باسمه تعالی

اقدامات عملی جهت پیشگیری و مقابله با باج‌افزار wannacrypt

اردیبهشت ماه ۹۶

۱ مقدمه

در روزهای اخیر باج افزاری تحت عنوان wannacrypt با قابلیت خود انتشاری در شبکه کشور ها شیوع یافته است. براساس رصدهای انجام شده توسط مرکز ماهر، این بدافزار در سطح شبکه کشور ما نیز رصد شده است.

تا این لحظه بیش از ۲۰۰ قربانی این باج افزار در کشور که بیشتر این آلودگی ها در حوزه پزشکی و سلامت شناسایی شده و اقدام جهت رفع آلودگی و پاکسازی آنها از سوی تیم های امداد و نجات مرکز ماهر (مراکز آپا) مستقر در استان های کشور در دست انجام می باشد.

این حمله را می‌توان بزرگترین حمله آلوده نمودن به باج‌افزار تاکنون نامید. این باج‌افزار به نام‌های مختلفی همچون WannaCry، Wana Decrypt0r، WannaCryptor و WCRY شناخته می‌شود. این باج‌افزار همانند دیگر باج‌افزارها دسترسی قربانی به کامپیوتر و فایل‌ها را سلب کرده و برای بازگرداندن دسترسی درخواست باج می کند.

باج‌افزار مذکور برای پخش شدن از یک کد اکسپلویت متعلق به آژانس امنیت ملی آمریکا به نام EternalBlue استفاده می‌کند که مدتی پیش توسط گروه shadowbrokers منتشر شد. این کد اکسپلویت از یک آسیب پذیری در سرویس SMB سیستم‌های عامل ویندوز با شناسه MS17-010 استفاده می‌کند. 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.

تصاویر زیر تصاویر پیامی است که باج‌افزار به قربانی نمایش می‌دهد. پیام باج‌افزار به زبان‌های مختلف قابل مشاهده است.

این باج‌افزار با استفاده از شبکه TOR و استفاده از حساب‌های بیت‌کوین هویت خود را مخفی نموده است. حساب‌های بیت‌کوین متعلق به این باج‌افزار از ساعات ابتدایی آلودگی پول زیادی به عنوان باج دریافت نموده‌اند. تابحال بیش از ۲۸ پرداخت دریافت شده است. یعنی تنها در ساعات اولیه بیش از ۹۰۰۰ دلار باج دریافت شده است.

نحوه تاثیرگذاری این باج‌افزار هنوز به صورت دقیق مشخص نشده اما موردی که مشخص است استفاده از ایمیل‌های فیشینگ و لینک‌های آلوده در سایت‌های غیر معتبر برای پخش باج‌افزار است.

این باج‌افزار فایل‌های با پسوند زیر را رمز می‌کند:

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm, .ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .ps1, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .snt, .onetoc2, .dwg, .pdf, .wk1, .wks, .123, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc

باتوجه به فعالیت این باج افزار در کشور ما، لازم است جهت پیشگیری از آلودگی به آن، مدیران شبکه نسبت به بروزرسانی سیستم‌های عامل ویندوز، تهیه کپی پشتیبان از اطلاعات مهم خود، بروزرسانی آنتی‌ویروس‌ها و اطلاع رسانی به کاربران جهت عدم اجرای فایل‌های پیوست ایمیل‌های ناشناس در اسرع وقت اقدام کنند.

۲ اقدامات پی‌شگی‌رانه

- **نصب وصله MS17-010 :**

آسیب‌پذیری MS17-010 در پیاده سازی سرویس SMB (پروتکل اشتراک گذاری فایل) در همه نسخه‌های 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 ۲۰۰۳ که مدتی است مورد پشتیبانی شرکت مایکروسافت قرار ندارند، خوشبختانه با توجه به اهمیت موضوع، شرکت مایکروسافت وصله‌های اختصاصی خود را در لینک زیر در دسترس قرار داده است:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

tes: 1 - 13 of 13 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size
Security Update for Windows 8 (KB4012598)	Windows 8	Security Updates	5/13/2017	n/a	872 KB
Security Update for Windows XP SP3 (KB4012598)	Windows XP	Security Updates	5/13/2017	n/a	665 KB
Security Update for Windows Vista (KB4012598)	Windows Vista	Security Updates	3/12/2017	n/a	1.2 MB
Security Update for Windows Server 2008 (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.2 MB
Security Update for Windows Server 2003 for x64-based Systems (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	5/13/2017	n/a	951 KB
Security Update for Windows 8 for x64-based Systems (KB4012598)	Windows 8	Security Updates	5/13/2017	n/a	984 KB
Security Update for Windows XP SP3 for XPe (KB4012598)	Windows XP Embedded	Security Updates	5/13/2017	n/a	665 KB
Security Update for Windows Server 2003 (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	5/13/2017	n/a	682 KB
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	5/13/2017	n/a	951 KB
Security Update for Windows Vista for x64-based Systems (KB4012598)	Windows Vista	Security Updates	3/12/2017	n/a	1.3 MB
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.2 MB
Security Update for Windows Server 2008 for x64-based Systems (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.3 MB
Security Update for WES09 and POSReady 2009 (KB4012598)	Windows XP Embedded	Security Updates	3/12/2017	n/a	665 KB

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 مسدود سازی پورت های مورد استفاده آن اقدام نمود.

- **غیر فعالسازی سرویس SMB در ویندوز ۷، ویستا و ویندوز سرورهای ۲۰۰۸ و ۲۰۰۸ R2 با استفاده از محیط powershell:**

- برای غیرفعال کردن SMBV1 روی سرور SMB:

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

- برای غیرفعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -
Type DWORD -Value 0 -Force
```

- برای فعال کردن SMBV1 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 1 -Force
```

- برای فعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -
Type DWORD -Value 1 -Force
```

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

- **غیر فعالسازی سرویس SMB در ویندوز ۸ و ویندوز سرور ۲۰۱۲ به بعد با استفاده از محیط powershell:**

- برای مشاهده وضعیت پروتکل سرور SMB:

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
```

- برای غیرفعال کردن SMBV1 روی سرور SMB:

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

- برای غیرفعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- برای فعال کردن SMBV1 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

- برای فعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

➢ مسدودسازی دسترسی به سرویس SMB بدون توقف سرویس

به عنوان راهکار جایگزین، می توان نسبت به بستن پورت های ۴۴۵ و ۱۳۹ مربوط به پروتکل SMB روی فایروال ویندوز اقدام نمود.

توجه:

خواهشمند است در صورت مشاهده آلودگی به بدافزار گزارش شده، سریعاً با مرکز پاسخگویی و امداد مرکز ماهر به شماره تلفن **۴۲۶۵۱۱۱۱-۰۲۱** تماس و یا از طریق ایمیل **cert@certcc.ir** اطلاع‌رسانی صورت پذیرد.