نوشته شده توسط مدیر
پنجشنبه, 11 خرداد 1396 ساعت 00:40 - آخرین بروزرسانی پنجشنبه, 25 خرداد 1396 ساعت 15:37

رویش مقابله با باج افزار wanna cry

wanna cry باج افزاری است که با استفاده از حفره امنیتی ویندوزهایی که بروز نشده اند و از طریق یکی از سرویسهای اشترلک فایل وارد سیستم شما می شود و تقریبا تمامی فایلها اعم از فیلم ، تصویر، فایلهای اجرایی و متنی، فایلهای اتوکد و هر آنچه که تصورش را بکنید را کد می کند و سپس یک فایل متنی برروی دسکتاپ شما ایجاد می نماید با این مضمون که تمامی فایلهای کاربردی شما کدگذاری شده اند و یک کد شناسائی برای شما ارائه می دهد و شما را به سایتی راهنمایی می نماید تا ازطریق آن سایت پرداخت هزینه معمولا مبلغی حدود 300 دلار را بکنید و سپس کلید رمز گشائی فایلها را به شما ارئه می دهد.

از آنجایی که سیستم های عاملی که در ایران مورد استفاده قرار میگیرند اکثر محصول شرکت مایکروسافت می باشند اعم از ویندوز xp ، ویندوز 7، ویندوز 8، ویندوز 10، ویندوزهای سرور و غیره و همه اینها نیز بصورت نسخه غیر اصلی و کرک شده استفاده می شوند معمولا گزینه بروز رسانی خودکار و یا همان update auto در این سیستم های عامل غیر فعال می باشند تا مبادا کرک سیستم عامل از بین برود. لذا مشکلات و حفره های امنیتی موجود از طریق پچ های ارائه شده توسط مایکروسافت از بین نمی روند. حال برای اینکه درگیر چنین مشکلاتی نشوید عملیاتی که در زیر پیشنهاد شده است را انجام دهید تا سیستم عامل و فایلهای شما از آسیب این بدافزار یا ransomware در امان باشد.

1-ویندوز را آپدیت کنید

آپدیت مایکروسافت را از طریق لینک زیر دریافت کنید، با انجام این کار تا حد زیادی می توانید جلوی ورود cry wanna به سیستمتان را بگیرید.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

2-پورت های 135 و 445 را ببندید

بر اساس گزارش های دریافتی از شرکت های ارائه دهنده آنتی ویروس، cry wanna از طریق پورت های SMB(Block Message Server) می تواند به سیستم ها نفوذ کند که با بستن پورت های 135 و 145 می توانید راه نفوذ آن را ببندید.

کاربران عادی معمولا کاری با این پورت ها ندارند و اغلب در سازمان ها و شرکت ها از این پورت استفاده می شود.

برای بستن این پورت ها لازم است با ادمین اصلی سیستم، کنسول را باز کنید.

cmd.exe -> run as administrator

و دو دستور زیر را اجرا کنید. برای اجرای هر دستور باید Enter بزنید.

netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=135 name="Block_TCP-135"

netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=445 name="Block_TCP-445"

3-پشتیبانی از SMBv 1 را غیر فعال کنید

راه دیگر جلوگیری از نفوذ cry wanna غیر فعال کردن SMBv 1 است که باز هم باید cmd را در حالت run as administrator باز کنید و دستور زیر را در آن اجرا کنید:

dism /online /norestart /disable-feature /featurename:SMB1Protocol

همچنین میتوانید:

1- استارت منو را باز کنید.

2- تایپ کنید PowerShell و کلید های Enter+Shift+Ctrl را فشار دهید یا گزینه ی "Run as administrator" را انتخاب کنید.

3- دستورات زیر را تایپ کنید و اینتر را فشار دهید :

Set-SmbServerConfiguration -EnableSMB1Protocol $false

Set-ItemProperty -Path "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParameters" SMB1 -Type DWORD -Value 0 -Force

پس از انجام تمام این کارها ما باز هم به شما توصیه می کنیم که همیشه یک نسخه پشتیبان از سیستم خود تهیه کنید زیرا باجگیرها همیشه در کمین هستند. شاید شما با اجرای دستورات بالا از نفوذ wanna cry راهند در همیشه دیگری باجگیرهای اما بمانید امان در...

همچنین در ویندوز 8 به بالا می توانید از pannel control وارد بخش feature and Program شوید، سپس گزینه ی Turn windows feature on or off را انتخاب کرده و برای گزینه File CIES/SMB1.0 Shearing Support ، را تیک بردارید.

1-ویندوز را آپدیت کنید

آپدیت مایکروسافت را از طریق لینک زیر دریافت کنید، با انجام این کار تا حد زیادی می توانید جلوی ورود cry wanna به سیستمتان را بگیرید.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

2-پورت های 135 و 445 را ببندید

بر اساس گزارش های دریافتی از شرکت های ارائه دهنده آنتی ویروس، cry wanna از طریق پورت های SMB(Block Message Server) می تواند به سیستم ها نفوذ کند که با بستن پورت های 135 و 145 می توانید راه نفوذ آن را ببندید.

کاربران عادی معمولا کاری با این پورت ها ندارند و اغلب در سازمان ها و شرکت ها از این پورت استفاده می شود.

برای بستن این پورت ها لازم است با ادمین اصلی سیستم، کنسول را باز کنید.

cmd.exe -> run as administrator

و دو دستور زیر را اجرا کنید. برای اجرای هر دستور باید Enter بزنید.

```
netsh advfirewall firewall add rule dir=in action=block protocol=TCP
localport=135 name="Block_TCP-135"
```

```
netsh advfirewall firewall add rule dir=in action=block protocol=TCP
localport=445 name="Block_TCP-445"
```

3-پشتیبانی از SMBv 1 را غیر فعال کنید

راه دیگر جلوگیری از نفوذ cry wanna غیر فعال کردن SMBv 1 است که باز هم باید cmd را در حالت administrator as run باز کنید و دستور زیر را در آن اجرا کنید:

```
dism /online /norestart /disable-feature /featurename:SMB1Protocol
```

همچنین میتوانید:

1- استارت منو را باز کنید.
2- تایپ کنید PowerShell و کلید های Enter+Shift+Ctrl را فشار دهید یا گزینه ی "as Run

.کنید انتخاب را "administrator
3- دستورات زیر را تایپ کنید و اینتر را فشار دهید :

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false  Set-ItemProperty -Path "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParameters" SMB1 -Type DWORD -Value 0 -Force
```

پس از انجام تمام این کارها ما باز هم به شما توصیه می کنیم که همیشه یک نسخه پشتیبان از سیستم خود تهیه کنید زیرا باجگیرها همیشه در کمین هستند. شاید شما با اجرای دستورات بالا از نفوذ wanna راهند در همیشه دیگری باجگیرهای اما بمانید امان در cry...

همچنین در ویندوز 8 به بالا می توانید از pannel control وارد بخش feature and Program شوید، سپس گزینه ی Turn windows feature on or off را انتخاب کرده و برای گزینه File CIES/SMB1.0 Shearing Support ، بردارید بر را تیک.