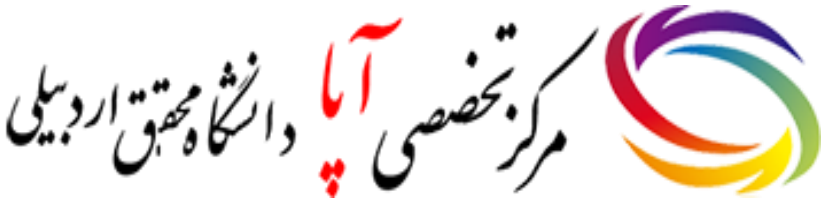
بسمه تعالی

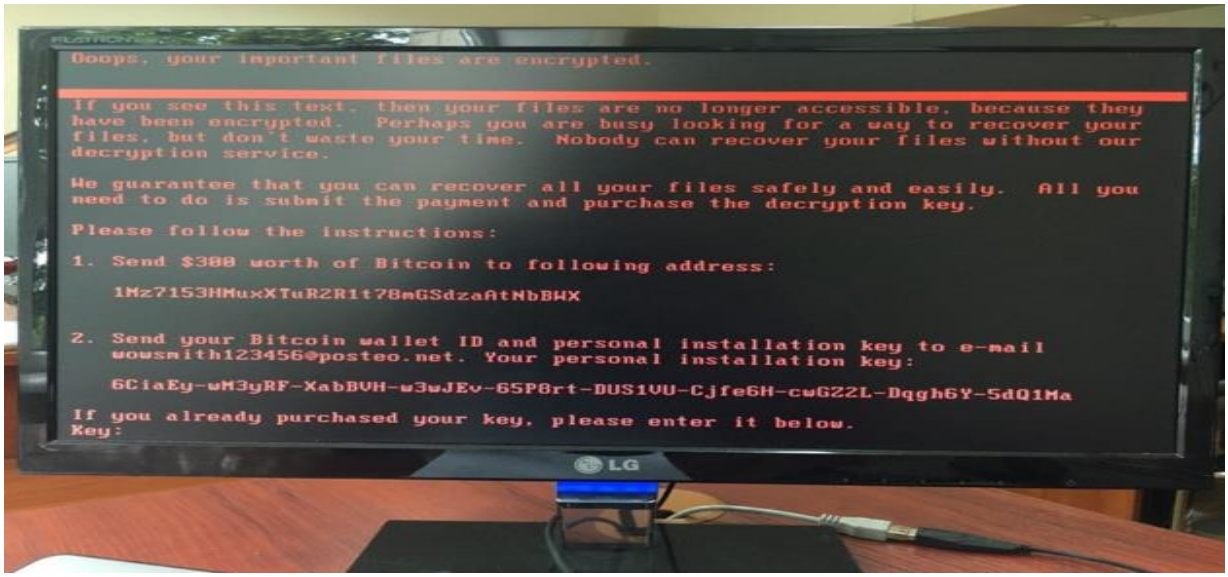


محافظت در برابر باج‌افزار Petya

باج افزار Petya

باج‌افزار (Ransomware) نوعی بدافزار فایلها یا سیستم قربانی را قفل می‌کند و با نمایش پنجره‌ای قفل شدن سیستم یا فایلهای کاربر را به وی اطلاع میدهد و در ازای دریافت مبلغی (باج) کلید رمزنگاری را در اختیار قربانی قرار می‌دهد. با وجود سازوکاری مانند بیتکوین، امکان دریافت مبلغ برای مهاجمین (بدون امکان ردیابی و یا ردیابی دشوار آن) فراهم شده است و مهاجمین از این تکنیک در باج‌افزارهای خود بهره می‌برند. در سالهای اخیر باج‌افزارها رشد فزاینده‌ای داشته‌اند، به نحوی که با ورود گوشی‌های هوشمند و سیستم عامل اندروید، باج‌افزارهای اندرویدی نیز برای آلوده کردن دستگاه‌های هوشمند، توسعه یافتند.

در ۲۷ ماه ژوئن سال ۲۰۱۷ باج افزار Petya کار خود را با آلوده کردن سیستم‌های کامپیوتری آغاز و به سرعت گسترش پیدا کرد. این باج‌افزار یکی از باج‌افزارهای پیچیده‌ای است که در چند روز گذشته، بسیاری از کشورهای جهان به خصوص کشورهای اورپایی را آلوده نموده است. باج‌افزار Petya از آسیب‌پذیری آشکار شده توسط گروه Shadow Brokers به نام ETERNAL BLUE استفاده می نماید که از طریق سرویس SMB و در سیستم‌های کامپیوتری با سیستم عامل ویندوز کار خود را پیش می‌برد. به دلیل قابلیت خود انتشاری این باج‌افزار، سیستم‌های کامپیوتری متصل به یک شبکه مستعد آلودگی می باشند و در صورت عدم رعایت نکات ایمنی به این باج‌افزار آلوده خواهند شد. البته در حال حاضر این آسیب‌پذیری توسط مایکروسافت مرتفع شده است اما کامپیوترهایی که بروزرسانی مربوطه را دریافت ننموده‌اند نسبت به این حمله و آلودگی به این باج‌افزار آسیب‌پذیر هستند.



راهکار های پیشگیرانه

الف- نصب وصله MS 17-010

آسیب‌پذیری یاد شده در پیاده سازی سرویس SMB (پروتکل اشتراک گذاری فایل) در همه نسخه‌های سیستم عامل ویندوز وجود دارد. راهکار اصلی و قطعی مقابله با این آسیب‌پذیری و جلوگیری از سوءاستفاده از آن لازم است آخرین بروزرسانی‌های سیستم عامل ویندوز اعمال گردد. برای این منظور لازم است با استفاده از ابزار بروزرسانی ویندوز (windows update) آخرین بروزرسانی‌های سیستم عامل دریافت شده و نصب گردد.
در خصوص سیستم‌های عامل ویندوز xp و 2003 که مدتی است مورد پشتیبانی شرکت مایکروسافت قرار ندارند، خوشبختانه با توجه به اهمیت موضوع، شرکت مایکروسافت وصله‌های اختصاصی خود را در لینک‌های زیر در دسترس قرار داده است:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

ب- غیرفعال سازی سرویس SMB

چنانچه به دلیلی امکان بروزرسانی سیستم عامل یا نصب وصله مربوطه وجود نداشته باشد لازم است دسترسی به سرویس SMB مسدود گردد. برای این منظور می توان با توجه به نسخه سیستم عامل نسبت به حذف و توقف سرویس و یا مسدودسازی پورت های مورد استفاده آن اقدام نمود.

- غیرفعال سازی سرویس **SMBv1** در ویندوز ۷، ویستا و ویندوزسرورهای 2008 و 2008 R2 با استفاده از محیط powerShell:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 0 –Force
```

- غیرفعال سازی سرویس **SMBv1**در ویندوز ۸، ویندوزسرورهای 2012 و 2012 R2 با استفاده از محیط powerShell:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

توجه کنید که برای اینکه تنظیمات بالا اعمال شود، باید کامپیوتر خود را ریستارت کنید.

ج- مسدودسازی پورتهای مورد استفاده

راهکار جایگزین، بستن پورت‌های 445 و 139 مربوط به پروتکل TCP روی دیواره‌آتش (Firewall) می‌باشد.

د-بروزرسانی آنتی‌ویروس:

تقریبا اکثر قریب به اتفاق آنتی ویروس‌های موجود هش‌های خود را جهت مقابله با این باج افزار بروز رسانی کرده‌اند. با آنها همگام شوید.

ه- توصیه مهم: از فایل های خود به صورت مرتب نسخه پشتیبان تهیه نمایید.