باج‌افزار AnimusLocker

Animus Locker بدافزار جدیدی از نوع باج‌افزار می‌باشد که در روزهای اخیر در فضای سایبری انتشار یافته و اقدام به رمزگذاری فایل‌های سیستم می‌کند. بعد از اتمام فرایند رمزگذاری، پسوند animus. را به انتهای فایل رمزشده اضافه کرده و سه فایل راهنما برای کاربر در داخل هر پوشه که فایل‌های موجود در آن رمزشده‌باشند، قرار می‌دهد که هر سه فایل دارای یک متن مشترک می‌باشند. طبق پیام موجود در داخل فایل‌های متنی، الگوریتم رمزگذاری فایل RSA می‌باشد ولی برخی از محققان امنیتی معتقدند که برای رمزگذاری از الگوریتم AES استفاده شده‌است. پیام نمایش داده‌شده برای کاربر با نام‌های زیر می‌باشد:

- ANIMUS_RESTORE.txt
- ANIMUS_RESTORE2.txt
- ANIMUS_RESTORE3.txt

```
<><><><><><><><><><><><><><># animus locker #<><><><><><><><><><><><><><>
SORRY! Your files are encrypted.
File contents are encrypted with random key.
Random key is encrypted with RSA public key (2048 bit).
We STRONGLY RECOMMEND you NOT to use any "decryption tools".
These tools can damage your data, making recover IMPOSSIBLE.
Also we recommend you not to contact data recovery companies.
They will just contact us, buy the key and sell it to you at a higher price.
If you want to decrypt your files, you have to get RSA private key.
In order to get private key, write here:
j0ra@protonmail.com
########
!ATTENTION!
Attach file is 000000000.key from %appdata% to email message,
without it we will not be able to decrypt your files
########
And pay 100$ on 1G5TThb5tcJ3LQbF4C4Tibgd9y7m3iYPFH wallet
If someone else offers you files restoring, ask him for test decryption.
 Only we can successfully decrypt your files; knowing this can protect you from fraud.
You will receive instructions of what to do next.
<><><><><><><><><><><><><><># animus locker #<><><><><><><><><><><><><><>
```

شکل ۱ – پیام متنی نشان داده‌شده برای کاربر

نحوه فعالیت بدافزار

نحوه شیوع و یا انتقال باج‌افزار به سیستم مشخص نیست لذا بعد از انتقال به سیستم شروع به کار کرده و اقدام به رمزگذاری فایل‌های سیستم می‌کند. باج‌افزار با تغییر کلید رجیستری، خود را در Run سیستم قرار داده و باعث می‌شود در هر بار اجرای سیستم، بصورت خودکار اجرا گردد. سپس یک فایلی را با

پسوند key. در آدرس C:\Documents and Settings\Administrator\Application Data ایجاد می-کند. بعد از رمزگذاری هر فایل پسوند Animus. را مانند شکل زیر در انتهای هر فایل اضافه می‌کند. در انتهای فرایند رمزگذاری، سه فایل متنی که هرسه مورد دارای متن یکسانی می‌باشند را در داخل هر پوشه قرار می‌دهد.

در فایل متنی نشان داده‌شده برای کاربر (شکل ۱)، مهاجمان برای بازیابی و رمزگشایی فایل‌های رمزشده درخواست ۱۰۰ دلار دارند. همچنین کاربر باید یک فایل با نام 000000000.key که توسط باج‌افزار در مسیر %appdata% ایجاد شده‌است را به آدرس ایمیل j0ra@protonmail.com ارسال کند. در این پیام به کاربر اعلام می‌کنند که از الگوریتم سخت رمزنگاری RSA استفاده شده‌است.

شکل ۲- نمونه‌ای از فایل‌های رمزشده

پاکسازی بدافزار از سیستم

برای پاکسازی بدافزار در سیستم در عمل کاری نمی‌توان انجام داد. ولی می‌توان با استفاده از فایل‌های پشتیبان که قبلا از سیستم گرفته‌است، اقدام به بازیابی اطلاعات کرد.

بعد از بازیابی فایل‌ها، سیستم را با استفاده از آنتی‌ویروس بروزشده، اسکن کرده و راهکارهای امنیتی را برای سیستم خود لحاظ می‌کنیم.

راه‌های مراقبت و پیشگیری

برای اینکه سیستم خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در مورد آن‌ها می‌توان یک آنتی‌ویروس قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه‌های مشکوک خودداری کنیم.

بیشتر برنامه‌هایی که از طریق تبلیغات یا از طریق کانال‌های دیگر ارائه می‌گردند مخرب بوده و احتمال آسیب رسیدن به سیستم می‌باشد. لذا از دانلود و نصب برنامه‌هایی که مشکوک به‌نظر می‌رسند باید خودداری کرد.

۳- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی سیستم را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار، به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر نگهداری کنیم.

۴- عدم بازکردن ایمیل‌های مشکوک

بیشتر حملات باج‌افزاری از طریق اسپم ایمیل‌ها با عناوین گول‌زننده انتشار می‌یابند. لذا باید از باز کردن این نوع از ایمیل‌ها خوودداری کرده و در همان لحظه آن‌ها را حذف کنیم. در این نوع از ایمیل‌ها، در داخل فایل‌های مانند word یا pdf بدافزار قرار داده شده و هنگام اجرای آن‌ها بدافزار اجرا شده و اقدام به نصب و راه‌اندازی خود در سیستم می‌کنند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۰۴۵ – ۳۱۵۰۵۷۱۸

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی