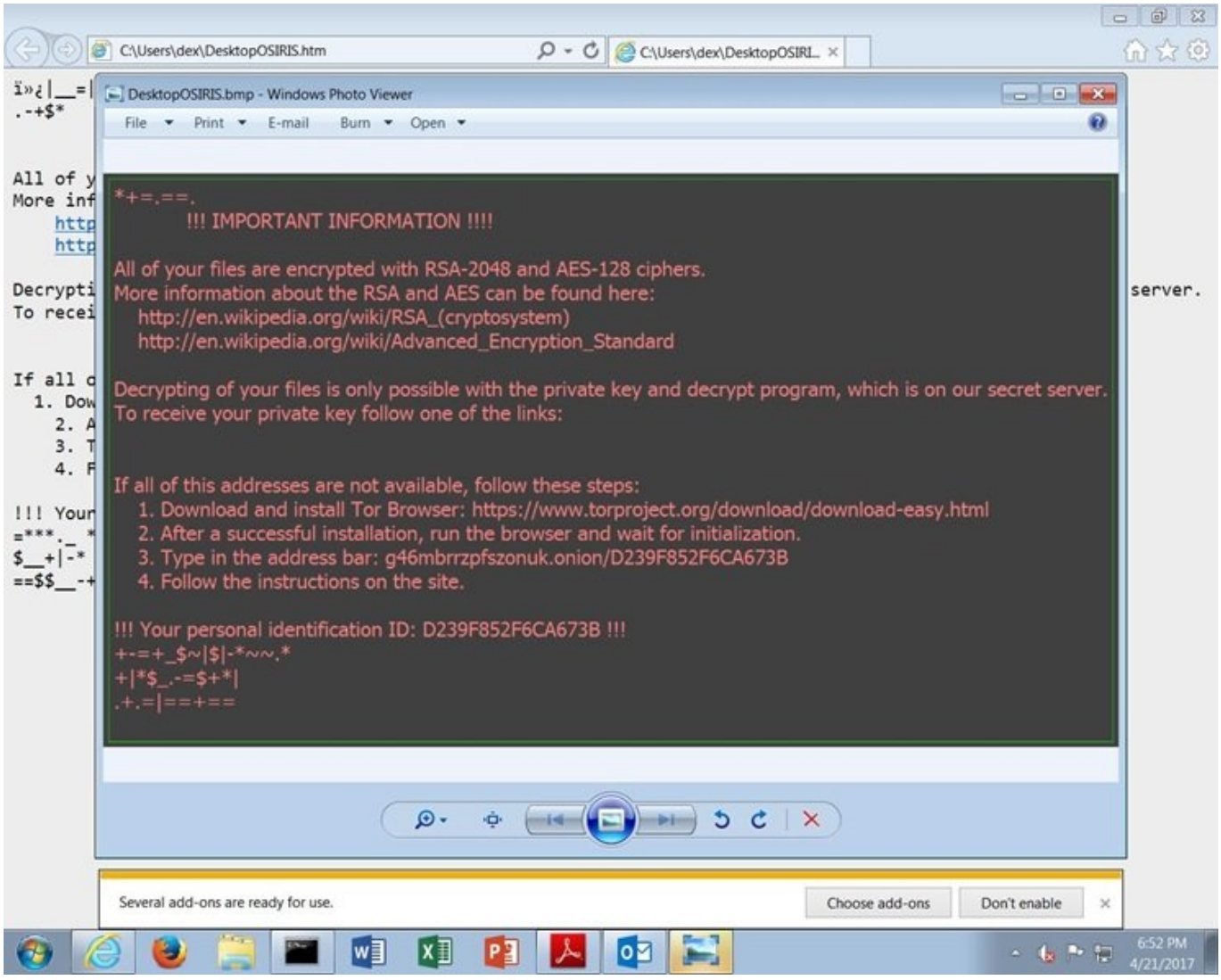


تعامل باتنت Necurs و باجافزار لاکی

کاملا احتیاط کنید؛ باج افزار Locky دومرتبه فعال شده است


```
*+=.==.
        !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: g46mbrrzpfszonuk.onion/D239F852F6CA673B
    4. Follow the instructions on the site.

!!! Your personal identification ID: D239F852F6CA673B !!!
+-=+_$~|$|-*~~.*
+|*$_.-=$+*|
.+.=|==+==
```

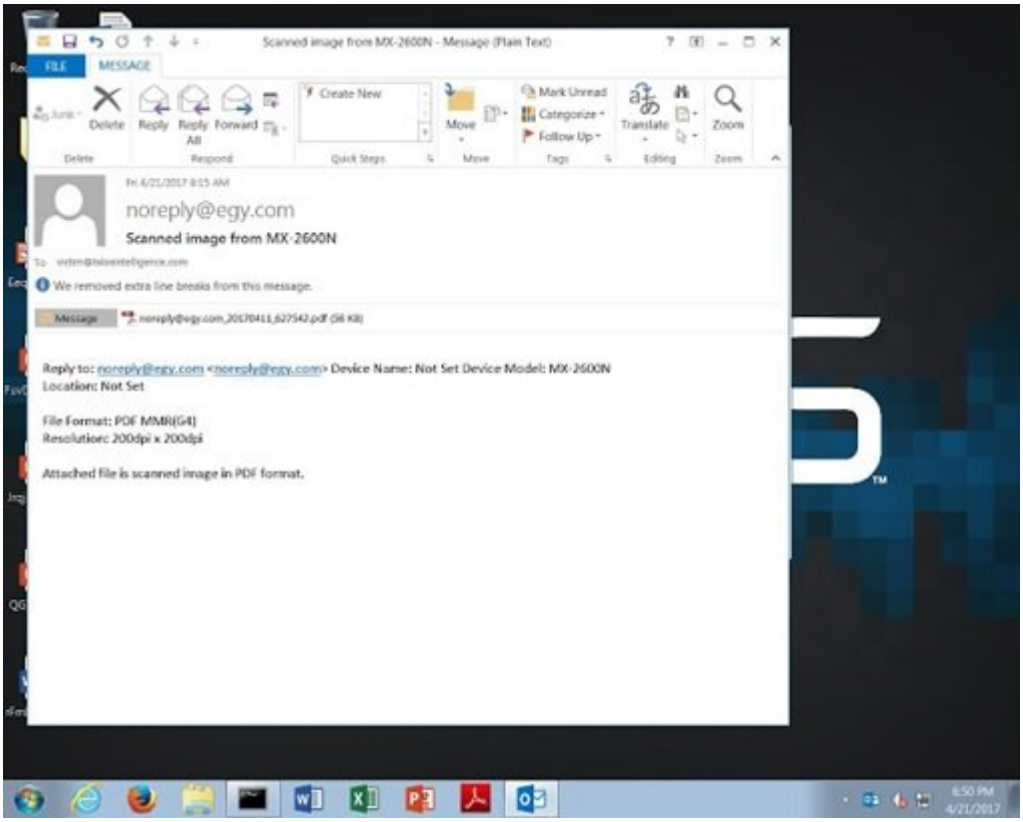
C:\Users\dex\DesktopOSIRIS.htm
C:\Users\dex\DesktopOSIRI...
DesktopOSIRIS.bmp - Windows Photo Viewer
File
Print
E-mail
Burn
Open
Several add-ons are ready for use.
Choose add-ons
Don't enable
6:52 PM
4/21/2017

زمانی که در مورد باجافزارها مطلبی مینویسیم، تعدادی از مردم تصور میکنند که این مشکل تنها محدود به کشورهای غربی است. اما واقعیت این است که هر کاربری در هر نقطه از جهان ممکن است قربانی باجافزارها شود . بر همین اساس پیشنهاد میکنیم خطر باجافزارها را جدی قلمداد کنید .

باجافزار Locky یکی از معروفترین باجافزارهای سال گذشته میلادی بود . اما به طور ناگهانی در ابتدای فصل 2017 میلادی فعالیت آن به کمترین حد ممکن رسید . اکنون نشانههایی از بازگشت این باجافزار همزمان با راهاندازی کمپین جدیدی مبتنی بر باتنت Necurs مشاهده شده است. Necurs باتنتی است که سال گذشته میلادی شناسایی شد و بر طبق گزارشهای رسمی تاکنون بیش از 1.7 میلیون کامپیوتر را آلوده ساخته است.

[ссылка]

SophosLab Necurs 21 5 Necurs pump-and-dump


Scanned image from MX-2600N - Message (Plain Text)
FILE
MESSAGE
Delete
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
noreply@egy.com
Scanned image from MX-2600N
We removed extra line breaks from this message.
Reply to: noreply@egy.com <noreply@egy.com> Device Name: Not Set Device Model: MX-2600N
Location: Not Set
File Format: PDF MMR(G4)
Resolution: 200dpi x 200dpi
Attached file is scanned image in PDF format.

[illegible]

[illegible] «[illegible]»: [illegible] [illegible] [illegible]

noreply@egy.com_20170411_627542.pdf - Adobe Reader
File Edit View Window Help
1 / 1
100%
Tools Sign Comment

see in 948699

Open File

The file '948699.docm' may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to:

● Open this file
○ Always allow opening files of this type
○ Never allow opening files of this type

OK
Cancel
6:51 PM
4/21/2017

اینگونه به نظر میرسد که هکرها از دو کمپین مختلف برای ارسال باجافزار استفاده میکنند . در یکی از این کمپینها موضوع ایمیلهای ارسالی ثابت بوده و در ادامه تغییراتی در آن به وجود میآید و کمپین دوم از یک عنوان برای ارسال دهها هزار ایمیل استفاده میکند . تکنیکی که باجافزار لاکی از آن استفاده میکند به کمپین Dirdex شباهت زیادی دارد . ضمیمه ایمیل حاوی یک فایل PDF است، اما در کنار آن یک فایل .DOCM ورد نیز ممکن است وجود داشته باشد.

HTTP Traffic

```
● GET http://uwdesign.com.br:80/9yg65                                                  Stream: 9    Transaction: 0
Server IP:  192.185.214.197          Server Port:  80          Resp. Content: <unknown>          Timestamp:  +88.0s
● POST http://188.120.239.230:80/checkupdate                                           Stream: 10   Transaction: 0
Server IP:  188.120.239.230          Server Port:  80          Resp. Content: <unknown>          Timestamp:  +139.0s
● POST http://188.120.239.230:80/checkupdate                                           Stream: 10   Transaction: 1
Server IP:  188.120.239.230          Server Port:  80          Resp. Content: <unknown>          Timestamp:  +140.0s
● POST http://188.120.239.230:80/checkupdate                                           Stream: 10   Transaction: 2
Server IP:  188.120.239.230          Server Port:  80          Resp. Content: <unknown>          Timestamp:  +141.0s
```

درون این سند ورد، ماکروی مخربی قرار دارد که به محض فعال شدن، باجافزار لاگی را روی کامپیوتر قربانی نصب کرده و فایلهای او را رمزنگاری میکند . بیاسینی میگوید : «در این مکانیزم توزیع یک ویژگی خاص وجود دارد. باجافزار برای آنکه روی سیستم قربانی نصب شود ارتباطی با او برقرار میکند تا کاربر فایل مخرب را اجرا کند . همین موضوع باعث میشود تا باجافزار بتواند از تکنیکهای امنیتی همچون سندباکس فرار کند . این باجافزار مادامی که کابر او را فعال نکند سیستم او را آلوده نمیکند و همین موضوع باعث میشود تا هیچگاه در دام سندباکس قرار نگیرد .»

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
10:40 - 12/02/1396

□□□□□
https://www.shabakeh-mag.com/security/7657/%DA%A9%D8%A7%D9%85%D9%84%D8%A7-%:□□□□
D8%A7%D8%AD%D8%AA%DB%8C%D8%A7%D8%B7-
%DA%A9%D9%86%DB%8C%D8%AF%D8%9B-%D8%A8%D8%A7%D8%AC-
%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-locky-
%D8%AF%D9%88%D9%85%D8%B1%D8%AA%D8%A8%D9%87-
%D9%81%D8%B9%D8%A7%D9%84-%D8%B4%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA