دستورالعمل مقابله با ویروس STUXNET(ویرایش ۸۹/۸/۱)

خواهشمند است به منظور مقابله مقابله با ویروس STUXNET به نکات زیر توجه فرمایید:

۱- دریافت و نصب تمامی اصلاحیه فوق العاده WINDOWS خصوصا اصلاحیه MS10-046(KB2286198),MS10-061(KB2347290),MS10-073(KB981957) به همه کاربران توصیه می گردد. یقینا عدم نصب به موقع اصلاحیه می تواند عواقبی نظیر سرقت اطلاعات سازمانی و آلودگی گسترده به انواع ویروس ها را در پی داشته باشد. جهت دریافت و نصب اصلاحیه های WINDOWS توصیه می گردد سرویس WSUS (WINDOWS SERVER UPDATE SERVICES) راه اندازی گردد.

۲- ویروس یاب شبکه باید معتبر (دارای لیسانس) و به روز بوده و توانایی گزارش گیری از تمامی رایانه های کاربران را داشته باشد.

۳- در جدول زیر مسیر ونام فایل های ایجاد شده توسط ویروس STUXNET معرفی شده است .تمامی رایانه های اداری و صنعتی باید بررسی گردد و در صورت وجود فایل های اشاره شده در جدول این تجهیزات به ویروس آلوده بوده و بایداین فایل ها حذف گردد و سپس مراحل پاکسازی انجام شود. همانگونه که در پی نوشت شماره ۳ پایین جدول توضیح داده شده است ، ابتدا باید از فایل های ردیف ۴و۵و۶و۷و۸ (با علامت ستاره مشخص شده است) به طور امن در یک حافظه جانبی و یا بر روی لوح فشرده کپی برداری شود تا در صورت لزوم در مراحل تحلیل و تشخیص پیشرفته بتوان از این فایل ها استفاده کرد.

لازم به ذکر است که اطلاعات جدید در مورد راههای مقابله با ویروس STUXNET به صورت مستمر در سایت www.nipc.net قرار داده می شود. لذا ضروری است این سایت مرتبا بازبینی شود.

پیدا شد	مسیر فایل	کپی شود
	%Windir%\inf\oem7A.PNF	
	%Windir%\inf\mdmeric3.PNF	
	%Windir%\inf\mdmcpq3.PNF	*
	%Windir%\inf\oem6C.PNF	*
	%Windir%System32\drivers\mrxnet.sys	*
	%Windir%System32\drivers\Mrxcls.sys	*
	%plcProj%\xutils\listen\xr000000.mdx	*
	%plcProj%\xutils\links\s7p00001.dbf	
	%plcProj%\xutils\listen\s7000001.mdx	
	%plcProj%\wincproj\OS(1)\GracS\cc_alg.sav	
	%plcProj%\wincproj\OS(1)\GracS\db_log.sav	
	%plcProj%\wincproj\OS(1)\GracS\cc_alg.sav	
	%plcProj%\wincproj\OS(1)\GracS\cc_tlg7.sav	
	%Windir%\help\winmic.fts	
	%plcProj%\~WRxxxxx.tmp	
	%Windir%System32\drivers\s7otbxsx.dll	
پیدا شد	**مسیر کلید رجیستری**	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\”ImagePath” = “%System%\drivers\mrxcls.sys”	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MrxCls\“Data”.	
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\”ImagePath” = “%System%\drivers\mrxnet.sys”	

پی نوشت ۱ : منظور از آدرس هایی که به صورت %Windir% نوشته شده است شاخه ی C:\Windows است که به دلیل تفاوت در محل قرار گرفتن این شاخه در سیستم های مختلف از % استفاده شده است.

پی نوشت ۲ : منظور از آدرس هایی که به صورت %plcProj% نوشته شده است شاخه ای است که پروژه ی PLC در آن قرار گرفته است که به دلیل تفاوت در محل قرار گرفتن این شاخه در سیستم های مختلف از % استفاده شده است.

پی نوشت ۳ : در صورت امکان اگر مواردی که در ستون **"کپی شود"** با علامت ستاره **"*"** مشخص شده است در سیستم ها یافت شدند آنها را به طور امن در یک حافظه ی جانبی و یا بر روی لوح فشرده نگهداری کنید تا در مراحل تحلیل و تشخیص پیشرفته بتوان از این فایل ها استفاده کرد.

پی نوشت ۴ : برای باز کردن رجیستری کافیست از منوی Start گزینه ی Run را انتخاب نموده و در آن Regedit را تایپ کرده کلید OK را بزنید . پنجره ای که برایتان باز خواهد شد رجیستری Windows می باشد که می توانید با استفاده از این محیط کلید های ذکر شده را از مسیرهای مربوطه پیدا کنید.