****

**ناوەندی شیکار Shikar Center**



**ناساندن و خۆپاراستن لە ڕانسۆموەیر**

ئامادەکردنی

هاوکار محمد

بەرهەمی ناوەندی شیکار

--١٢--

**٢٠٢٢**

**ناوەڕۆک**

[پێشەکی ....................................................................................................... ٣](#پێشەکی)

[ناساندنی ڕانسۆموەیر ....................................................................................... ٣](#رانسۆموەیر_چییە)

[جۆرەکانی ماڵوەیر .......................................................................................... ٤](#جۆر)

[بەناوبانگترین ڕانسۆموەیرەکانی ساڵی ٢٠٢١ .......................................................... ١٠](#بەناوبانگترین_٢٠٢١)

[پێنج گەورەترین هێرشی ڕانسۆموەیر لە مێژودا ....................................................... ١٠](#گەورەترین_هێرشەکان)

[WannaCry ........................................................................................... ١١](#وانەکرای)

[چۆنییەتی خۆپاراستن لە ڕانسۆموەیر ................................................................. ١٣](#خۆپاراستن)

[هەنگاوە خێراکان بۆ ئەوەی کێشەکە گەورەتر نەبێت ................................................ ١٥](#هەنگاوە_خێراکان)

[هەنگاوەکانی پاککردنەوەی کۆمپیوتەرەکەت لە ماڵوەیری ڕانسۆموەیر ............................ ١٦](#چارەسەری_رانسۆموەیر)

[هەنگاوەکانی چارەسەر کردنی فایلە قوفل بووەکانت/ئینکریپت بووەکانت ......................... ١٨](#دیکریپتکردن)

[هەندێک بەرنامەی ڕیکۆڤەری ....................................................................... ١٩](#ریکۆڤەری)

[هەندێک ئامۆژگاری بەسود .......................................................................... ٢٢](#ئامۆژگاری)

[وتەی کۆتایی .......................................................................................... ٢٦](#کۆتایی)

[سەرچاوەکان .......................................................................................... ٢٧](#سەرچاوەکان)

**پێشەکی**



هەندێک کەس بابەتی کراک کراو دادەبەزێنن وەک چالاک کردنی ئۆفیس و ویندۆز و ئۆتۆکاد...هتد، یان داگرتنی کتێب و فیلم کە لەبنەرەتدا بەپارەیە، وە هەوڵدەدەن بە بەلاش بەدەستی بخەن و توشی ڤایرۆسێک دەبن کە فایلەکان قوفڵ دەکات بەو ڤایرۆسە/ماڵوەیرە دەوترێت ڕانسۆموەیر.

کۆمەڵێک وشەی بەکارهاتووی نێو ئەم بابەتە

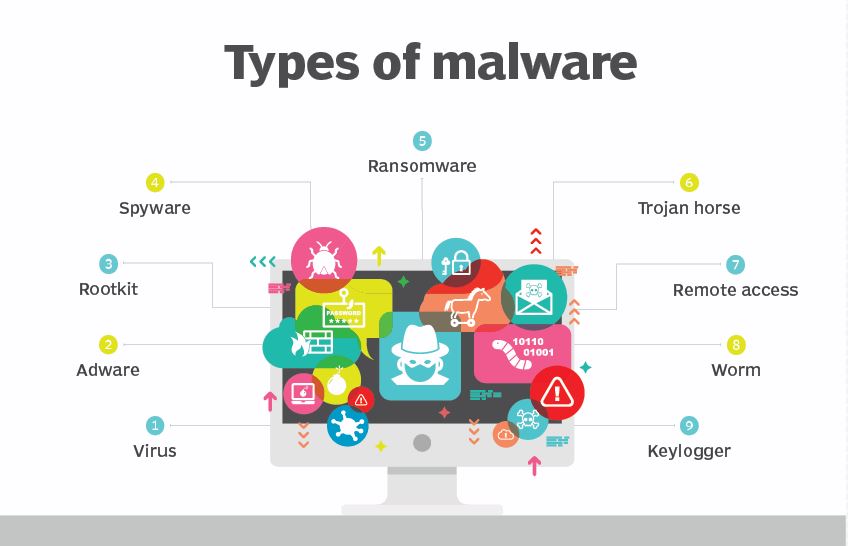
Ransomware – Malware - Malicious Software - Encrypt - Victim - Decrypt - Bitcoin - WannaCry - Extension - Protect - Problem - Virus - Recovery - Virtual Machine

**ناساندنی ڕانسۆموەیر**

****

ڕانسۆموەیر جۆرێکی ماڵوەیرە کە هەڕەشە لە کەسی نێچیر/توشبوو دەکات، بە بڵاوکردنەوەی داتاکانی یان قوفڵ کردنی داتاکانی و داواکردنی پارە لە کەسی توشبوو بۆ پێدانی کلیلی کردنەوەی فایلە قوفڵ بووەکانی کەسی توشبوو، مێژوی ئەم جۆرەی ماڵوەیرە دەگەرێتەوە بۆ ساڵی ١٩٨٩

**جۆرەکانی ماڵوەیر**



سەرچاوەی وێنە ماڵپەری techtarget.com

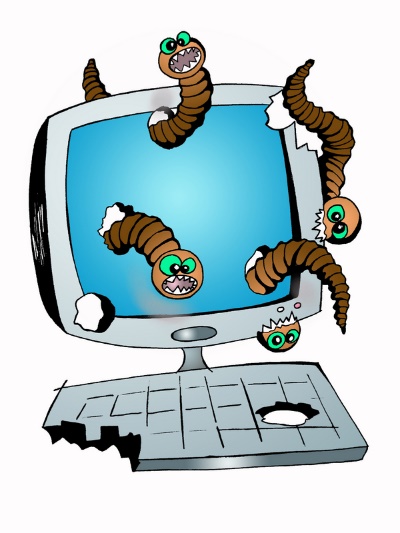
هەر یەکە لە ترۆجان و ۆرم و ڤایرۆس و کیلۆگەر و ڕانسۆموەیر...جۆرە جیاوازەکانی ماڵوەیرن کە ئەم وشەیەش کورتکراوەی malicious software کە بەکوردی دەتوانین بڵێین واتای نەرمەواڵای کیناوی/زیانبەخش دێت، لە خوارەوە جۆرە جیاوازەکانی ماڵوەیر ڕون دەکەینەوە بۆتان.

Virus – ڤایرۆس



ڤایرۆس بەربڵاوترین جۆری ماڵوەیرە، کە دەتوانێت خۆی جێبەجێ بکات واتە فرمان لە دروستکەرەکەی وەرنەگرێت و بڵاوببێتەوە بە بەرنامە و فایلەکانی تردا، ڤایرۆسەکان یەکجار دروست دەکرێن و دواتر بە شێوەی خۆکارانە کار دەکەن و فرمان وەرناگرن بەڵکو ئەو فرمانانەی کە پێیان دراوە وەک رۆبۆت لەسەر کۆمپیوتەرەکان جێبەجێی دەکەن بەهۆی زۆر چالاکی ڤایرۆسەکانەوە ئەوا ئاسان دەدۆزرێنەوە لەلایەن دژە ڤایرۆسەکانەوە.

Worm - کرم



کرم دیارترین کاری ئەوەیە کە دەتوانێت خۆی کۆپی بکات بەبێ ئەوەی پشت بە بەرنامەی خانەخوێ ببەستێت، بەواتایەکی تر یەکەم کردم کە دێتە نێو کۆمپیوتەرێکەوە و و خۆی کۆپی کرد بۆ دوو کرم ئەوا هەر یەکەیان و کرمێکی سەربەخۆن و هەر یەکەیان بەجیا کرمێکی تر کۆپی دەکەن بەبێ گەرانەوە بۆ یەکتر و بۆ یەکەم کرم، کرمەکان بەهۆی خۆ کۆپی کردنی بەردەوامەوە بەشێوەیەکی زۆر خێرا لە کۆمپیوتەرەکاندا بڵاودەبنەوە بەبێ گەرانەوە بۆ فرمانی کەسی دروستکەرەکانیان.

Spyware – نەرمەواڵای سیخوری

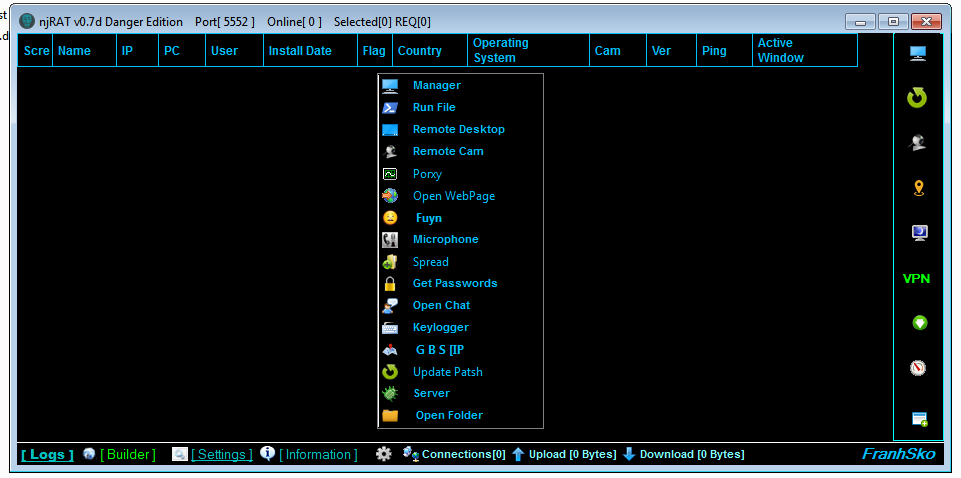


نەرمەواڵای سیخوری زانیاری و داتای ئامێر و بەکارهێنەران کۆ دەکاتەوە، هەروەها چاودێری چالاکی بەکارهێنەران دەکات، بەکورتی وەک لە ناوەکەیدا دیارە ئەم جۆرەی ماڵوەیر سیخوری بەسەر کەسانی توشبوەوە دەکات کە دەکرێت چاودێری وشە نهێنییەکانی کەسی توش بوو یان سەردانی کردنی ماڵپەرەکان ...بگرێتەوە.

