گزارش امنیتی

عنوان گزارش: دسترسی به NanoCore RAT با انجام فیشینگ از طریق فایل PDF

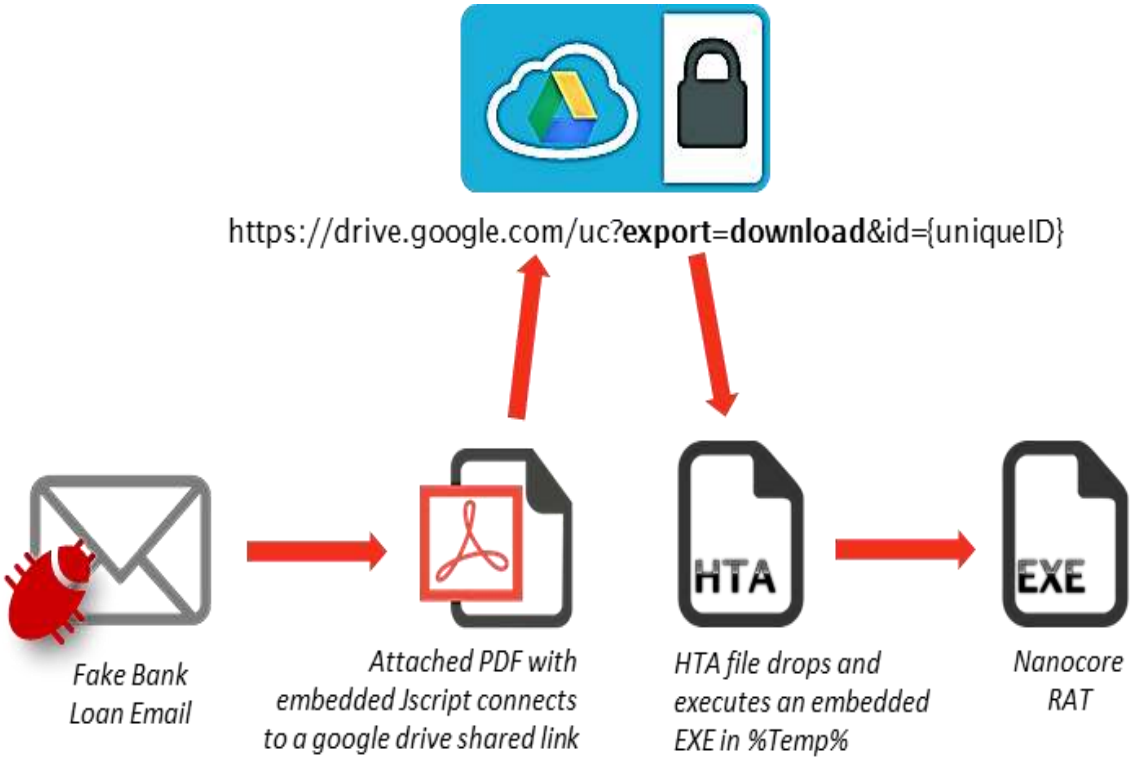
بسمه‌تعالی

دسترسی به NanoCore RAT با انجام فیشینگ از طریق فایل PDF

توسعه‌دهندگان بدافزار از روش‌های توزیع متنوعی استفاده می‌کنند تا کاربران را گمراه نموده و مانع انجام راهکارهای AV شوند .

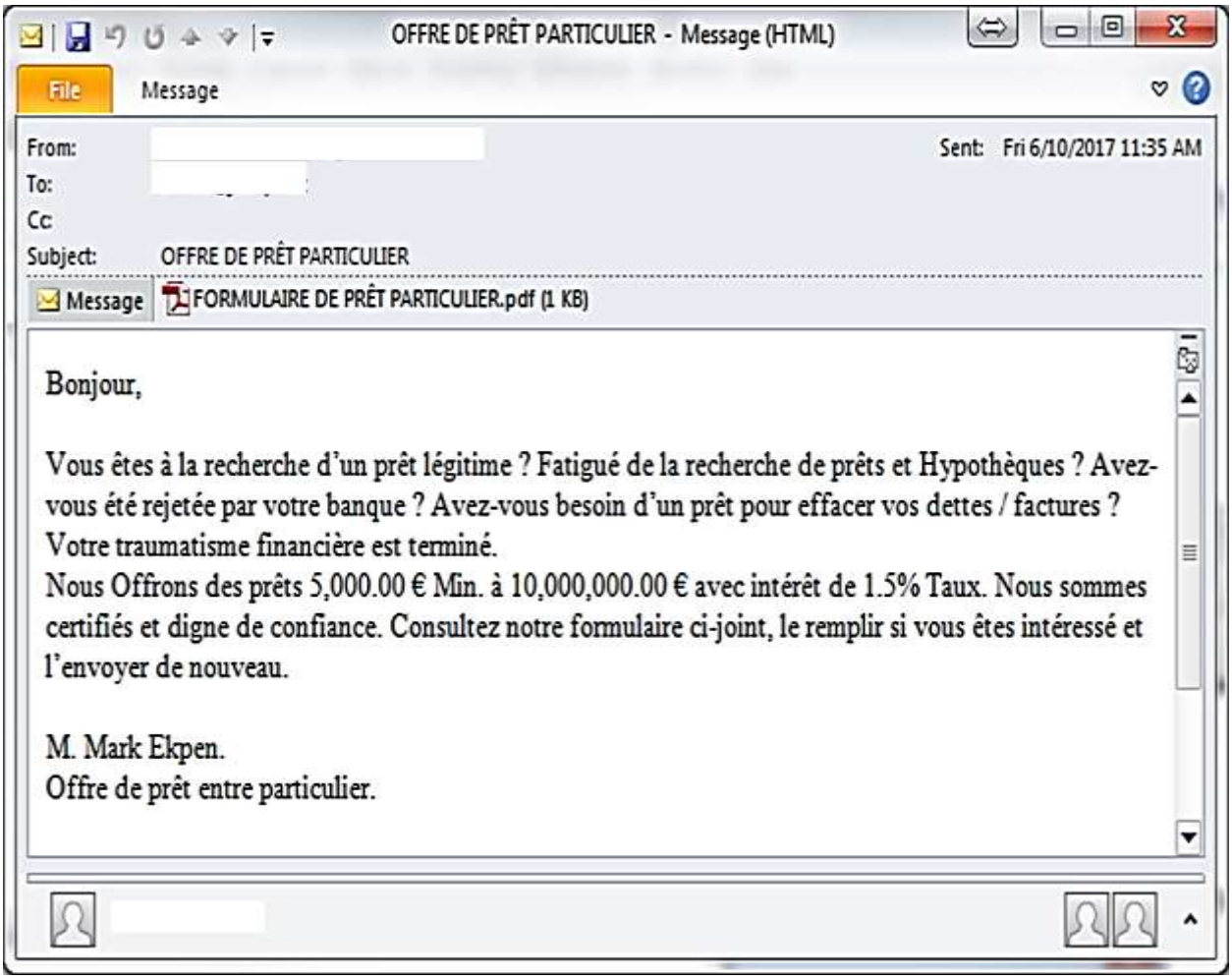
اخیراً نمونه‌ای از حملات فیشینگ که شهروندان فرانسوی را تحت هدف قرار داده، مشاهده شده است. در این حملات، از یک فایل PDF که اسکریپت‌های جاوا در آن تعبیه شده، برای دانلود فایلی از یک لینک اشتراکی گوگل درایو، استفاده می‌شود. بنظر می‌رسد که فایل دانلود شده یک فایل برنامه‌ایِ HTML (به اختصار HTA) است، که کاربرد این فرمت در موارد راه‌اندازی بدافزارها رو به افزایش است. این نوع فایل معمولاً به منظور دانلودگر فایل باینری اصلی استفاده می‌شود. در حملات مذکور، فایل باینری اصلی یک کلاینت NanoCore RAT بود. اما در این مورد، خود فایل باینری اصلی در فایل HTA تعبیه شده بود. بدین صورت، فایل HTA بطور موثر مانند پوششی برای محافظت این فایل باینری در مقابل اسکن بر اساس نوع فایل در شبکه مانند سرویس‌های ضد اسپم عمل می‌کند.

۱ تحلیل زنجیره‌ی مرگ



شکل ۱. زنجیره‌ی مرگ.

مهاجمین در این گروه ایمیل اسپم، کاربران فرانسوی‌زبان را طعمه قرار می‌دهند تا از طریق یک پیشنهاد دروغین وام بانکی، یک فایل پیوست PDF را باز کنند.

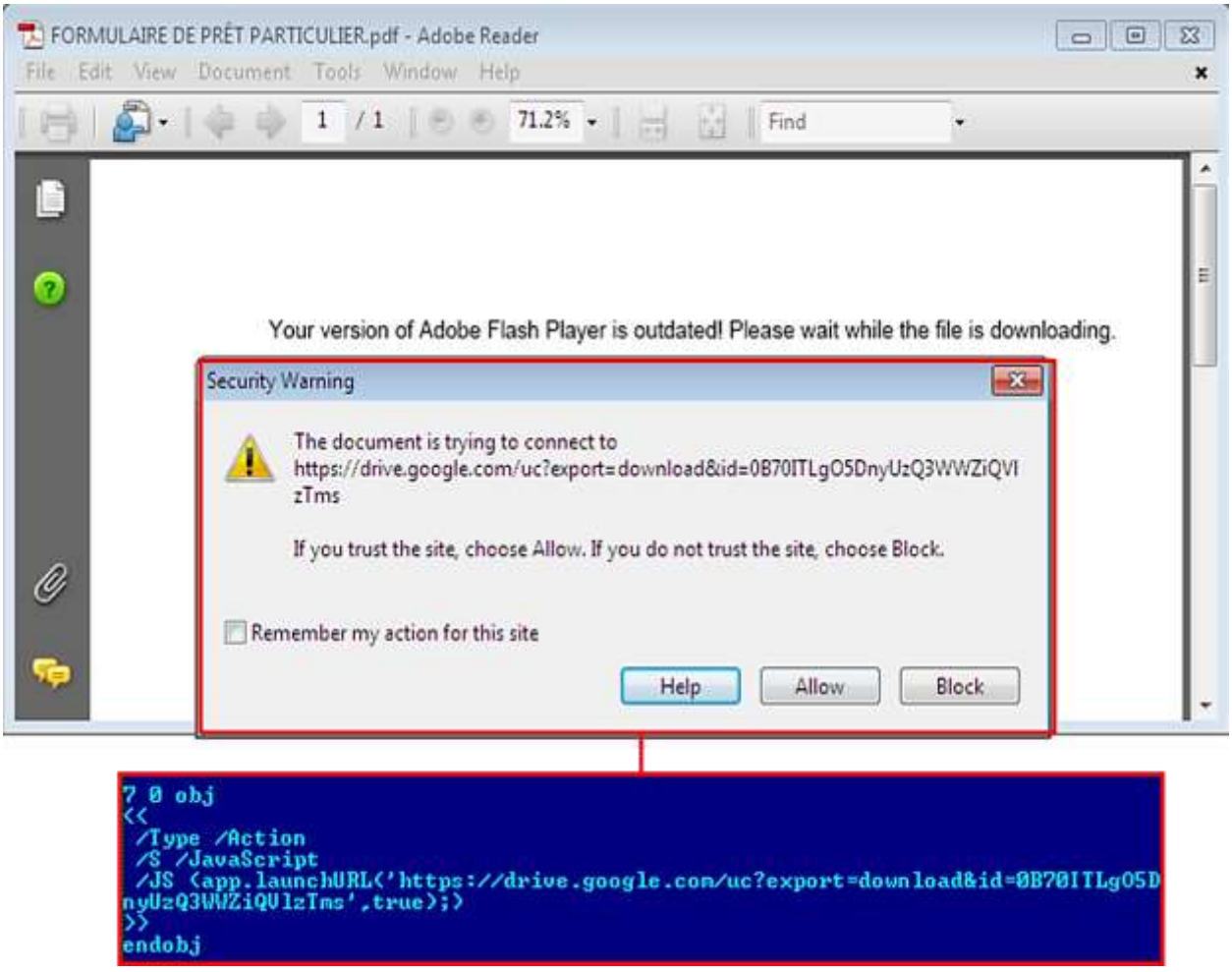


شکل ۲. ایمیل اسپم به زبان فرانسوی، بهمراه PDF پیوست مخرب.

زمانیکه یک کاربر ناآگاه این PDF را باز کند، یک اسکریپت تعبیه شده اجرا می‌شود که سعی در دانلود یک فایل HTA مخرب از یک لینک اشتراکی گوگل درایو دارد. خوشبختانه این عمل موجب نمایش یک اخطار امنیتی از طرف Adobe Reader می‌شود.

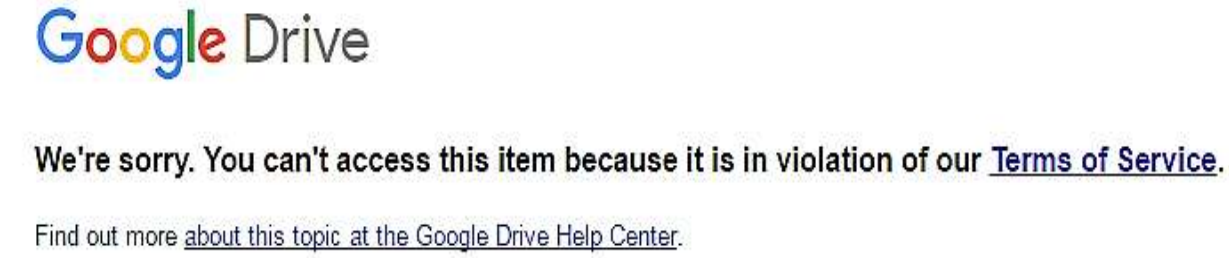
با این حال مهاجمین برای عبور از این اخطار امنیتی از شهرت سایت دانلود گوگل بهره می‌گیرند، که بسیاری از کاربران ممکن است تصور کنند این لینک امن است. و به همین طریق تصور خواهند کرد که فایلی که دانلود می‌شود مورد اعتماد و امن است.

به علاوه، متن PDF به نادرستی ادعا می‌کند که کاربر از نسخه‌ای قدیمی از برنامه Flash Player استفاده می‌کند، و این منظور را می‌رساند که فایلی که دانلود خواهد شد، به روزرسانی برنامه Flash Player است.



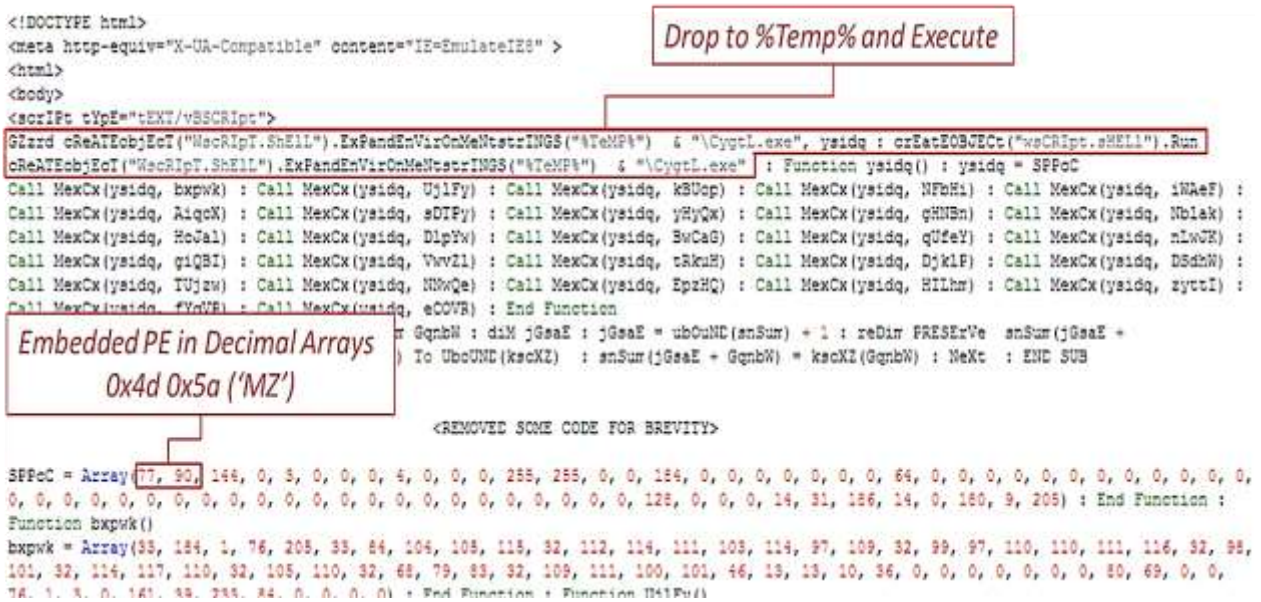
شکل ۳. اسکریپت تعبیه شده در PDF سعی در دانلود از گوگل درایو دارد.

