باسمه تعالی

راهنمای امنیتی مایکروسافت برای 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.

۲ راهبرد دقیق مایکروسافت برای مقابله

دیدن کسب و کار و افرادی که توسط این گونه حملات سایبری تحت تاثیر هستند، دردناک است. تیم ما در روزهای گذشته به سختی کار کرده است تا تمام کارهای ممکن را برای محافظت از مشتریانمان در نظر بگیرد. در اینجا چند نکته وجود دارد که باید ذکر شود :

- اگر شما از ویندوز ویستا، ۷، ۸،۱ و ۱۰ استفاده می کنید : ما در ماه مارس یک بروزرسانی امنیتی را منتشر کردیم که آسیب هایی که این حمالات مورد سواستفاده قرار می دهند را مورد توجه قرار می داد. آن دسته از افرادی که به روزرسانی امنیتی ویندوزشان فعال است در برابر این آسیب پذیری مصون هستند. ما به آن دسته از کسانی که هنوز به روزرسانی امنیتی را اعمال نکرده اند پیشنهاد می کنیم تا فوراً Microsoft Security Bulletin MS17-010 را جایگزین کنند.
- فعال کردن Windows Defender : ما اوایل امروز برای مشتریانی که از Windows Defender استفاده می کنند، یک به روزرسانی منتشر کردیم که این تهدید را به عنوان Ransom:Win32/WannaCrypt تشخیص می دهد. برای بیشتر کردن امینت ، نرم افزارهای ضد بدافزارِ روی سیستم خود را به روز نگه دارید. مشتریانی که از نرم افزار ضدبدافزار شرکت های امنیتی استفاده می کنند می توانند توسط تامین کنندگانشان مطمئن شوند که آیا در امنیت هستند یا نه.
- اگر از ورژن های قدیمی تر ویندوز استفاده می کنید : مشتریانی که از ورژن هایی از ویندوز استفاده می کنند که برای مدت طولانی پشتیبانی دریافت نکرده اند ممکن است که به روزرسانی امنیتی ماه مارس که در بالا به آن اشاره شد را دریافت نکرده باشند. با توجه به تاثیرات بالقوه روی مشتریان و کسب و کارشان ما برای پلتفرم ها، یک به روزرسانی امنیتی سفارشی منتشر کردیم. در حال حاضر به روزرسانی های امنیتی ویندوز XP ، ۸ و ویندوز سرور ۲۰۰۳ به طور گسترده موجود هستند.
- دیگر گام هایی که باید در نظر گرفت : این نوع حمله ممکن است در طول زمان تکامل یابد. بنابراین هر نوع اقدام امنیتی اضافی موجب افزیش سطح حفاظت شما می شود(به عنوان مثال برای محافظت بیشتر در برابر حملات SMBv1 ، مشتریان باید پروتکل های از قبیل legacy protocols روی شبکه شان را مسدود کنند). برخی از حملات مشاهده شده از تاکتیک های رایج فیشینگ مانند malicious attachments استفاده می کنند. بنابراین مشتریان باید هنگام باز کردن مستنداتی که از منابع نامشخص یا غیرقابل اعتماد هستند، هشیار باشند. اطلاعات بیشتر درباره این بدافزار را

می توانید از مرکز حفاظت در برابر بدافزار ماکروسافت روی وبلاگ Windows Security بخوانید.

ما در حال کار با مشتریانمان هستیم تا کمک های بیشتری را مهیا کنیم و این وبلاگ را با اطلاعات دقیق به روز خواهیم کرد.

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

۳ منابع دیگر

دانلود به روز رسانی های امنیتی : *Windows Server 2003 SP2 x64*,*Windows Server 2003 SP2 x86*,*Windows XP SP2 x64*,*Windows XP SP3 x86*,*Windows XP Embedded SP3 x86*,*Windows 8 x86*,*Windows 8 x64*

دانلود ورژن های محلی به روزرسانی امنیتی برای ویندوز XP ، ۸ و ویندوز سرور :

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

خواندن اطلاعات کلی درباره *ransomware*[۱] :

https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

دانلود به روزرسانی امنیتی *MS17-010* :

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

٤ پرسش و پاسخ

من در کجا می توانم راهنمایی های رسمی ماکروسافت را دریافت کنم ؟

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

آیا به روز رسانی برای ویندوز XP و ۲۰۰۳ موجود است؟

بله و لینک دانلود انتهای مقاله زیر موجود است.

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

آیا به روزرسانی روی ویندوزهای بدون مجوز اجرا می شود؟

[۱] باج افزار

توصیه می شود که به روزرسانی روی ویندوز مجوز دار اجرا شود

۵ درباره ویندوز R۲ ۲۰۰۳ چطور؟

به روزرسانی ویندوز ۲۰۰۳ باید روی ویندوز 2003 R2 نیز اعمال شود.

٦ آیا نصب پچ از رخداد *ransomware* جلوگیری می کند؟

خیر. استفاده از *MS17-010* تنها می تواند از پخش بدافزار جلوگیری کند و در برابر آلودگی محافظت نمی کند. بر اساس گزارشات، این بدافزار از مهندسی اجتماعی برای هدف قرار دادن شرکت ها استفاده می کند. به کاربران خود هشدار دهید که در ایمیل های دریافتی ماکروها را باز، کلیک یا فعال نکنند.

- اولویت این است که آنتی ویروس شما بتواند بدافزار را شناسایی کند.
- بررسی کنید که امضاهای شما به روز هستند
- اطمینان یابید که کاربران شما سطح دانش مورد نیاز را دارند تا هرگز ضمایم مشکوک را باز نکنند حتی اگر این ضمایم آیکون آشنایی داشته باشند(مانند PDF). اگر باز کردن یک فایل ضمیمه پیشنهاد اجرای یک برنامه را بدهد، کاربر تحت هیچ شرایطی نباید اجرای برنامه را بپذیرد و در موارد مشکوک کاربر باید با مدیر مشورت کند.
- پیاده سازی فیلترینگ قوی در *O365* :

http://blogs.msdn.com/b/tzink/archive/2014/04/08/blocking-executable-content-in-Office-365-for-more-aggressive-anti-malware-protection.aspx

- تبادل حفاظت آنلاین

http://TechNet.Microsoft.com/en-us/library/jj723164(v=Exchg.150).aspx
http://TechNet.Microsoft.com/en-us/library/jj200684(v=Exchg.150).aspx
http://TechNet.Microsoft.com/en-us/library/jj723119%28V=Exchg.150%29.aspx

راهنمایی های امنیتی برای حفاظت در برابر ***Ransomware***

https://social.technet.microsoft.com/wiki/contents/articles/29787.microsoft-protection-center-security-tips-to-protect-against-ransomware.aspx

۷ آیا ***ransomware*** تنها در زمانی که کاربر دسترسی ادمین روی سیستم کلاینت داشته باشد موثر است؟

خیر. این قسمت از ***ransomware*** مانند دیگر بخش ها، هرگاه اجرا شود، تمام مواردی را که کاربر در آن سطح به آنها دسترسی دارد رمزنگاری می کند و اگر کاربر یک مدیر باشد عواقب آن وسیع تر است. بعلاوه این *ransomware* تلاش می کند تا کپی های سایه(shadow copy) را غیر فعال کند و تغییرات رجیستری در *HKLM hive* که دسترسی سطح کاربر را نیاز دارد ایجاد کند. *ransomware* در زمان تلاش برای پخش شدن، از یک آسیب پذیری استفاده می کند که هرگاه به کار گرفته شود به بدافزار دسترسی سطح سیستم را می دهد. و در کل به معنای این است که این حمله ممکن است بسیار موفق و مخرب باشد حتی اگر کاربر روی سرور یا ایستگاه کاری اصلاح نشده دسترسی سطح ادمین نداشته باشد.