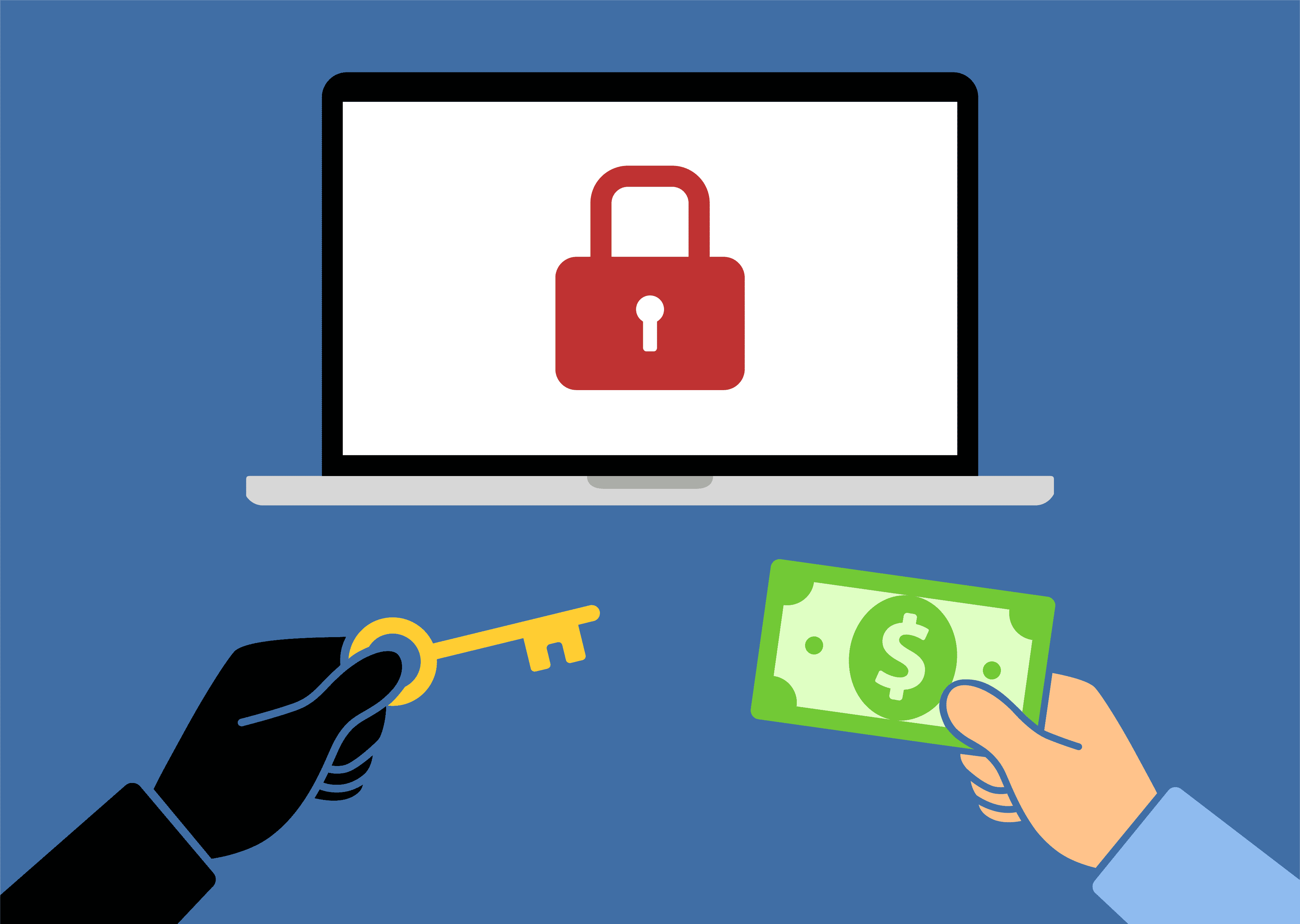
Trojan Horse – ئەسپی ترۆجان



ئەسپی ترۆجان دیزاین کراوە بۆ ئەوەی وەک بەرنامەیەکی بەسود دەربکەوێت بۆ گەشتن بە سیستەمێک، پاش دامەزراندنی بەرنامەی دیاری کراو، ترۆجانەکان دەتوانن کردارە خراپەکانیان جێبەجێ بکەن، بەشێوەیەکی رونتر بەنمونە بەرنامەی مایکرۆسۆفت ئۆفیس لەبنەرەتدا بە پارەیە و دەبێت بەکارهێنەر بەرنامەکە بکرێت، هاکەرەکان دێن بەرنامەی ئۆفیس کراک دەکەن وە ترۆجانێکی لەگەڵ پەیوەست دەکەن لەم کاتەدا بەرنامەی ئۆفیسی کراک کراو وەک ئەسپی تەروادە بەکاردێنن و هاکەر ماڵوەیرەکەی دەکاتە نێو بەرنامەی ئۆفیسەوە، کەسی بەکارهێنەر کاتێک بەرنامەی ئۆفیس دەکاتەوە ئەوا لە روکاردا بەبێ هیچ گرفتێک کار دەکات، بەڵام لە پشتەوە ماڵوەیر / ترۆجانی هاکەر دەست بە چالاکی دەکات لە نێو سیستەمی کەسی توشبودا، بەرنامەی ئێن جەی ڕات کە یەکێکە لە بەرنامەکانی ڕات کە بۆ دروست کردنی ترۆجان بەکاردێت کۆمەڵێکی یەکجار زۆر فرمانی مەترسیدار هاکەر دەتوانێت جێبەجێی بکات لەسەر کەسی توشبوو. دەکرێت ڤایرۆس، ڕانسۆموەیر، کیلۆگەر، ۆرم... پەیوەستی بەرنامەیەکی بەسود بکرێت، ئەو کاتە بەرنامە بەسودەکە دەبێتە ئەسپی تەروادەی یۆنانی کۆن و ماڵوەیرەکەش دەبێتە سەربازەکانی نێو ئەو ئەسپە.