گوگل درایو اقدامات امنیتی مختص به خود را دارد، و پیش از دانلود یا به اشتراک‌گذاری فایل‌ها، آنها را از نظر دارا بودن ویروس اسکن می‌کند. در شکل زیر تصویر نشان داده شده توسط گوگل درایو برای لینک‌های اشتراکی که به عنوان مخرب تشخیص داده شده‌اند، آمده است.



شکل ۴. لینک نمایش داده شده توسط گوگل درایو برای لینک مشخص شده بعنوان مخرب.

با این وجود در این تحلیل، به دلایلی فایل آلوده بعنوان مخرب تشخیص داده نشد و بدین وسیله این فایل به یک نقطه حمله موثر تبدیل شد. فایل دانلود شده یک HTA با یک VBScript است که یک فایل باینری تعبیه شده را رمزگشایی می‌کند. سپس این فایل در دایرکتوری %TEMP% کاربر، ذخیره شده و اجرا می‌شود. پس از تحقیقات بیشتر، مشخص شد که این فایل باینری یک ابزار مدیریت از راه دور به نام NanoCore است.

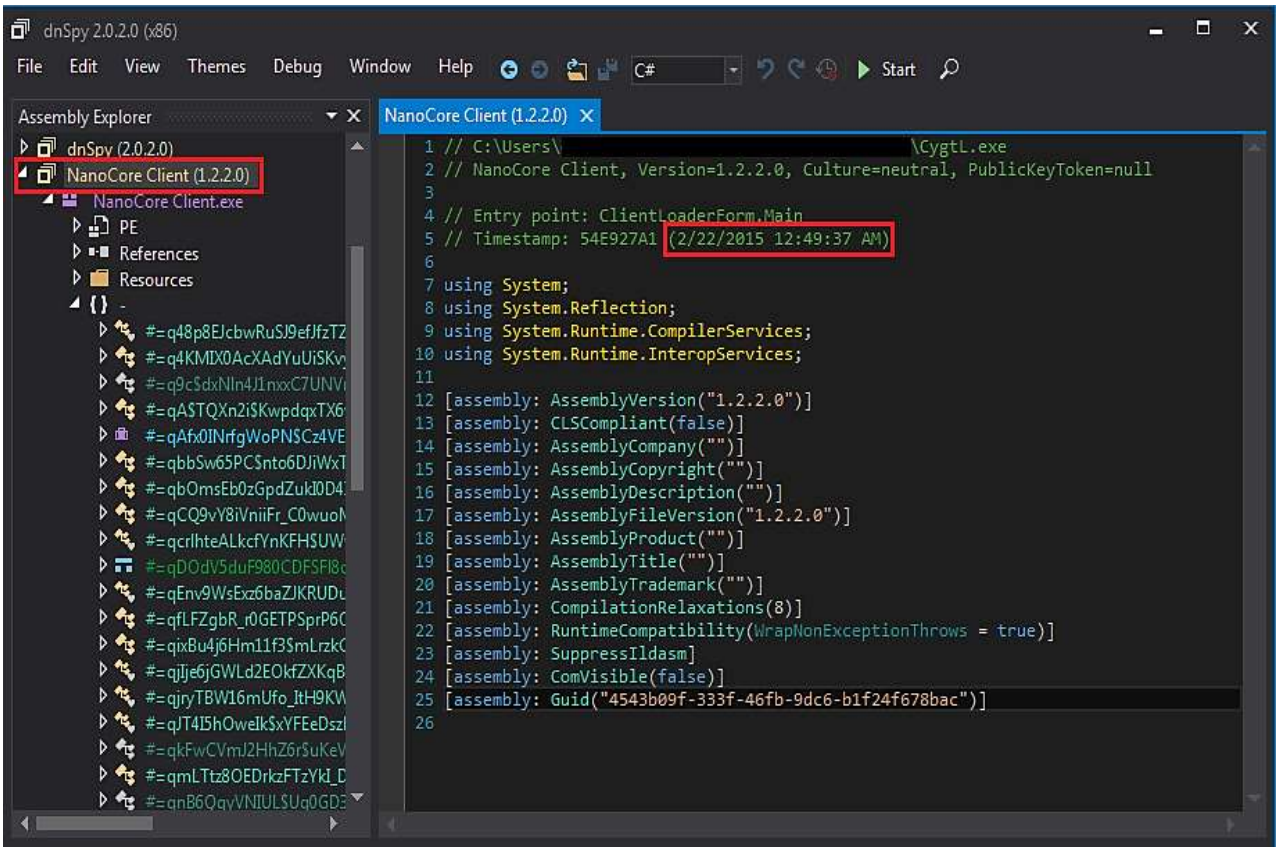


شکل ۵. فایل HTA بهمراه فایل باینری تعبیه شده.

NanoCore ۲

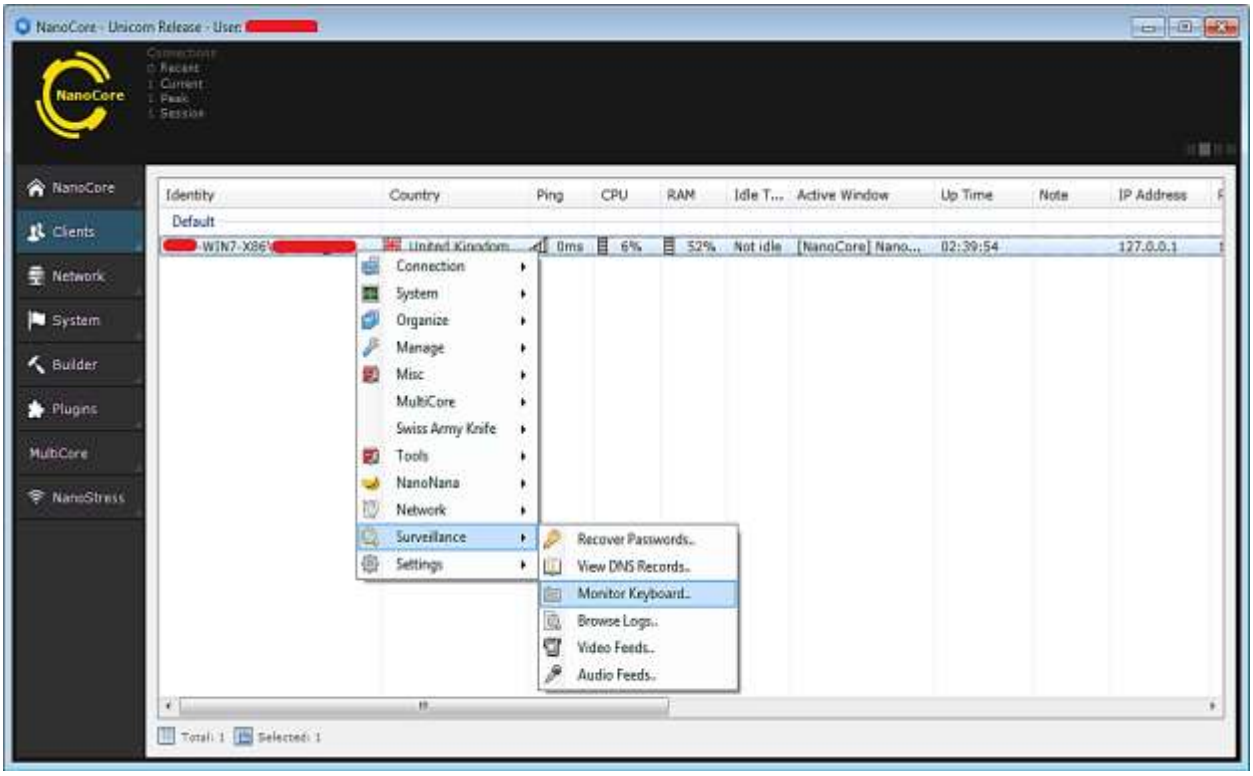
در صنعت ابزارهای مدیریت از راه دور (به اختصار RAT)، NanoCore نامی جدید نیست. بر طبق برخی گزارشات، NanoCore از اوایل سال ۲۰۱۳ با قیمت ۲۵ دلار آمریکا در حال انتشار بوده است. RATها در حدفاصل ظریف میان نظارت و سرقت باقی مانده‌اند. هم می‌توانند به سادگی بعنوان یک ابزار مدیریت از راه دور استفاده شوند، و هم می‌توانند مانند توپخانه‌ای برای جرائم سایبری استفاده شوند. بعنوان مثال می‌توان به گزارش دستگیری نویسنده‌ی NanoCore اشاره کرد. وی بدلیل فروش این ابزار به مجرمین سایبری، مجرم شناخته شد.

اما این خبر باعث توقف کلاهبرداران از توزیع آن نشد. بویژه زمانیکه نسخه‌های کرَک شده‌ی آن در انجمن‌های هک بطور رایگان توزیع شد.



شکل ۶. کلاینت ایمن شده‌ی NanoCore.

کنترل از راه دور، دستکاری فایل‌ها، دانلود و اجرا، و بازیابی رمز عبور تنها برخی از قابلیت‌های ارائه شده توسط NanoCore به کاربران آن هستند. در ادامه تصویری از نسخه کرَک شده‌ی آخرین نسخه‌ی NanoCore (1.2.2.0) نشان داده شده است. این نسخه سال ۲۰۱۵ منتشر شد.



شکل ۷. نسخه‌ی کرَک شده NanoCore (سازنده‌ی 1.2.2.0).

۳ نتیجه‌گیری

مهاجمین سایبری با تمرکز برروی جزئیات اصلی مانند نام فایل و شهرت و اعتبار سایت دانلود، راه‌های خلاقانه‌ای برای جلب اعتماد کاربران و قربانی قرار دادن آنها می‌یابند. همانطور که در این گزارش نشان داده شد، این گروه فیشینگ، از اعتماد گوگل درایو برای رساندن یک بدافزار سوءاستفاده می‌کند. همینطور خود این بدافزار مجهز به تکنیک‌هایی برای پیشگیری از اقدامات امنیتی اولیه می‌باشد.

همچنین مشهود است که مجرم شناخته شدن توسعه‌دهندگان RAT به دلیل همکاری با مجرمین سایبری و کمک به آنها، تاثیری در توزیع برنامه‌های مشابه در صنعت امنیت ایجاد نمی‌کند. به علاوه، با توزیع و

دسترس‌پذیر شدن نسخه‌های کرَک‌شده‌ی چنین نرم‌افزارهایی برای عموم، جدا از بهره‌بردن از ابزار مدیریت راه دور رایگان، برخی به دنبال یافتن طعمه و قربانی می‌گردند.

۴ مراجع

[1] Https://blog.fortinet.com/2017/10/12/pdf-phishing-leads-to-nanocore-rat-targets-french-nationals