# امنیت اطلاعات

بولتن تحلیلی ■ اردیبهشت ماه ۱۳۹۸

در این شماره می‌خوانید:

- بدافزار Wizzmonetize
- آخرین اخبار باج‌گیرها در اردیبهشت ماه
- بسته‌های اصلاحیه نرم افزاری
- خطر، درمیان ایمیل های جعلی


## بدافزار Wizzmonetize

تبلیغ افزار Wizzmonetize یکی از پردردسرترین تبلیغ افزارهای شناخته شده در حملات سایبری به شمار می‌رود. علت این امر آن است که بدافزار با باز کردن تب‌های جدید مرورگر، برای کاربر ایجاد مزاحمت می‌کند، این کار به صورت مداوم و هر چند دقیقه یکبار در سیستم اتفاق می‌افتد و عملا امکان کار با سیستم را مختل می‌کند.

تبلیغ افزارها بدافزارهای تبلیغاتی هستند که موجب نمایش تبلیغات یا ظاهر شدن بنرهای تبلیغاتی متعددی در سیستم شده و شما را تشویق به خرید محصولات یا استفاده از سرویس‌های خود می‌کنند. این نوع از بدافزارها معمولاً ناخواسته و بدون اطلاع کاربر وارد سیستم می‌شوند.

تبلیغ افزار Wizzmonetize محیطی را برای دانلود و اجرای سایر بدافزارها ایجاد می‌کند در نسخه‌های جدید تا جایی که سیستم قربانی ظرفیت داشته باشد، تبلیغ افزارها و تروجان‌هایی با هدف جاسوسی را بر روی آن دانلود و اجرا می‌کند. علاوه بر این که هر کدام از بدافزارهای دانلودی عملیات مخرب خود را انجام می‌دهند، حجم زیادی از حافظه نیز اشغال می‌گردد و در نتیجه باعث کند شدن سیستم می‌گردد.

تبلیغ افزار Wizzmonetize معمولا از طریق سایت های آلوده مثل سایت‌هایی که در آن‌ها بازی‌های آنلاین انجام می‌شود، هرزنامه‌ها، فایل-های به روز رسان جعلی نرم افزارها و غیره بر روی سیستم قربانی دانلود و اجرا می‌شود.

این تبلیغ‌افزار تنها به دانلود یک خانواده بدافزار اکتفا نمی‌کند بلکه هر چه بیشتر بر روی سیستم قربانی باقی بماند نمونه‌های دیگری از خانواده‌های مختلف دانلود و اجرا می‌کند در واقع دانلود این خانواده‌ها بر اساس تصمیم سرور مهاجم بوده و کاملا پویا می‌باشد. از جمله این خانواده‌ها می‌توان به Linkury، EoRezo، Amonitize، ELEX و ... اشاره کرد که اکثرا از دسته تبلیغ‌افزارها و و تروجان‌هایی با هدف جاسوسی هستند.

### علائم آلودگی به بدافزار WizzMonetize:

۱. باز شدن ناگهانی مرورگرهای سیستم و متعاقب آن باز شدن تب‌های پشت سر هم با آدرس‌های متفاوت یکی از علائم آلوده شدن به این بدافزار می‌باشد.

۲. وجود چندین پردازه در لیست پردازه‌های جاری سیستم که همگی دارای اسامی نامفهوم باشند و زیرمجموعه آنها مرورگرهای سیستم باز شده باشند.

۳. وجود یکی از کلید رجیستری‌های زیر در سیستم.

"@\HKEY_CURRENT_USER\SOFTWARE\Microsoft\wewewe"

"@\HKEY_CURRENT_USER\SOFTWARE\Microsoft\ewMon"

"@\HKEY_CURRENT_USER\SOFTWARE\Microsoft\BigTime"

۴. وجود پوشه‌های زیاد در مسیرهای ProgramFiles و ProgramData با اسامی تصادفی و نامفهوم که داخل آنها فایل‌های exe و فایل‌هایی از نوع Config (عموما با نام cast.config) وجود داشته باشد.

اطلاعات فایل‌هایی که در سیستم قربانی دیده شده است:

| عنوان | نمونه MD5 فایل | حجم فایل | تشخیص پادویش | عملکرد |
|---|---|---|---|---|
| 79OMZJEX97ZB.exe | 336c3a2bcec-c642ca7451246be68b757 | ۵۲ KB | Adware.Win32.WizzMonetize.ap | دانلودر بدافزار |
| SecondL.exe | b52bbd6acd78b6f0c-574c6e23497512b | ۷ KB | Adware.Win32.WizzMonetize.ap | دانلودر دوم |
| OneTwo.exe | a8184ae85e3ee-a785e2fb19b861c2c49 | ۳۸ KB | Adware.Win32.WizzMonetize.ap | دانلودر سوم |
| Up.exe | A876962ddcc27402f8e-15f5ab4864248 | ۲/۲۶ MB | Adware.Win32.WizzMonetize.ap | فایل بروزرسان بدافزار |
| AdsShow.exe | bed137e13172448a-47b267a43daabc5e | ۵۳۴ KB | Adware.Win32.FileTour.ap | Redirector |
| wizzcaster_install-er_v2.exe | e05a4306989258d76f-ce906d461be67d | ۳۸ KB | Adware.Win32.WizzMonetize.ap | فایل نصب کننده یک نسخه از بدافزار |
| wizzcaster_uninstall-er_v2.exe | 392862144023af94141d-07d35ab13e73 | ۲۸ KB | Adware.Win32.WizzMonetize.ap | فایل uninstaller بدافزار |

## دانلودر اصلی بدافزار

فایل دانلودر 79OMZJEX97ZB.exe ماژول کوچکی است که تنها شبهه کد base64ی بصورت هاردکد درون خود دارد. با استفاده از یک کلید ثابت این شبهه کد base64 را دیکد کرده و بصورت یک فایل exe مستقل به اجرا در می‌آورد. عملیات اصلی بدافزار و دانلود فایل توسط این فایل دیکدشده انجام می‌گیرد.

سه فایل وجود دارد که فایل دانلودر 79OMZJEX97ZB.exe به محض اجرا، آن‌ها را دانلود می‌کند. مقایسه گونه قبلی این بدافزار با گونه جدید نشان می‌دهد که اسامی سه فایل دانلود شده که در جدول مشخصات فایل‌ها ذکر شد، تا کنون ثابت بوده اما بدافزار توانایی تغییر این فایل‌ها را دارد زیرا این بدافزار XMLای از سرور خود دریافت می‌کند که اسامی و لینک‌های دانلود فایل‌ها در آن قرار دارد ولی این سه فایل از نسخه قدیمی تا کنون اسامی و رفتار ثابتی داشته‌اند. این فایل‌ها عبارتند از OneTwo.exe، SecondL.exe و up.exe .

## شرح عملیات فایل SecondL.exe

این فایل به محض اجرا فایل AdsShow.exe را دانلود و اجرا می‌کند. لینک دانلود فایل بصورت هاردکد در SecondL.exe تعبیه شده است. SecondL.exe فایل دانلود شده را با نام تصادفی در سیستم ذخیره می‌کند.

فایل AdsShow.exe وظیفه باز کردن مرورگر پیش فرض سیستم و redirectکردن مرورگر به سایت‌های تبلیغاتی و بعضا مخرب را دارد. این کار بصورت بی پایان و تا زمانی که حافظه سیستم توانایی داشته باشد ادامه خواهد یافت. بقای این بدافزار در مسیر زیر در پوشه‌های با نام تصادفی ذخیره می‌شود. نام فایل نیز بصورت تصادفی انتخاب می‌شود و با نام Adshow ذخیره نمی‌شود.

AppData%\[Random]\[Random].exe%

## فایل OneTwo.exe

ساختاری مشابه فایل 79OMZJEX97ZB.exe دارد. در واقع آنرا با نام wizzcaster_installer_v2.exe می‌شناسیم.

فایلهای wizzcaster_v2.exe و wizzcaster_uninstaller_v2.exe از طریق این فایل دانلود می‌شوند. این فایل‌ها در مسیر ProgramFiles و با نام تصادفی در پوشه‌های تصادفی ذخیره می‌شوند. فایل wizzcaster_ v2.exe نمونه‌های از نسخه‌های مختلف بدافزار است. اینکه wizzcaster_ installer_v2.exe کدام نسخه از بدافزار را بر روی سیستم نصب می‌کند قبلا توسط نفوذگر مشخص می‌شود و لینک آن در محتوای xml قرار می‌گیرد.

## فایل up.exe

این فایل updater.exe می‌باشد. ساختار این فایل نیز مشابه دو فایل قبلی است و کد آشکار آن با دیکد الگوریتم base64 بدست می‌آید. این فایل همان طور که از نام آن پیداست وظیفه update نسخه‌های قبلی بدافزار را بر روی سیستم برعهده دارد.

توجه کنید که نسخه‌های مختلف بدافزار لینک‌های دانلود متفاوتی از سوی سرور دریافت می‌کنند. این امر باعث تفاوت در نوع تبلیغ افزارها نیز می‌شود.

