کم اطلاعی امنیتی مدیر ارشد اطلاع رسانی کشور:

همانطور که در شماره پیـشین خبرنامه عنوان شد، پنجمین کنفرانس بین‌المللی انجمن رمز ایران در روزهای پانزدهم الی هفدهم مهر سال جاری به میزبانی دانشگاه صنعتی مالک اشتر تهران برگزار شد. در آخرین نشست روز اول با عنوان **"دسترسی به اهداف چشم انداز بیست ساله در موضوع افتا"** مسئول محترم شورایعالی اطلاع رسانی کـشور اشـاره بـه مطـالبی نمودنـد کـه از کم اطلاعی ایشان نسبت به مقوله امنیت در دنیای سایبر خبر می دهد. جناب آقای دکتر شهریاری در سـخنان خـود به دریافت هرزنامه (ایمیل های spam) در پست الکترونیکی خود و اتلاف زمانی برای مشخص نمـودن سـالم و یـا آلوده بودن پیام ها اشاره کردند و در ادامه با تاکید بر لزوم استفاده از ابزارهای ضدهرزنامه موجود، این سوال را پیش کشیدند که چرا نباید از برنامه های مقابله خارجی استفاده کرد؟! در جواب ایشان مختصراً عرض می شود:

- جناب آقای دکتر! لطفاً با توجه به موضوع نشست، مروری اجمالی بر سند افتا بیندازید: ***بر اساس بنـد ۵-۱ سند راهبرد ملی امنیت فضای تبادل اطلاعات کشور (افتا)، و با توجه به ناامن بودن محصولات خارجی، لزوم بکارگیری و اتکاء به توانایی های داخلی و اهتمام به استفاده از بخش غیردولتی، مورد تاکید می باشد.***
- جناب آقای دکتر! آیا فقط مشکل شما بحث inbox و هرزنامه است؟
- جناب آقای دکتر! مگر شما از ابزارهای اشاره شده، روی سیستم خود نداشـته ایـد کـه بـه ایـن مـشکل برخورد نموده اید؟
- جناب آقای دکتر! برخلاف سخنانی که بیان کرده اید، مالزی و خیلی از کشورهای مشابه دیگر قـادر بـه تولید چنین ابزاری نیستند. در واقع فناوری تولید چنین ابزارهائی در دست معدود کشورها است و آنهـا نیـز در کنار ارائه این ابزارها سیاستهای امنیتی خود را دنبال می کنند. بـرای مثـال در بـین مـالکین ابزارهـا و سازمان های امنیتی آن کشور، توافق هایی در جهت عدم ردگیری برنامه هـائی بـا اهـداف خـاص انجـام گرفته است که تاکنون بعضی از آن توافقات پشت پرده، برملا شده است.
- جناب آقای دکتر! بعضی از این شرکت ها خود طراح و تولید کننـده ابزارهـائی بـرای سـوء اسـتفاده یـا جاسوسی با اهداف مشخص بوده که از حمایت دولت متبوع خود نیز بهره مندند. نمونه های رایگان مشابه ابزارهای فوق در اینترنت به وفور یافت شده و هر شخص مبتدی نیز با کمی اطلاعات مـی توانـد از آنهـا استفاده نموده و آلودگی را دامـن بزنـد. گفتنـی اسـت نـرم افزارهـای Magic Lantern و keyboard graber توسط بعضی از ضد ویروس های غربی شناسائی نمی شود. *(منبع: مهران رایانه)*

کرم فعال Trojan.ns:

W32/Trojan.ns نوعی کرم ایرانی است با حجم ۳۹۳۲۱۶ بایت که در محیطهای ویندوز ۲۰۰۰، XP، NT و ... قابل اجراست. پس از اجرای «تروجان ان اس»، با یکبار Restart شدن سیستم، به محض Login شدن و بالا آمدن ویندوز، سیستم مجدداً خاموش می شود. این کرم فعال (!) که اقدامات مخرب بسیاری انجام می دهد، خود را در فرایندهای در حال اجرا، با نام solari.exe قرار داده و در مسیرهای زیر یک کپی از خود بر جای می گذارد:

```
%Root%\My Document.exe
%Root%\NewFolder.exe
%Root%\Yahoo.exe
%Root%\Windows.exe
%AppData%\alna.scr
%Programs% Startup\solari.exe
```

و خود را در مسیر تمام پوشه ها با نام پوشه جاری کپی می کند:

```
]CurrentPath] [NameFolder]\[NameFolder].exe
```

