امنیت اطلاعات

بولتن تحلیلی ■ مرداد ماه ۱۳۹۸

پادویش®
Padvish®

بولتن تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

خبر اختصاصی پادویش

کشف بدافزار جدید استخراج ارز دیجیتال

به گزارش تیم تحلیل بدافزار پادویش، بدافزار جدیدی با نام Eqtonex کشف شده است که از قدرت پردازش سیستم قربانیان برای استخراج ارز دیجیتالی استفاده می‌کند. این بدافزار برای انتشار خود از اکسپلویت EternalBlue و و درب پشتی ایجاد شده توسط ابزار Doublepulsar استفاده می‌کند.

اکسپلویت EternalBlue توسط گروه ShadowBrokers به سرقت رفته و به طور عمومی در سال ۲۰۱۷ میلادی منتشر شد و به عنوان بخشی از حمله جهانی باج افزار WannaCry مورد استفاده قرار گرفت. از آن زمان، بدافزارهای زیادی برای انتشار خود از آن استفاده کرده‌اند. این اکسپلویت، آسیب پذیری موجود در پروتکل SMB نسخه ۱ را هدف قرار می‌دهد.

هدف نهایی بدافزار Eqtonex استخراج ارز دیجیتال است. در حال حاضر بدافزارهایی که از چنین شیوه آلودگی استفاده می‌کنند رو به افزایش هستند. این بدافزار از نوع ماینر بوده و از پردازنده سیستم قربانی برای استخراج ارز دیجیتالی بیت کوین استفاده می کند.

علائم آلودگی به بدافزار Eqtonex :

• وجود یک پردازه با نام تصادفی در سیستم که مقدار زیادی از cpu را به خود اختصاص داده است و باعث کندی سیستم شده است.

• وجود فایلی به نام boy.exe در مسیر %WinDir%

• در مسیر ویندوز، یک پوشه با نام تصادفی که طول آن پنج حرف است، وجود دارد که داخل آن تعدادی dll و یک فایل به نام svchost.exe وجود داشته که بدافزار از آن برای آلوده کردن دیگر سیستم‌های موجود در شبکه استفاده می‌کند (این همان فایل EternalBlue است).

• اگر کاربر در خط فرمان دستور Netsh ipsec static show all را اجرا کند، یک فیلتر با نام ipsec_ply در بین سیاست‌های ارتباطی خود خواهد دید.

شرح عملکرد فایل اصلی بدافزار :

بدافزار بلافاصله پس از اجرا یک نسخه کپی از خودش را در مسیر ویندوز قرار داده و پس از آن یک پوشه با نام تصادفی در مسیر ویندوز ایجاد کرده، یک کپی دیگر از خود را در آن قرار داده و آنرا اجرا می‌کند و سپس یک فایل با نام end.bat را نیز در مسیر ویندوز قرار داده و خود را حذف کرده و ادامه‌ی فعالیت‌ها را به آن نسخه از خود که در پوشه تصادفی در مسیر ویندوز قرار داده بود، واگذار می‌کند.

به طور خلاصه، فعالیت این batch فایل این است که یک فیلتر با نام ipsec_ply ایجاد کرده و پورتهای ۴۴۵ و ۱۳۹ سیستم آلوده را که برای انتقال فایل مورد استفاده قرار می‌گیرند می‌بندد و فقط کسانی که خودش بخواهد توانایی برقراری ارتباط با این سیستم را دارند. با بررسی های صورت گرفته بر روی فایل، این فیلترها در سیستم عامل XP اعمال نمی‌شوند.

پس از اینکه فیلترهای مورد نظر بر روی سیستم قربانی اعمال گردید، فایل end.bat را از سیستم حذف کرده و اقدام به قرار دادن dll های مورد نیاز اکسپلویت Eternalblue و درب پشتی Doublepulsar در فایل تصادفی که در مسیر ویندوز ایجاد کرده بود، می‌کند. همچنین با قرار دادن خود در مسیرهای رجیستری زیر:

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\shell

بقای خود را در سیستم قربانی تضمین کرده تا با هربار اجرای سیستم، فایل بدافزار نیز اجرا شود. در نهایت یک فایل دیگر نیز با نام تصادفی در همان پوشه تصادفی ذکر شده در بالا قرار می‌دهد که با استفاده از توان پردازشی سیستم قربانی، اقدام به استخراج ارز دیجیتال کرده و باعث کندی سیستم قربانی می‌شود.