آیا تنها غیرفعال کردن سرور *SMB v1* روی تمام ماشین ها به ما کمک می کند تا در برابر این آسیب پذیری محافظت شویم؟

نخستین راه نصب پچ است. اما در جواب سوال ، بله *SMBV1* باید حذف شود اما به شیوه ای برنامه ریزی شده. لطفاً به لینک زیر مراجعه نمایید.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

آیا ما همچنین نیاز به غیرفعال کردن کلاینت *SMB v1* روی تمام ماشین ها داریم؟

خیر. تنها مولفه سرور *SMBv1* روی ماشین کلاینت غیرفعال شود و نه *Lanmanworkstation*

اثرات حذف *SMBv1* چیست؟

- شما هنوز در حال اجرای ویندوز XP یا *WS2003* تحت یک توافق پشتیبانی سفارشی هستید
- ویندور XP قادر به دسترسی به موارد به اشتراک گذاشته شده توسط ویندوز سرور ۲۰۰۳ یا هر سیستم عامل دیگری نیست.
- ویندوز ویستا و سیستم عامل بالاتر قادر به دسترسی به موارد به اشتراک گذاشته شده روی یک *Windows 2003 Member Server* یا *Domain Controller* (اگر هنوز شما آنها را در محیط داشته باشید) نیست.
- شما تعدادی نرم افزار مدیریتی از کار افتاده دارید از طریق لیست مرورگر *master* شبکه همسایگی نیاز به دستچینی مدیران دارند.

- به منظور "اسکن برای به اشتراک گذاری" پرینترهای چندکاره قدیمی را با سفت افزارهای قدیمی تر اجرا می کند.

لطفاً برای جزئیات بیشتر به مقاله زیر مراجعه کنید.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

اگر ما باید سرویس سرور *smb v1* را غیرفعال کنیم، مقادیر رجیستری برای غیرفعال کردن آن چیست؟

وقتی که شما از ویندوزهای قدیمی تر از ویندوز ۸٫۱ و ویندوز سرور *2012 R2* استفاده می کنید، شما نمی تواند *SMB1* را حذف کنید – اما شما می توانید آن را غیرفعال کنید: *KB 2696547* – برای دریافت نحوه فعال و غیرفعال کردن *SMBv1* ، *SMBv2* و *SMBv3* در ویندوز ویستا، ویندوز سرور ۲—۸، ویندوز ۷ ، ویندوز سرور *2008 R2* ، ویندوز ۸ و ویندوز سرور ۲۰۱۲ به لینک زیر مراجعه کنید.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

چگونه می توانیم بفهمیم که *SMB v1* در محیط ما فعال است. آیا می توانیم به طور فعالانه آن را چک کنیم؟

بله. قبل از استفاده از محیط این مورد را تست کنید.

https://blogs.technet.microsoft.com/ralphkyttle/2017/04/07/discover-smb1-in-your-environment-with-dscea/

ویندوز ۲۰۱۶ و ویندوز ۱۰ راهی را فراهم می کند تا حسابرسان (audit to usage) از *SMBv1* استفاده کنند که در لینک زیر قابل مشاهده است.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

آیا در حال حاضر ویندوز ۱۰ تحت تاثیر است؟

https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

کد سواستفاده به کار گرفته شده توسط *WannaCrypt* طراحی شده تا تنها در برابر ویندوز ۷ و ویندوز سرور ۲۰۰۸ (یا سیستم عامل های قدیمی تر) کار کند بنابراین تا به حال کامپیوترهای ویندوز ۱۰ تحت تاثیر این نوع حملات نبوده است.

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

تا امروز مشتریانی که ویندوز ۱۰ را استفاده می کنند هدف این حملات نبوده اند.

اما می توان گفت که ویندوز ۱۰ نیز نیاز به اصلاح دارد زیرا که این حملات می توانند توسعه پیدا کنند. بعلاوه ، توصیه شده است تا پس از مطالعه کامل لینک زیر SMBv1 از کلاینت ها و ویندوز سرورها حذف شود.
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

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.