

باسمه تعالی

هشدار؛ شیوع نسخه جدید باج افزار STOP

هشدار؛ شیوع نسخه جدید باج افزار STOP

باج افزار STOP (djvu)، فعال ترین و شایع ترین باج افزار سال ۲۰۱۹ شناخته شده است. در سال جدید میلادی نیز این باج افزار بسیار فعال بوده و افراد زیادی درگیر آن شده اند. این باج افزار دارای نسخه های گوناگونی است و تاکنون بیش از ۲۰۰ نسخه مختلف از آن شناسایی شده است. در نسخه های جدید این باج افزار، پسوندهای TOPI و KODC به انتهای فایل های رمز شده افزوده شده و پیغامی مشابه شکل زیر نمایش داده می شود.

ATTENTION!

Don't worry, you can return all your files!

All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.

The only method of recovering files is to purchase decrypt tool and unique key for you.

This software will decrypt all your encrypted files.

What guarantees you have?

You can send one of your encrypted file from your PC and we decrypt it for free.

But we can decrypt only 1 file for free. File must not contain valuable information.

You can get and look video overview decrypt tool:

<https://we.tl/t-Oc0xgfzC7q>

Price of private key and decrypt software is \$980.

Discount 50% available if you contact us first 72 hours, that's price for you is \$490.

Please note that you'll never restore your data without payment.

Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:

help [redacted] c

Reserve e-mail address to contact us:

help [redacted] ir

Your personal ID:

0197 [redacted] 5t1

در روزهای اخیر تعداد زیادی از مراکز و کاربران ایرانی به این باج افزار آلوده شده اند. عمدتاً این باج افزار از طریق اجرای برنامه های کرک شده، keygen ها، activator ها، فایل های نصب جعلی برنامه ها و اجرای فایل های پیوست آلوده پست های الکترونیکی منتشر می شود. بنابراین توصیه می شود کاربران حتماً از منابع مطمئن اقدام به تهیه برنامه های مورد نیاز خود نموده و از سایت های غیر مطمئن برای دانلود برنامه ها استفاده نکنند.

در صورتی که سیستم آلوده شده توسط این باج افزار به اینترنت دسترسی نداشته باشد، احتمال بازیابی اطلاعات بیشتر است. برخی از نسخه های این باج افزار با داشتن دسترسی به اینترنت با دامنه ring2.ug برای مبادله کلید رمزنگاری ارتباط خواهد داشت. بنابراین به منظور کاهش هر چه بیشتر خسارات ناشی از این گونه باج افزار بهتر است هرچه سریعتر ارتباط با این دامنه مسدود گردد.