## روش مقابله و پاک‌سازی سیستم

این بدافزار توسط آنتی ویروس پادویش شناسایی می‌شود و برای این بدافزار پاکسازی انجام می‌شود. جهت پیشگیری از ورود این دست بدافزارها به سیستم پیشنهاد می‌شود ترجیحا وارد سایت هایی که از قبل نسبت به صحت آنها اطمینان ندارید نشوید. همچنین سعی کنید قبل از اجرای فایل‌هایی که بطور ناخواسته وارد سیستم شما شده‌اند آنها را توسط یک آنتی ویروس مطمئن پویش نمایید.

## دزدی اطلاعات توسط بدافزار Bifrose

یکی از بدافزار های خطرناکی که می تواند امنیت سیستم را دچار اختلال نماید بدافزار Bifrose است. بدافزار Bifrose با باز کردن یک درب پشتی (Backdoor) امکان دسترسی از راه دور و نفوذ به سیستم را برای نفوذگر فراهم می کند. این بدافزار دارای قابلیت های زیادی است ولی بیشتر شهرتش به دلیل وجود قابلیت کی لاگر بودن آن است.
Backdoor ها برنامه‌هایی هستند که امکان دور زدن مکانیسم امنیتی یک سیستم را به نفوذگر می‌دهند. میزان شیوع آلودگی این بدافزار به صورت متوسط است. از دیگر قابلیت‌های این بدافزار می‌توان به سرقت اطلاعات، ذخیره تصاویر از محیط سیستم، دستکاری در فایلها و رجیستری و اجرای دستورات از طریق کیبورد و موس اشاره کرد.

### علائم آلودگی به بدافزار Bifrose:

۱. تزریق بدافزار Bifrose به پردازه explorer.exe و iexplorer.exe و عملیات اجرای فایل از این پردازه‌ها
۲. ایجاد یک درب پشتی(Backdoor) روی سیستم قربانی
۳. کپی از خود با نام loadqm.exe به‌صورت رندم در یکی از دو آدرس زیر:
* دایرکتوری ویندوز
* دایرکتوری سیستم
۴. حذف فایل wmisnt.exe در صورت وجود و کپی کردن از روی فایل اصلی با نام wmisnt در مسیر system32
آنتی‌ویروس پادویش این بدافزار را شناسایی کرده و از سیستم حذف می‌کند. جهت پیشگیری از ورود این دست بدافزارها به سیستم پیشنهاد می‌شود از کلیک بر روی لینک‌های مشکوک خودداری نموده و فایل‌های ضمیمه ایمیل‌ها را قبل از اجرا، حتما پویش کنید. همچنین در صورت امکان همیشه سیستم‌عامل و آنتی‌ویروس خود را به روز نگه دارید.


### باج افزار STOP

باج افزار STOP در این ماه بسیار فعال بوده و با رمزگذاری اطلاعات قربانی پسوندهای , norvas, kiratos, etols, hofos را به فایل های آلوده اضافه می‌کند.

### باج‌افزار Scarab

باج افزار Scarab در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند CRABSLKT را اضافه می‌کند.

### باج‌افزار Dharma

باج افزار Dharma در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند txt را اضافه می‌کند. در برخی نسخه‌ها نیز بعد از رمزگذاری پسوند ETH wal یا gate یا را اضافه می کند.

### باج‌افزار Phobos

باج افزار Phobos در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند phoenix را اضافه می‌کند.

### باج‌افزار Paradise

باج افزار Paradise اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند sambo را اضافه می‌کند.

### باج‌افزار WannaOof

باج افزار WannaOof در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل های آلوده پسوند oof را اضافه می‌کند.

# اصلاحیه‌های امنیتی اردیبهشت ماه

شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی می منتشر کرد.
درجه اهمیت ۲۲ مورد از آسیب‌پذیری‌های ترمیم شده توسط این اصلاحیه‌ها (Critical) و ۵۷ مورد از آنها (Important) اعلام شده است.
برای جزئیات بیشتر به لینک زیر مراجعه شود.

https://portal.msrc.microsoft.com/en-us/security-guidance

شرکت ادوبی اصلاحیه‌های امنیتی ماه میلادی می را منتشر کرد.
مجموعه اصلاحیه‌های امنیتی ماه میلادی می برای محصولات زیر منتشر شد:

Flash Player
Acrobat and Reader
Media Encoder

جزئیات بیشتر در لینک‌های زیر قابل مطالعه است:

https://helpx.adobe.com/security/products/flash-player/apsb19-26.html
https://helpx.adobe.com/security/products/acrobat/apsb19-18.html
https://helpx.adobe.com/security/products/media-encoder/apsb19-29.html

به روزرسانی‌های امنیتی سیسکو
سیسکو به روزرسانی‌هایی را برای رفع چندین آسیب‌پذیری در برخی محصولات خود ارائه کرده است.
توصیه می‌شود نسبت به بروزرسانی اقدام شود.
اطلاعات بیشتر در خصوص به روزرسانی‌ها در لینک زیر قابل مطالعه است.
https://tools.cisco.com/security/center/publicationListing.x

# خطر، درمیان ایمیل های جعلی

ارسال ایمیل، یکی از رایج‌ترین روش‌هایی است که کلاهبرداران برای آلوده کردن سیستم‌های شما بکار می‌گیرند. در این روش، ایمیل‌ها بسیار طبیعی به نظر می‌رسند و شکل ظاهری ایمیل‌های سالم را دارند. به طور مثال نام فرستنده معتبر و آشنا بوده و یا نام لینک‌های موجود در متن ایمیل کاملا معتبر به نظر می‌رسد.

## برای جلوگیری از سو استفاده های احتمالی نکات زیر را با دقت بخوانید :

۱. اولین و مهمترین راه؛ باز نکردن ایمیل‌هایی است که فرستنده آن را نمی‌شناسید.

۲. فایل‌های ضمیمه شده را باز نکنید؛ چنانچه ایمیلی از شخصی ناشناس دریافت کردید که حاوی فایل پیوست بود، یا حتی اگر آن شخص را می‌شناختید ولی منتظر ایمیلی از سمت او نبودید، به هیچ عنوان فایل پیوست را باز نکنید. در صورت که ایمیلی از طرف دوست، شرکت و ... که در آن به انجام کاری تاکید شده است دریافت کردید، حتما با فرد مقابل به صورت تلفنی هماهنگ کنید.

۳. وسوسه نشوید؛ چنانچه ایمیلی دریافت کردید که وعده‌های آن‌چنانی از قبیل برنده شدن و... به شما داد، به آن اعتماد نکنید. اگر ایمیلی حاوی متن «شما برنده‌ی ۱۰۰ هزار دلار شده‌اید.» دریافت کردید فریب نخورید.

۴.مراقب ایمیل‌هایی با موضوعات زیر باشید:

خطر! شخصی با نام کاربری شما وارد اینترنت بانک شما شده است

هشدار! گذرواژه شما منقضی شده است

Account has been suspended

Unauthorized login attempt

این ایمیل‌ها شما را به سمت هدف خودشان هدایت می کنند.

۵. اگر در مورد لینک موجود در ایمیل خیلی کنجکاو هستید، روی لینک کلیک نکنید بلکه آدرس آن را کپی کرده و در یک پنجره دیگری آن را باز کنید.

۶. کامپیوتر خود را با نصب یک آنتی ویروس مناسب محافظت کنید.

## آلودگی به باج‌افزار از طریق هک و اقدامات لازم جهت جلوگیری از آن

نفوذ به شبکه یا هک شدن یکی از بزرگترین خطراتی است که همه سازمان‌ها را تهدید می‌کند. فعالیت هکرها این روزها بیشتر به چشم می‌خورد و سازمان هایی که رویکرد پیشگیرانه ای نسبت به تهدیدات ندارند، با عواقب جدی مواجه خواهند شد.

به گزارش پادویش در روزهای اخیر نفوذ هکرها به شبکه و اجرای باج‌افزار توسط آنها، بارها مشاهده شده است. لذا توصیه می‌شود جهت پیشگیری، اقدامات زیر صورت گیرد:

- بستن پورت ریموت و غیرفعال کردن سرویس ریموت دسکتاپ از طریق اینترنت (روی تمام سرورها و نیز سیستمهای دیگر)
- اطمینان از عدم باز بودن پورت ۱۴۳۳ برای سرورهای SQL از سمت اینترنت
- تغییر نام کاربر Administrator در تمام شبکه و سرورها به نامی که قابل حدس زدن نباشد
- اعمال پسوردهای دارای پیچیدگی لازم در تمام اکانتهای ادمین دامین و لوکال سرورها و سایر سیستم ها
- اعمال پسوردهای دارای پیچیدگی لازم برای آنتی ویروس پادویش
- اطمینان از نصب آخرین وصله‌های امنیتی ویندوز و نرم افزارهای کاربردی
- داشتن فرآیند منظم بکاپ‌گیری دوره‌ای و اطمینان از صحت بکاپ‌ها
- استفاده از Tape برای تهیه نسخه پشتیبانی
- اطمینان از فعال بودن داده بان پادویش
- اطمینان از به روز بودن پادویش
- انجام کامل فرآیند امن‌سازی مبتنی بر استانداردهای موجود مانند ISMS و اخذ مشاوره امنیت شبکه

WWW.PADVISH.COM