هکرها با استفاده از بدافزار ارتقا یافته‌ی Agent Tesla، رمزهای عبور WiFi را سرقت می‌کنند.

خلاصه‌ی خبر:

Agent Tesla یک سارق اطلاعات[1] قابل خرید از فوروم‌ها و دارای قابلیت keylogging و تروجان دسترسی از راه دور (RAT) است. این بدافزار که حداقل از سال ۲۰۱۴ تاکنون فعال است و به تازگی در لیست "۱۰ مورد از رایج‌ترین تهدیدات" رتبه‌ی دوم را به خود اختصاص داده است، اخیراً بوسیله‌ی صدور فرمان netsh نه تنها لیستی از WiFiهای دردسترس و رمزهای عبور هر پروفایل، بلکه اطلاعات گسترده‌ای را در مورد سیستم مانند کلاینت‌هایFTP، مرورگرها، نام‌کاربری، نام رایانه، نام سیستم‌عامل، معماری CPU، رم و غیره را نیز استخراج می‌کند.

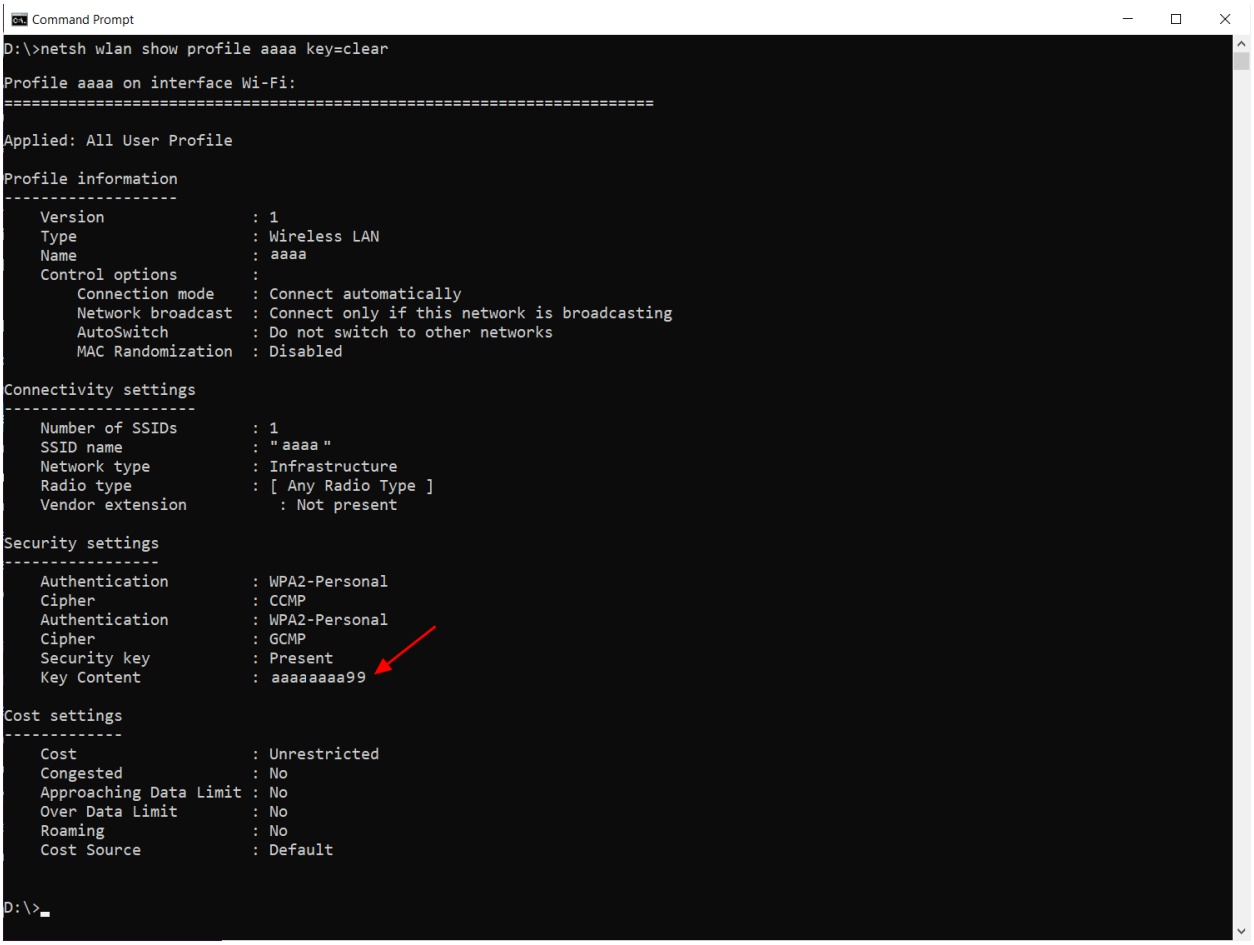
[1] Info-stealer

برخی از انواع جدید بدافزارهای سرقت اطلاعاتی Agent Tesla اکنون دارای یک ماژول اختصاصی برای سرقت رمزهای عبور WiFi از دستگاه‌های آلوده هستند، اطلاعات کاربری که ممکن است در حملات بعدی برای گسترش و به خطر انداختن سایر سیستم‌ها در همان شبکه‌ی بی‌سیم استفاده شود.

نمونه‌های جدید به شدت مبهم‌سازی شده‌اند و توسط نویسندگان بدافزار طراحی شده‌اند تا بوسیله‌ی صدور یک دستور netsh با یک آرگومان **wlan show profile** و لیست‌کردن تمام پروفایل‌های WiFi در دسترس، اطلاعات کاربری بی‌سیم را از رایانه‌های به خطر افتاده جمع‌آوری کنند.

همانطور که تیم اطلاعات تهدید Malwarebytes دریافته‌اند، برای به‌دست‌آوردن رمزهای عبور WiFi از SSIDهای کشف شده (نام شبکه‌های Wi-Fi)، سارق اطلاعاتی Agent Tesla برای نمایش و استخراج رمزعبور، برای هر پروفایل یک دستور جدید *netsh* را با اضافه‌کردنSSID و یک آرگومان *key=clear* صادر می‌کند.

به گزارش Malwarebytes فایل اجرایی علاوه بر پروفایل‌های Wi-Fi، اطلاعات گسترده‌ای را در مورد سیستم شامل کلاینت‌های FTP ، مرورگرها ، بارگیری فایل‌ها ، اطلاعات دستگاه (نام کاربری، نام رایانه، نام‌سیستم عامل، معماری CPU، رم) جمع آوری کرده و آن‌ها را به لیست اضافه می‌کند.



۱- رمز عبور WiFi نشان داده شده

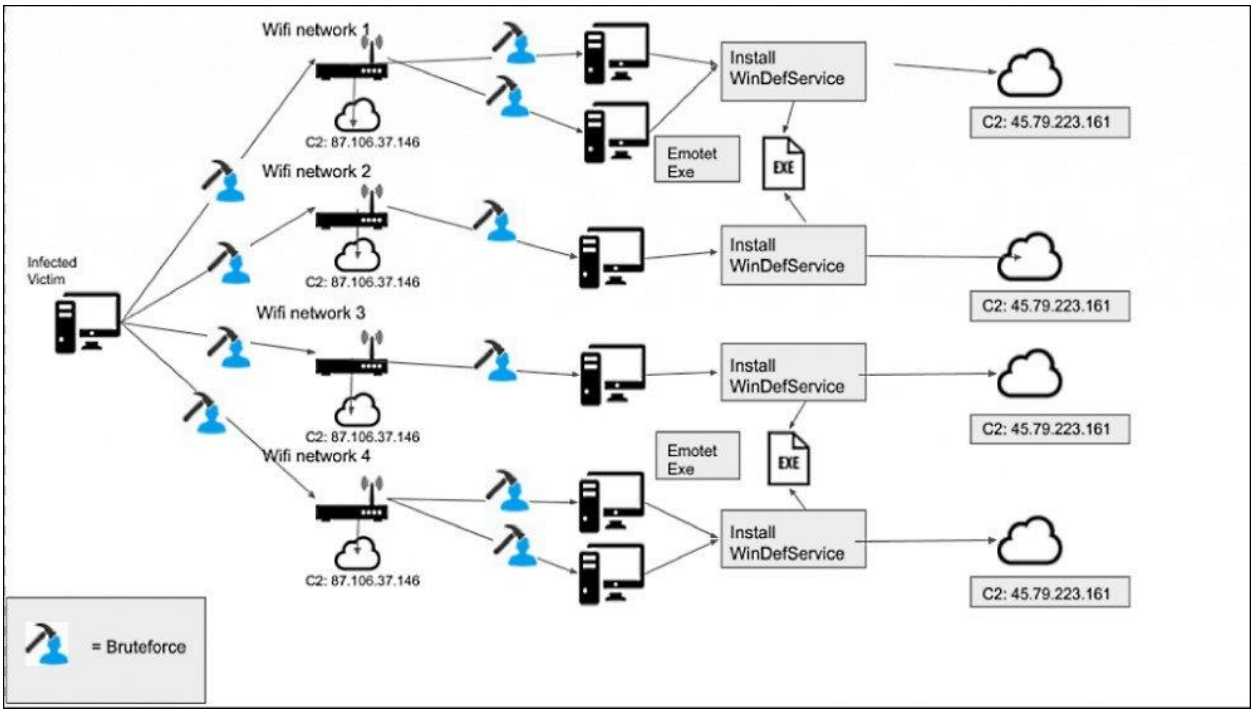
Emotet نیز به ماژول WiFi مجهز شد.

Agent Tesla تنها بدافزاری نیست که اخیراً با قابلیت‌های WiFi به روز شده است. یک نمونه از Trojan Emotet که در اوایل سال جاری مشاهده شد نیز با یک ابزار توزیع‌کننده‌ی WiFi مستقل، به‌روزرسانی شده بود که به آن امکان می‌داد قربانیان جدید متصل به شبکه‌های بی‌سیم ناامن اطراف را آلوده کند.

محققان Binary Defense که نمونه‌های تازه به‌روزشده‌ی Emotet را کشف کرده بودند، به BleepingComputer گفتند، این توزیع‌کننده‌ی مستقل حداقل دو سال توسط تیم Emotet و بدون اینکه هیچ تغییر قابل توجه‌ای بوجود آید، مورد استفاده قرار گرفته‌است.

به‌گفته‌ی یک محقق که شاهد استفاده از توزیع‌کننده‌ی Wi-Fi Emotet بر روی سراسر شبکه‌های یکی از مشتری‌های خود بوده‌است، توسعه‌دهندگان Emotet بعداً این توزیع‌کننده را به یک ماژول کرم Wi-Fi همه‌جانبه، ارتقا داده و از آن علیه کاربران عادی استفاده کردند.

با تمرکز جدید تیم Emotet بر روی این ماژول توزیع‌کننده‌ی WiFi، آن‌ها در مسیر مستقیمی جهت توسعه‌ی یک ماژول کرم Wi-Fi بسیار توانمند و بسیار خطرناک قرار دارند که با استفاده‌ی فعال از آن در عمل، علیه کاربران معمولی، روز به روز حضور پررنگ‌تری خواهد داشت.



۲- توزیع‌کننده‌ی **WiFi** متعلق به **Emotet** در عمل

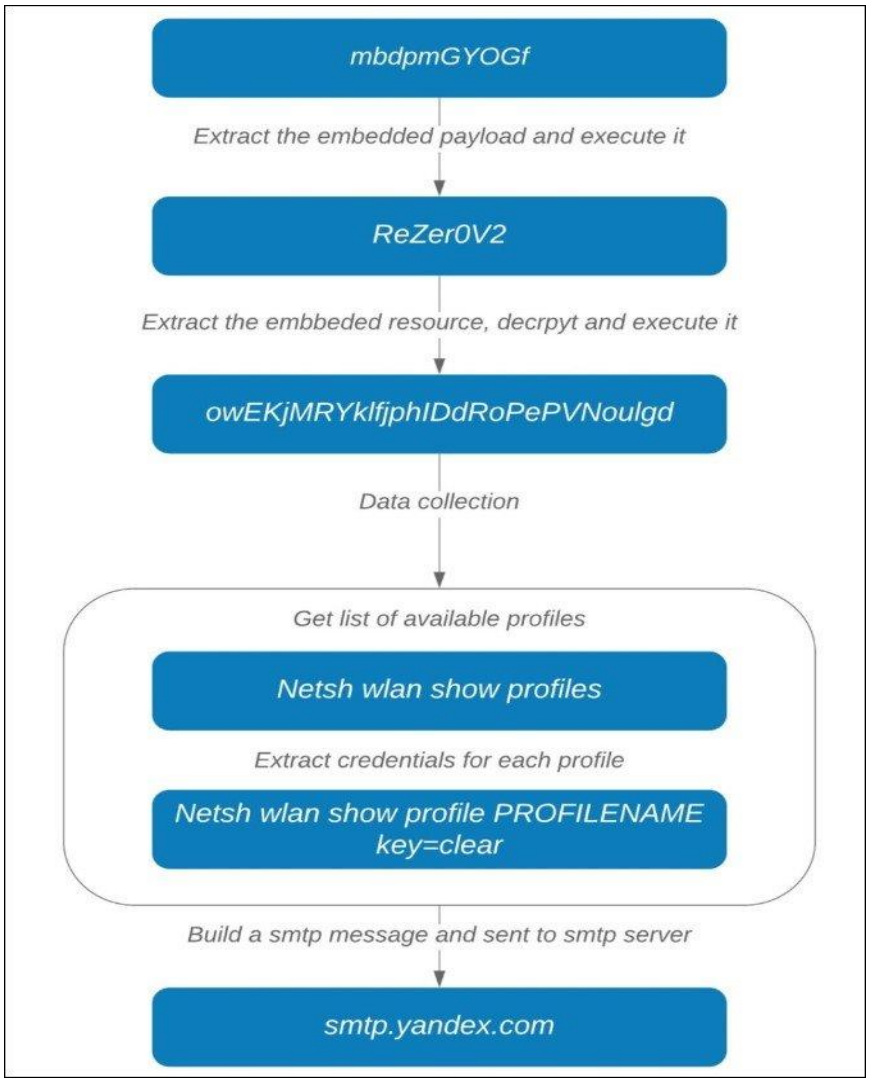
بدافزاری با ویژگی‌های keylogging و RAT

Agent Tesla یک برنامه‌ی سرقت اطلاعات قابل خرید از فوروم‌ها که دارای قابلیت keylogging و تروجان دسترسی از راه دور (RAT) است از حداقل ۲۰۱۴ تاکنون فعال است.

Malwarebytes می‌گوید: "در ماه‌های مارس و آوریل ۲۰۲۰، این برنامه به طور فعال از طریق کمپین‌های هرزنامه در قالب‌های مختلف مانند پرونده‌هایZIP ، CAB، MSI، IMG یا اسناد Office توزیع شد."

هم اکنون ایمیل‌های تجاری مخاطره‌آمیز که از آن‌ها برای ثبت ضربات بر روی صفحه‌کلید و عکس گرفتن از دستگاه‌های آلوده استفاده می‌کنند، در میان کلاهبرداران بسیار محبوب است.

بدافزار سارق اطلاعات همچنین می‌تواند به هدف جمع‌آوری اطلاعات سیستم، سرقت داده‌ها و محتوای کلیپ بورد، از بین بردن آنالیزهای درحال اجرای پردازش‌شده و متوقف‌کردن انتی ویروس، مورد استفاده قرار گیرد.



۳- سرقت رمزعبورهای WiFi توسط Agent Tesla

برای جلوگیری از آلوده شدن به پی‌لود Agent Tesla، باید هنگام باز کردن ایمیل‌های مشکوک یا هنگام بازدید از لینک‌های دریافت شده از طریق ایمیل، بسیار محتاط باشید و همچنین از بارگیری پیوست‌ها در ایمیل‌هایی که از فرستنده‌های ناشناس دریافت کرده‌اید، خودداری کنید.

Agent Tesla در رده بندی "۱۰ مورد از رایج‌ترین تهدیدات" که توسط پلت‌فرم آنالیز بدافزارهای تعاملی Any.Run در دسامبر ۲۰۱۹ انجام‌شد، با ثبت ۱۰،۳۲۴ نمونه‌ی آپلودشده برای تجزیه و تحلیل در طول سال گذشته، در رده‌ی دوم قرار گرفت.

منبع:

https://gbhackers.com/new-agenttesla-malware/

https://www.bleepingcomputer.com/news/security/hackers-steal-wifi-passwords-using-upgraded-agent-tesla-malware/