禪

باجافزاری که نیامده هک شد

اولین باجافزار مبتنی بر زبان Go کار خود را با شکست آغاز کرد!

```
□
□What happened to your files ?
□All of your files were protected by a strong encryption with RSA4096
□More information about the encryption keys using RSA4096 can be found here: ht        ikipedia.org/wiki/RSA_(cryptosystem)
□
□How did this happen ?
□!!! Specially for your PC was generated personal RSA4096 Key , both publ       rivate.
□!!! ALL YOUR FILES were encrypted with the public key, which has been t      rred to you       uter via the Internet.
□!!! Decrypting of your files is only possible with the help of the private ke      lecrypt prog      which is on our Secret Server
□
□What do I do ?
□So , there are two ways you can choose: wait for a                    d, or st      aining BITCOIN NOW! , and restore your data easy way
□If You have really valuable data, you better not w                    other w      get your files, except make a payment
□
□
□Your personal ID: D7[redacted]E87
□
□For more specific instructions, please visit your                    different addresses pointing to your page below:
□
□1 - http://rp4roxeuhcf2vgft.onion.to
□2 - http://rp4roxeuhcf2vgft.onion.cab
□3 - http://rp4roxeuhcf2vgft.onion.city
□
□If for some reasons the addresses are not available, follow these steps:
□
□1 - Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
□2 - Video instruction: https://www.youtube.com/watch?v=NQrUZdsw2hA
□3 - After a successful installation, run the browser
□4 - Type in the address bar: http://rp4roxeuhcf2vgft.onion
```

زبان برنامهنویسی Go که به منظور ارائه یک زبان چهارچوب کارآمد، ساده و قدرتمند از سوی گوگل به جامعه برنامهنویسان تقدیم شد، برای اولین بار از سوی هکری برای ساخت یک باجافزار مورد استفاده قرار گرفت . اما بر خلاف آنچه این هکر برنامهنویس تصور میکرد، باجافزار او در همان راند اول مغلوب شد و به تاریخ پیوست !

آنگونه که شرکت سازنده نرمافزارهای امنیتی دکتر وب (Dr.web) گزارش کرده است، به تازگی باجافزاری در فضای سایبری منتشر شده است که Trojan.Encoder.6491 نام داشته و خود را به شکل Windows_Security.exe به کاربران تحمیل میکند . نویسنده باجافزار برای آنکه بتواند کاربران را فریب دهد، باجافزار خود را سهشنبه هفته گذشته همزمان با ارائه بولتن ماهیانه مایکروسافت عرضه کرده است. به این امید که کاربران با دیدن نام Windows_Security اغفال شوند و این باجافزار را روی سیستم خود نصب کنند.

مطلب پیشنهادی

بدافزار استخراج کننده اطلاعات

کارمندان دولت مراقب نسخه جدید بدافزار **H1N1** باشند

Trojan.Encoder.6491 فرآیند رمزنگاری فایلها را بر اساس الگوریتم AES انجام داده و قادر است 140
فرمت فایلی مختلف را رمزنگاری کند . همچنین برای آنکه قربانیان بتوانند همچنان از سیستم خود
استفاده کرده و باج مربوطه را پرداخت کنند، پوشه‌های اصلی مربوط به ویندوز را رمزنگاری نمیکند .
کاربران این توانایی را دارند تا باجافزار Trojan.Encoder.6491 را در سیستم خود مشاهده کنند، به
دلیل اینکه باجافزار بعد از آنکه فایلها را رمزنگاری میکند، نام آنها را تغییر میدهد . باجافزار
از فایلی به نام photo.png استفاده کرده و فرآیند کدگذاری نام فایلها را بر مبنای الگوریتم
Base64 انجام میدهد . در ادامه پسوند ENC را به انتهای نام فایلها در قالبی شبیه به cGhvdG8=.enc
و... اضافه میکند . زمانی که تروجان نصب میشود در ادامه فرمان "vssadmin.exe Delete Shadows /All
/Quiet" را به منظور حذف تمامی کپیها و نقاط بازگشتی (Restorepoints) که از سوی کاربر ساخته شده است
به مرحله اجرا در میآورد . بعد از اتمام فرآیند کدگذاری با استفاده از تابع main_ListenForPayment
مقدار بیتکوین کیف الکترونیکی را مورد بررسی قرار میدهد .

اما خبر خوب این است که پژوهشگران شرکت دکتر وب موفق شدهاند رخنهای را در مکانیزم رمزنگاری این باجافزار شناسایی کنند و بر مبنای همان رخنه یک رمزگشا که قادر است فایلهای قفل شده را بدون آنکه کاربران نیازی داشته باند باجی را برای دستیابی به فایلهای خود پرداخت کنند، طراحی کنند . اما خبر بد این است که این رمزگشا تنها در اختیار مشتریان این شرکت قرار میگیرد . در نتیجه برای دستیابی به این ابزار رمزگشا باید یکی از مشتریان این شرکت امنیتی مستقر در روسیه باشید و هزینه مربوطه را پرداخت کنید .

نکته خندهدار و قابل تعمل این است که هر دو طرف به یک اندازه از کاربران برای دسترسی به فایلهایشان پول دریافت میکنند . در حالی که مشتریان دکتر وب برای دسترسی به این ابزار رمزگشا باید مبلغ 30 دلار را پرداخت کنند، نویسنده این باجافزار نیز برای آنکه کاربران بتوانند به فایلهای کدگذاری شده خود دسترسی داشته باشند مبلغ 30 دلار را به عنوان باج دریافت میکند .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
26/07/1395 - 03:00
برچسب:
امنیت - باج افزار - هک - Windows_Security.exe - Trojan.Encoder.6491 - Go - رمزنگاری

نشانی
□□□□:https://www.shabakeh-mag.com/security/5064/%D8%A7%D9%88%D9%84%DB%8C%D9%86-%D8%A8%D8%A7%D8%AC%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-%D9%85%D8%A8%D8%AA%D9%86%DB%8C-%D8%A8%D8%B1-%D8%B2%D8%A8%D8%A7%D9%86-go-%DA%A9%D8%A7%D8%B1-%D8%AE%D9%88%D8%AF-%D8%B1%D8%A7-%D8%A8%D8%A7-%D8%B4%DA%A9%D8%B3%D8%AA-%D8%A2%D8%BA%D8%A7%D8%B2-%DA%A9%D8%B1%D8%AF