روال کار فایل s.bat:

روال کار به این صورت است که این فایل با استفاده از فایل EternalBlue (Svchost.exe) اقدام به پیدا کردن IP های فعال در شبکه و بررسی اینکه آیا آسیب پذیر هستند یا خیر می‌کند و نتیجه‌ی بدست آمده را در یک فایل به نام result.txt که آن نیز در همین پوشه است قرار می‌دهد.

روش مقابله و پاک‌سازی سیستم

آنتی ویروس پادویش این بدافزار را شناسایی کرده و از سیستم حذف می‌کند. جهت پیشگیری از آلودگی های احتمالی توسط بدافزارهایی که از آسیب‌پذیری EternalBlue استفاده می‌کنند، پیشنهاد می‌شود از وصله امنیتی ارائه شده توسط مایکروسافت ms17-010 استفاده کنید. بخش جلوگیری از نفوذ (IPS) آنتی ویروس پادویش این گونه آسیب‌پذیری‌ها را شناسایی کرده و از ورود آن به سیستم قربانی جلوگیری می کند.

خبر اختصاصی پادویش

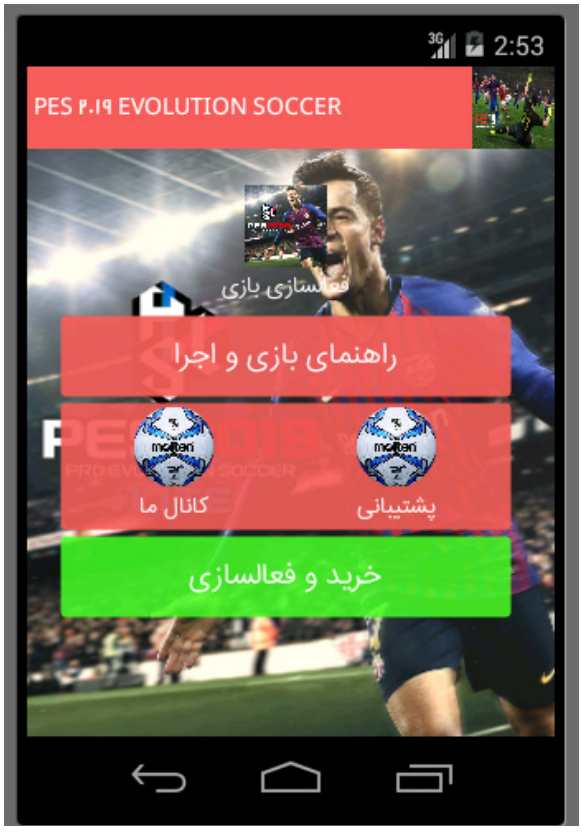
حملات فیشینگ توسط بدافزار اندرویدی GameCo

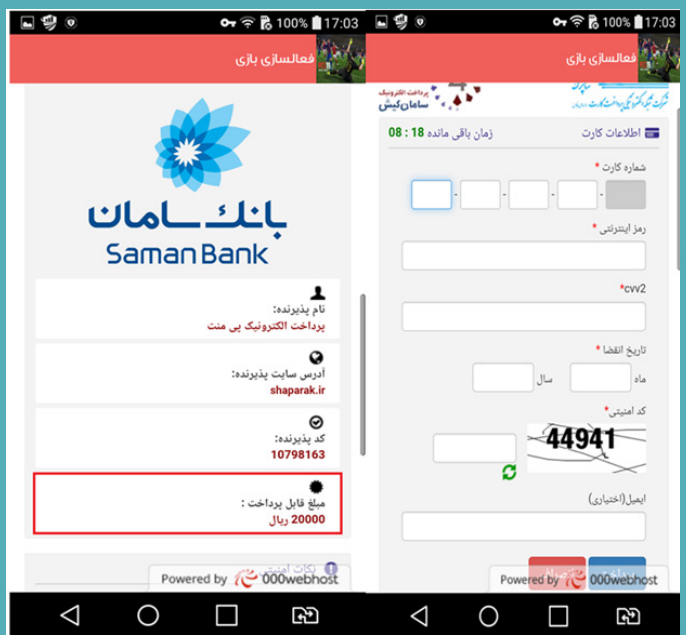
حملات فیشینگی جدیدی توسط تیم تحلیل پادویش شناسایی و تحلیل شده است. بدافزار اندرویدی GameCo از نوعی حمله فیشینگ، برای سرقت اطلاعات حساس حساب‌های کاربری استفاده می‌کند. این بدافزار معمولا شامل اپلیکیشن‌هایی با نام‌های "PES 2019 EVOLUTION SOCCER" ، "خرید شارژ نصف قیمت"، "ESET mobile security" و "بازی‌هایی با نام‌های مستهجن" می‌باشند که همگی دارای یک packagename یکسان به نام ir.game.co هستند. کاربران معمولا تبلیغات این برنامه‌ها را در کانال‌های تلگرامی و یا اینستاگرام مشاهده می‌کنند و در نتیجه با دانلود و نصب این برنامه‌ها آلوده می‌شوند. اغلب مهاجمان با ترغیب کاربران در جهت دستیابی به امکانات بیشتر در برنامه‌های نصب شده، از پرداخت‌های درون برنامه‌ای استفاده می‌کنند.

در این گزارش به طور مثال اپلیکیشن "PES 2019 EVOLUTION SOCCER" را بررسی می‌کنیم. این برنامه ادعا می‌کند که با پرداخت هزینه، به شما امکان مشاهده و استفاده از امکانات بازی را می‌دهد. اما در واقع صفحه پرداخت آن یک صفحه پرداخت جعلی بوده که اقدام به سرقت اطلاعات حساب بانکی کاربران می‌نماید. همچنین این برنامه دارای پکیج‌های تبلیغاتی برای نمایش تبلیغات در برنامه، نیز می‌باشد. بدافزارنویس، صفحات جعلی پرداخت را بر روی host های رایگان که عموما فیلتر هستند قرار داده است، در نتیجه برای اینکه بتواند صفحات جعلی پرداخت را برای کاربر باز کند، کاربر را ملزم می‌کند که برای دستیابی به امکانات برنامه از فیلترشکن استفاده کند. به طور مثال در این اپلیکیشن برای دستیابی به این هدف، اینگونه وانمود می‌کند که "به علت خارجی بودن برخی سرورهای پشتیبانی آفلاین برای اجرای بدون مشکل برنامه از فیلترشکن استفاده کنید. "

در این اپلیکیشن برای اتصال به اینترنت و دریافت دیتا از کلاس DownloadTask، استفاده شده است و برای نمایش اطلاعات ورودی در ویوهای اکتیویتی اصلی، از فایل‌های json که در مسیر assets برنامه قرار گرفته اند، استفاده می‌شود. فایل‌های json به نام‌های (datas/data.json و menu/menu.json و title/title.json) است. هریک از این اطلاعات مختص به یک ویو خاص در اکتیویتی های مختلف برنامه می‌باشند. اطلاعات فایل json پارس شده و کد مربوط به هربخش، جهت نمایش در ویو مدنظر لود می‌شود.

بعد از پارس شدن فایل‌های json و اجرای کدهای آنها در برنامه، اهداف زیر دنبال می‌شود:





```
LoadCounter: undefined
PAN_Array: undefined
PAN_Name: undefined
PAN_Name_Temp: undefined
PANCounter: undefined
PasswordSkippedFields: undefined
requestDetails: { ... }
  documentUrl: undefined
  frameAncestors: [ ]
  frameId: 0
  ip: null
  method: "POST"
  originUrl: "https://newhoster.000webhostapp.com/
  Source/Saman/payment=5698542365.php?amount="
  parentFrameId: -1
  proxyInfo: { ... }
  requestBody: { ... }
    formData: { ... }
      CARD1: (1) [ ... ]
      CARD2: (1) [ ... ]
      CARD3: (1) [ ... ]
      CARD4: (1) [ ... ]
      CVV2: (1) [ ... ]
        0: "123"
        length: 1
        <prototype>: [ ]
      EMAIL: (1) [ ... ]
        0: ""
        length: 1
        <prototype>: [ ]
      MONTH: (1) [ ... ]
        0: "12"
        length: 1
        <prototype>: [ ]
      PASSWORD: (1) [ ... ]
        0: "123456789"
        length: 1
        <prototype>: [ ]
      YEARS: (1) [ ... ]
      <prototype>: { ... }
    <prototype>: { ... }
  requestId: "1019"
  tabId: 22
  timeStamp: 1564818770800
  type: "main_frame"
  url: "https://newhoster.000webhostapp.com/Source/Saman/token.php"
  <prototype>: { ... }
RequestUrlHostName: undefined
SelectedValue: undefined
SelectedValueLength: undefined
SkipFieldFlag: undefined
```

• با فشرده شدن کلیدهای "کانال ما" و "پشتیبانی" ، یک اینتنت توسط اندروید برای باز کردن آدرس‌های
https://telegram.me/joinchat/AAAAAEFEG5G1Ym_DVHK-Vw
https://telegram.me/joinchat/AAAAAEHQb0xPRcm6t3_1qA
به مرورگر ارسال می‌شود.

• با فشرده شدن کلید "فعالسازی بازی" ، یک اینتنت توسط اندروید برای باز کردن آدرس https://newhoster.000webhostapp.com/Source/Saman/payment=5698542365.php?amount=20000 به مرورگر ارسال می‌شود. این آدرس در واقع صفحه جعلی "درگاه بانکی" می‌باشد که کاربر به سمت آن ارجاع داده می‌شود.

• اگر کاربر برروی گزینه "راهنمای بازی و اجرا" کلیک کند. اکتیویتی مربوطه باتوجه به اطلاعات فایل json که در مسیر assets/data/1.json قرار گرفته است، لود شده و به کاربر نمایش داده می‌شود. در توضیحات نمایش داده شده، ذکر می‌شود که "به علت خارجی بودن برخی سرورهای پشتیبانی آفلاین، برای اجرای بدون مشکل برنامه از فیلترشکن استفاده کنید".

• در این برنامه قسمتی به نام "جهت فعالسازی از دکمه زیر استفاده کنید" وجود دارد که به محض کلیک برروی آن مستقیما کاربر به سمت صفحه پرداخت جعلی درگاه بانکی https://newhoster.000webhostapp.com/Source/Saman/payment=5698542365.php?amount=20000 ارجاع داده می‌شود. در این بخش، به محض وارد کردن اطلاعات کارت بانکی کاربر و فشردن دکمه پرداخت، تمام اطلاعات کارت بانکی کاربر برای سرور مهاجم https://newhoster.000webhostapp.com/Source/Saman/token.php ارسال می‌شود. بدین‌ترتیب مهاجم با در دست داشتن کل اطلاعات کارت بانکی، می‌تواند به راحتی از حساب کاربر برداشت کند.

سایر نمونه‌ها و URLهای آلوده:

نمونه‌های دیگری از این خانواده را در جدول زیر مشاهده می‌کنید. هش(MD5) هریک از این اپلیکیشن‌ها در جدول موجود است و روبروی هرکدام، URLهایی مشخص شده که به‌عنوان درگاه پرداخت بانکی جعلی، برای هر نمونه می‌باشد. به محض کلیک کاربر جهت پرداخت‌های درون برنامه‌ای، به سمت URL آلوده هدایت می‌شود و با وارد کردن اطلاعات کارت بانکی، این اطلاعات به سمت سرور مهاجم ارسال خواهد شد. بسیاری از این سرورها غیرفعال شده‌اند ولی تعدادی از آنها ازجمله نمونه‌ای که در بالا توضیح داده شده، هم اکنون فعال هستند. برای اطلاعات بیشتر می توانید آدرس زیر را مشاهده کنید:
https://threats.amnpardaz.com/malware/trojan-android-phishing-/gameco

URL	MD5
http://fast-p-a-y.ga/Asan-Pardakht-12	65af54d4e7dc62e0f7ba954d48c9dea4
http://panel.kakopay.com/startpay/paylink/4A6560938F	985558b2085182fe5bf9c1477953c779
http://pay.warlord.it/reza-moqadam/payment=5698542365.php?amount=15000	9ed6fad40e6705e5d466cb2cec202e35
http://dargah-sighehe.tk/eh/pay?random=8662239	728c7e6e5bc12f7ffa2411c32dc26012
http://goo.gl/eAi4th	581d0d936b410726e82ae1cae2e016e8
http://panel.javadpay.com/startpay/paylink/8E412751CB	b5f0a7e66360bb162fd2648e4c6cd402
http://shaparak.life/payment=11543459sh?amount=20000	4a63cf04a647d1b116582b94c1142758
https://ranjbarpay.com/bmp-shaparak/payment=11543459sh?amount=20%2C000	26233c8989add48251454cf39399c0e5
http://sep-shaparakea.ml/payx	3b99a9c10eb8ec5b0cec385f7eea1c90
http://asan.samanpay.info//payment=11543459sh?amount=10%2C000	89244a6d35a0c179a83896a43ede629f
http://panel.baranpall.com/startpay/paylink/9330CC0884	6a967f989b33189230850e925251b8b2
http://goo.gl/KbYVJR	b99cadd8778f8bff3d4ca026dc1853f7
http://fucku4.tk	9fa5c2b39c987ced99c00e7addabdc0c
http://ertyyfjkhklkdthffxdhdcfhndctgnhdfhshtrdtfytj.xyz/payment.html	bbc59207bd1bb1e056f53ce010f50140
http://panel.baranpall.com/startpay/paylink/47AD5E6698	1a15fdd7b3836c4a8fb422c778b5903e
http://media-tarfand-page.tk/Saman	a66cc4fe3524ddd700b5ef8e8e307afe
http://panel.baranpall.com/startpay/paylink/CE5C0358E2	8e9ede958eda088e1394bc66ec0b8e58
https://newhoster.000webhostapp.com/Source/Saman /payment=5698542365.php?amount=20000	78822db4d035d0e0da50fb63238fc6d3
https://newhoster.000webhostapp.com/Source/Saman /payment=5698542365.php?amount=20000	3bcca8307f6e8a5ad71cf7711d6450cc
http://online-pardakht.com/i	b06c9738ccf3b8e30f85a6ffdad49a42
http://prdakht.website/y	ba2f5a9cbf3fdf9a1262f0ae309286a5
http://185.183.97.102/s/pna/index.php	cbe44a0d5cf6f5c3132fedc01444a570
http://aplsam.cf/meleet/?price=20,000	bf2826e76faa311d908457904b93dbbf
http://1o2.ir/P4game	f9a84cf6f3b1a0a1433aba6d593c4e20
http://panel.baranpall.com/startpay/paylink/75D1A3F8EC	47af6c2b3b471b38c1cf015f714fc274
http://mamad.samanpay.info//payment=11543459sh?amount=20000	93d6ab738d20a434d832a40de6925eb2
http://www.rsarayan.legendaryhost.ir/suorse%20ha/%40UlteraAddBot /data/catch/final/payment=11543459sh?amount=20%2C000	de8d95f5e75a8e3b65dcaf15cd834dc0
http://asnpy.website/y	70e2bcb897c8320b4b8e100fe5c0552a
http://soltahnhost.cpanelserver.ir	30c372b3e71b29482f6007a41b0845a0
http://samanshap.cf/payment.php	d50bc0b2d9a671781aacc05d8494ea85
http://asay.vip/saman.ir	6f175982641a8a1f86845c5f0a16cb63
http://shahprc.tk/G/payment=5698542365.php?amount=20000	3d1ac8a778938fdf881278a353ea12ac
https://ahesmaeilzadeh.ir/bmp-shaparak/payment=11543459sh?amount=20%2C000	7647618215232ea1d7c16e4cd4fd96c4
http://asanplpla.website/y	4a0218018b5a1a4ab48dad61d6f6dce4
http://asanpardakhet.com	b71964f27e676caddd13a34e7367e9ee
http://mutluyillar.xyz/lib/payment=11543459sh.php?amount=20000	a20c0359ed41bb601a9a66a241d114f3
https://bit.ly/2RuuZom	ec6011a9766a58575bf6ff7bbe054d5f
http://best98.ga	cf24f835f56a1d634dd8e352d50403f1
https://worldsource.yoozhosting.ir/asan-shaparak/payment=11543459sh?amount=20%2C000	b9efb4321e5eb8e40b8415d90e910edb
http://panel.baranpall.com/startpay/paylink/5D730A4A03	0d9de8ab47819f43a037086e812c55bf
http://shaparak.bid/payment=11543459sh?amount=10,000	a56916d02fd79e19ec8c0d75bf25e4f5
https://www.asaplmir.sevenserver.eu/cgi/new/sqq/payment	ace3f6f9541a7d880cbf46786cafd25c
https://whimsey.xyz/Sara-khodadaddi/payment=5698542365.php?amount=10%2C000	db4fdf215300f4fc75c29eff5ed47431
https://shargestar.com/p	5430a08f2f8e5deb6659a33890569a79
http://yon.ir/QhYer	e6669155a551d8deffd184bddd440190
https://dante.speed-host.ir/asan-shaparak/payment=11543459sh?amount=50%2C000	8626f418dc822fb5a491e20763d19544
http://irshahparak.website	c85e2689b7f061ea7c04392c86f99c1f

روش مقابله و پاک‌سازی سیستم

آنتی‌ویروس پادویش این بدافزار را شناسایی کرده و از دستگاه حذف می‌کند.

روش های پیشگیری از آلوده شدن گوشی:

۱. از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر جلوگیری کنید.

۲. هنگام نصب برنامه‌های موبایلی به مجوزهای درخواستی دقت کنید.

۳. از فایل‌ها و اطلاعات ذخیره شده در گوشی پشتیبان گیری مداوم انجام دهید.

۴. از نسخه‌های غیررسمی برنامه‌ها استفاده نکنید. برنامه‌هایی مانند تلگرام نسخه‌های غیررسمی زیادی دارند، بیشتر این برنامه‌ها از طریق کانال‌های تلگرامی انتشار می‌یابند.

۵. از هر اپلیکیشنی که خرید می‌کنید بعد از ورود به صفحه پرداخت، دقت کنید که صفحه‌ی موردنظر از نوع فیشینگ نباشد.

اصلاحیه‌های امنیتی مرداد ماه

شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی «اوت» منتشر کرد.
برای جزئیات بیشتر به لینک زیر مراجعه شود.

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

شرکت ادوبی اصلاحیه‌های امنیتی ماه میلادی «اوت» را منتشر کرد.
جزییات بیشتر در لینک‌های زیر قابل مطالعه است:

https://helpx.adobe.com/security/products/after_effects/apsb19-31.html
https://helpx.adobe.com/security/products/character_animator/apsb19-32.html
https://helpx.adobe.com/security/products/premiere_pro/apsb19-33.html
https://helpx.adobe.com/security/products/prelude/apsb19-35.html
https://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html
https://helpx.adobe.com/security/products/acrobat/apsb19-41.html
https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html
https://helpx.adobe.com/security/products/photoshop/apsb19-44.html

به‌روزرسانی‌های امنیتی سیسکو
سیسکو به‌روزرسانی‌هایی را برای رفع چندین آسیب‌پذیری در برخی محصولات خود ارائه کرده است.
توصیه می‌شود نسبت به به‌روزرسانی اقدام شود.
جزئیات آسیب‌پذیری‌ها در جدول زیر ارائه شده است.

https://tools.cisco.com/security/center/publicationListing.x

اخبار باج افزارها

باج‌افزار Phobos

این باج‌افزار همچنان سهم قابل‌توجهی از آلودگی‌ها را به خود اختصاص داده است که در کشورمان نیز شیوع دارد و به فایل‌های آلوده پسوندهای help, banjo را اضافه می‌کند.

باج افزار STOP

باج افزار STOP در این ماه بسیار فعال بوده و با رمزگذاری اطلاعات قربانی پسوندهای، vesad ,nvetud ,cosakos, ntuseg,brusaf,pedro را به فایل‌های آلوده اضافه می‌کند.

باج‌افزار Maoloa

باج افزار Maoloa اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند Hades666 را اضافه می‌کند.

باج‌افزار Dharma

باج افزار Dharma در نسخه جدید اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند com2 را اضافه می‌کند. در برخی نسخه‌ها نیز بعد از رمزگذاری پسوند Q1G یا Acuf2 را اضافه می‌کند.

باج‌افزار Cryakl

باج افزار Cryakl اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند junior را اضافه می‌کند.

باج‌افزار Haka

باج افزار Haka اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند haka را اضافه می‌کند.

باج‌افزار Lilocked

باج افزار Lilocked اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند lilocked را اضافه می‌کند.

باج‌افزار Nemesis

باج افزار Nemesis اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند WECANHELP را اضافه می‌کند.

باج‌افزار Dragon

باج افزار Dragon اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند locked را اضافه می‌کند.

باج‌افزار GonnaCry

باج افزار GonnaCry اقدام به رمزگذاری اطلاعات قربانی کرده و به فایل‌های آلوده پسوند GNNCRY را اضافه می‌کند.

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