رسیدگی به سیستم های آلوده

Abolfazl Hooshiar

MUMS Infrastructure

فهرست محتویات

باسمه تعالی

انتخاب روش جهت رسیدگی به سیستم های آلوده

در هنگامی که یک سیستم به عنوان حمله کننده (Attacker) اعلام می شود کار های زیر باید انجام شود :

۱- خارج کردن سیستم از شبکه و پاکسازی آن توسط یکی روش های ذکر شده(**قسمت روش های پاک سازی**)

۲- نصب بروز رسانی Anti-virus و اسکن کامل سیستم

۳- بروز رسانی کامل ویندوز Windows Update

مروری بر عملکرد بد افزار ها[1]

معمولاً وقتی که یک بد افزار سیستم قربانی را آلوده می کند ، برای عملکرد صحیح خود کار های زیر را انجام می دهد :

۱- از کار انداختن دور زدن و یا تغییر عملکرد Anti-virus سیستم به نحوی که امکان شناسایی یا حذف آن وجود نداشته باشد.

۲- تلاش جهت جلوگیری از نصب و بروز رسانی Anti-virus جدید

a. جلوگیری از دسترسی کاربر به سایت های امنیتی و Anti-virus جهت دانلود یا بروز رسانی Anti-virus
b. جلوگیری از دانلود ، کپی و نصب Anti-virus جدید

۳- تلاش برای اجرای مجدد و در حافظه قرار گرفتن جهت ادامه کار بعد از restart یا Shutdown

a. مخفی سازی فایل های بد افزار
b. در صورت شناسایی شدن malware ، مقاومت در برابر Delete شدن
c. دستکاری ویندوز برای عدم نمایش فایل های Hidden (حتی در صورت تنظیم برای نمایش)
d. اجرا malware به عنوان یک سرویس
e. از کار انداختن سرویس Windows Update

---

[1] Malware – (بدافزار) واژه ای که شامل ویروس ، تروجان ، کرم ، روت کیت و ...

f. قرار دادن مسیر اجرای malware در Startup رجیستری
g. کپی malware در Root درایو های سیستم برای اجرا شدن با دوبار کلیک کاربر روی درایو
h. کپی malware در Root درایو های قابل حمل (فلش دیسک ها) جهت انتشار روی سیستم های دیگر

۴- در نهایت استفاده ای که نویسنده Malware در نظر گرفته است :

a. سرقت اطلاعات
b. تخریب اطلاعات
c. حمله به دیگر سیستم های شبکه محلی یا اینترنت جهت گسترش بیشتر
d. و...

موارد ذکر شده حالت عمومی دارد و بد افزار ها اغلب دارای عملکردی شبیه به موارد فوق هستند . ممکن است تفاوت هایی در حالات و رفتار های آنها وجود داشته باشد.

هدف از بیان موارد فوق برای این بود که بنا به عملکرد عمومی بد افزار ها پس از آلوده شدن سیستم ، جهت پاکسازی آن روش درستی انتخاب شود تا با اتلاف وقت زیاد ، مواجه نشوید.

روش های پاک سازی

۱– نصب مجدد ویندوز

با توجه به دستکاری های بد افزار ، در صورت امکان (بی یا کم اهمیت بودن)، نصب سیستم عامل جدید می تواند در وقت شما صرفه جویی کند.

۲– حذف Anti-virus قبلی نصب Anti-virus جدید

با توجه به عملکرد های ذکر شده در بالا ، احتمال صرف وقت زیاد و عدم موفقیت زیاد است. به دلیل احتمالات زیر:

- کندی سرعت سیستم
- عدم موفقیت در حذف Anti-virus قبلی
- عدم موفقیت در نصب Anti-virus جدید
- عدم بروز رسانی

۳–پاکسازی سریع توسط Anti-virus ثانویه Second Opinion Solution (SOS)

در صورتی که Anti-virus روی سیستم دارید و نمی خواهید آن را حذف کنید ، می توانید از SOS کسپرسکی استفاده کنید. این محصول بصورت موازی و در کنار Anti-virus قبلی شما نصب می شود و هیچ تداخلی با عملکرد آن نخواهد داشت.

http://www.kaspersky.com/downloads/productupdates/downloads-kaspersky-anti-virus-second-opinion-solution

۴–پاکسازی سریع توسط Rescue Disk

Rescue Disk یک سیستم عامل لینوکسی است که روی آن Anti-virus نصب شده و آپدیت است و توانایی بوت سیستم را دارد. نیازی نیست سیستم هیچ کار انجام دهد

این فایل روی CD ، DVD و یا USB flash Disk رایت شده و سپس سیستم را توسط آن Boot می شود . پس از Load شدن سیستم عامل Anti-virus بصورت اتوماتیک باز می شود و سپس از کاربر می خواهد پس از انتخاب درایو های موجود ، روی Start Scan کلیک کند.

این یک حالت مطمئن و سریع برای پاکسازی بد افزار از روی سیستم عامل است. در این حالت هارد دیسک سیستم در حالت آفلاین مورد اسکن قرار می گیرد و هیچ بد افزاری (فایلی) در حالت اجرا نیست و هیچگونه مقاومتی در برابر اسکن و حذف ، اتفاق نخواهد افتاد.

اغلب Anti-virus های مطرح ، امکان دانلود فایل بوت Rescue Disk را برای کاربران گذاشته اند. از قبیل :

- Kaspersky
- Symantec
- Bit Defender
- Mac-Afee

کافیست به وب سایت این شرکت ها رفته و سپس عبارت Rescue Disk را در آن جستجو کنید.

آموزش کامل دیسک نجات را می توانید از مسیر زیر دانلود فرمایید :

http://itc.mums.ac.ir/sites/ITInfra/DocLib1/HowTO-KaspeR-Rescue-Disk-boot.pdf

ابوالفضل هوشیار

کارشناس واحد زیر ساخت