و با کپی شدن این کرم همراه با فایل Autorun.inf، بر روی درایوهای سیستم و Cool Disk، این کرم منتشر میشود. کرم W32/Trojan.ns با ایجاد کلید زیر در رجیستری با شروع به کار Windows اجرا می شود:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Msconfige = "%Programs%\Startup\solari.exe"
```

این کرم از طریق پاک کردن بعضی از فایلهای سیستم نیز باعث بروز اختلال در یک سری از کارهای ویندوز می‌شود. برای کسب اطلاعات تکمیلی در خصوص جزئیات اقدامات این کرم و راه مقابله با آن، به سایت آزمایشگاه تحقیقات ویروس‌های رایانه‌ای ایمن به آدرس www.imenantivirus.com/encycf/W/W_00502.HTM مراجعه فرمایید.

راهنمای آزمایش امنیت شبکه (قسمت هفدهم – پویش آسیب پذیری ها، بخش اول):

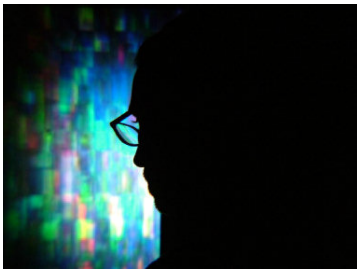
نرم افزارهای پویش آسیب پذیری ها (Vulnerability Scanning) همانند پویشگر پورت عمل می کنند، با این تفاوت که علاوه بر شناسایی میزبان ها و پورت های باز، اطلاعات بیشتری در مورد آسیب پذیری های مرتبط نیز جمع آوری و ارائه می نمایند. نرم افزارهای پویش آسیب پذیری ها – با استفاده از ابزارهای کُنشگرایانه – این امکان را به مدیران شبکه و مدیران سیستم می دهد که پیش از اینکه نفوذگران از یک حفره استفاده کنند، خود آنها اقدام به شناسایی و کشف آن نمایند. نرم افزارهای پویش آسیب پذیری ها درصدد شناسایی حفره های موجود در

تهیه کننده: پشتیبانی فنی شرکت مهندسی مهران رایانه | تلفن: ۲۲۰۵۰۷۸۰ – ۲۶۲۰۲۴۹۳
آدرس: تهران- انتهای بلوار آفریقا – خ شهید طاهری – ایثار۳ – ایثار۲ – شماره ۱۰ – ساختمان مهران | نمابر: ۲۲۰۵۳۹۲۷

میزبان های پویش شده (hosts scanned) می باشند. این برنامه ها همچنین می توانند نرم افزارهای out of date، وصله های اصلاحی برنامه های کاربردی و بسته های به‌روزرسانی سیستم ها را شناسایی نمایند. برای نیل به این هدف، این نرم افزارها اقدام به پویش سیستم عامل‌ها و اکثر برنامه های جاری در میزبان ها نموده و آنها را با دیتابیس خاص مقایسه می کنند. در واقع آنها از یک دیتابیس بزرگ آسیب پذیری بهره می گیرند. پویشگرها علاوه بر اینکه اغلب اطلاعات و راهنمایی های مهمی درباره آسیب های کشف شده ارائه می کنند، می توانند به طور خودکار، خرابی ها و نواقص را نیز رفع و رجوع نمایند. البته این امر هنگامی رخ می دهد که اپراتوری که به پویش آسیب پذیری ها می پردازد، حق دسترسی مدیریتی یا root به میزبان آلوده داشته باشد. *(منبع: مهران رایانه)*

«فانوس جادویی»، اسباب شرمندگی نورتون و مکافی!

فانوس جادویی نرم افزاری است که توسط FBI طراحی و تولید شده است. اولین گزارش هایی که در مورد این نرم افزار منتشر شده، مربوط به MSNBC (در نوامبر سال ۲۰۰۱) و آسوشیتدپرس می باشد. Magic Lantern (فانوس جادویی) در لوای پیوست ایمیل و با سوء استفاده از رخنه های رایج موجود در سیستم عامل ها، در رایانه کاربران نصب می شود. به دنبال افشای عمومی این نرم افزار، مناقشات و بحث و گفتگوهای بسیاری در مورد «توانایی» یا «الزام» نرم افزارهای ضدویروس به شناسایی و ردگیری این جاسوس افزار FBI در گرفته است. در اینجا به عکس‌العمل دو مورد از شرکت های مطرح ضدویروس در این خصوص اشاره می‌شود: **۱.** شرکت تولید کننده ضدویروس McAfee به مقامات FBI اطمینان داده که مکافی این نرم‌افزار را ردگیری نخواهد کرد! **۲.** شرکت سیمانتک نیز در حال همکاری با FBI به منظور ممانعت از شناسایی این نرم‌افزار توسط نورتون است. به گفته یکی از محققان سیمانتک، محصولات ضدویروس نورتون به طور ویژه (!) این تروجان را نادیده می‌گیرد. *(منبع: wikipedia)* ■



- ☑ *نظرات، انتقادات و پیشنهادهای شما برای ما مهم و ارزشمند است: support@MehranCo.com*
- ☑ *منابع اخبار و تصاویر در "پشتیبانی فنی شرکت مهندسی مهران رایانه" موجود است.*
- ☑ *وب سایت رسمی شرکت مهندسی مهران رایانه www.MehranCo.com می باشد.*
- ☑ *استفاده از اخبار و مطالب خبرنامه "با ذکر منبع" بلامانع است.*