودیت در دستیابی به دایرکتوری سیستم ویندوز NT . در ادامه به بررسی هر یک از رویکردهای فوق ، خواهیم پرداخت .

پیشگیری نهم – رویکرد اول : ایمن سازی ریجستری سیستم

کرم ILOVEYOU از مجوزهای ضعیف نسبت داده شده به کلیدهای ریجستری RUN و RUNSERVICES ، استفاده و اهداف خود را تامین نموده است . مجوزهای دستیابی پیش فرض در رابطه با کلیدهای فوق ، امکان تغییر محتویات و یا حتی ایجاد محتویات جدید را در اختیار کاربران قرار می دهد.مثلا" می توان با اعمال تغییراتی خاص در رابطه با کلیدهای فوق ، زمینه اجرای اسکریپت های خاصی را پس از ورود کاربران به شبکه و اتصال به سرویس دهنده بصورت تکراری فراهم نمود . (پس از ورود کاربران به شبکه ، اسکریپت ها بصورت اتوماتیک اجراء خواهند شد) . بدین منظور پیشنهاد می گردد که مجوزهای مربوط به کلیدهای فوق بصورت جدول زیر تنظیم گردد : (پیشنهادات ارائه شده شامل کلیدهای اساسی و مشخصی است که توسط ILOVEYOU استفاده و علاوه بر آن کلیدهای اضافه دیگر را نیز شامل می شود) :

کلید ریجستری	Groups User /	مجوزهای پیشنهادی
MACHINE\SOFTWARE\Microsoft\Windows کلیدها و زیر کلیدها پارامترهای استفاده شده توسط زیر سیستم های win32	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Write, Execute Full Control Full Control
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run کلیدها و زیر کلیدها شامل اسامی امورد نظر که در هر مرتبه راه اندازی سیستم ، اجراء خواهند شد.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce کلیدها و زیر کلیدها شامل نام برنامه ای که در اولین مرتبه ورود به شبکه کاربر ، اجراء می گردد.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx کلیدها و زیر کلیدها شامل اطلاعات پیکربندی برای برخی از عناصر سیستم و مرورگر. عملکرد آنان مشابه کلید RunOnce است.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions کلیدها و زیر کلیدها شامل تمام تنظیمات Shell Extebsion که از آنان بمنظور توسعه اینترفیس ویندوز NT استفاده می گردد.	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control Full Control

بمنظور اعمال محدودیت در دستیابی به ریجستری ویندوز از راه دور ، پیشنهاد می گردد یک کلید ریجستری ایجاد و مقدار آن مطابق زیر تنظیم گردد :

```
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\SecurePipeServers\winreg
Name: RestrictGuestAccess
Type: REG_DWORD
Value: 1
```

پیشگیری نهم – رویکرد دوم : ایمن سازی اشیاء پایه

ایمن سازی اشیاء پایه باعث ممانعت کدهای مخرب در ابطه با اخذ مجوزها و امتیازات مدیریتی توسط یک (DLL(Dynamic lonk Library می گردد . بدون پیاده سازی سیاست امنیتی فوق ، کدها ی مخرب قادر به استقرار در حافظه و لود نمودن فایلی با نام مشابه بعنوان یک DLL سیستم و هدایت برنامه به آن خواهند بود. در این راستا لازم است ، با استفاده از برنامه ویرایشگر ریجستری ، یک کلید ریجستری ایجاد و مقدار آن مطابق زیر تنظیم گردد :

```
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Session Manager
Name: AdditionalBaseNamedObjectsProtectionMode
Type: REG_DWORD
Value: 1
```

پیشگیری نهم – رویکرد سوم : ایمن سازی دایرکتوری های سیستم

کاربران دارای مجوز لازم در خصوص نوشتن در دایرکتوری های سیستم (winnt/system32 و winnt/system) می باشند . کرم ILOVEYOU از وضعیت فوق ، استفاده و اهداف خود را دنبال نموده است . پیشنهاد می گردد ، کاربران تائید شده صرفا" دارای مجوز Read دررابطه با دایرکتوری های و فایل ها ی مربوطه بوده و امکان ایجاد و یا نوشتن در دایرکتوری های سیستم، از آنها سلب گردد. در این رابطه ، تنظیمات زیر پیشنهاد می گردد :

فایل / فولدر	Groups User /	پیشنهادی
%WINNT% فایل ها ، فولدرها شامل تعداد زیادی از فایل های اجرائی سیستم عامل	Administrators Authenticated Users CREATOR OWNER SYSTEM	Control Full Read, Execute Full Control Full Control
%WINNT/SYSTEM% فایل ها ، فولدرها شامل تعداد زیادی از فایل های DLL ، درایور و برنامه های اجرائی	Administrators Authenticated Users CREATOR OWNER SYSTEM	Control Full Read, Execute Full Control Full Control
%WINNT/SYSTEM32% فایل ها ، فولدرها شامل تعداد زیادی از فایل های DLL ، درایور و برنامه های اجرائی (برنامه های سی و دو بیتی)	Administrators Authenticated Users CREATOR OWNER SYSTEM	Control Full Read, Execute Full Control Full Control