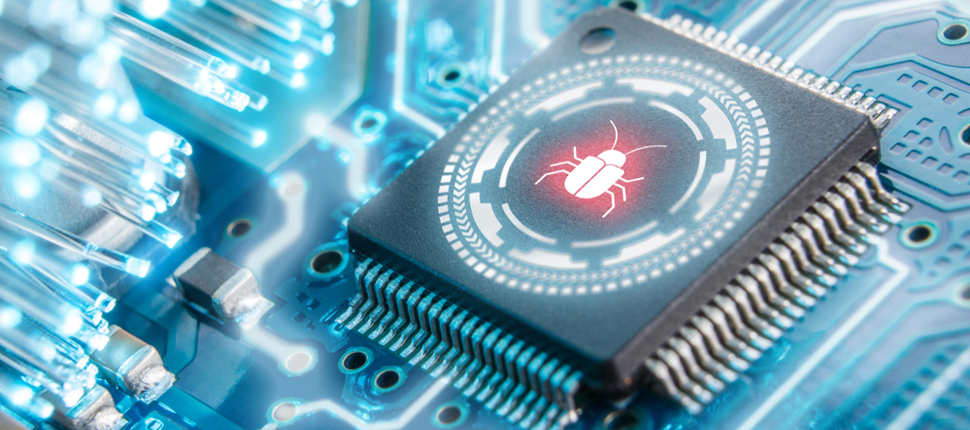


Ransomware – ڕانسۆموەیر



ڕانسۆموەیرەکان سیستەمی بەکارهێنەرە توشبووەکان داتاکانیان تەشفیر/ ئینکریپت دەکەن، پاشان تاوانبارانی سایبەر داوای پارە لە کەسی قوربانی دەکەن لە بەرامبەر دیکرپت کردنی / کردنەوەی داتاکانی سیستەمی کەسی قوربانی.

Rootkit – ڕوتکیت



ڕوتکیت پرۆگرامێکی نهێنی کۆمپیوتەرە کە دیزاین کراوە بۆ دەست گەشتنی بەردەوام بە کۆمپیوتەر لە کاتێکدا بەشێوەیەکی چالاک بوونی خۆی دەشارێتەوە، روت-کیت لە وشەی روت-ی سیستەمی یونیکسەوە هاتووە وە ئەم جۆرەی ماڵوەیر دەسەڵاتی بەرێوەبەری هەیە لەسەر ئەو ئامێرانەی کە جێگیر دەبێت تیایاندا، کێشەی ئەم جۆرەی ماڵوەیر ئەوەیە دۆزینەوەی لەسەر ئامێرەکان مەحاڵە، چونکە لە چینە نزمەکاندا کار دەکات وەک کێرناڵی سیستەم و بایۆس وە پاش دۆزینەوەی ئەوا سرینەوەی ئاسان نییە، زۆر جار دەبێت ئەو بەشەی کۆمپیوتەر بگۆردرێت کە ڕوتکیتی لەسەر جێگیر کراوە.

Backdoor – پشتەوە / دەرگای پشتەوە



ڤایرۆسی پشتەوە یان ترۆجانی لە دورەوە فرمان پێکراو، بەشێوەیەکی نهێنی دەرگایەک دەکاتەوە لە سیستەمدا کە ڕێگە بە کۆنترۆڵ کردنی ئامێرەکان دەدات لە دورەوە.

Adware – ئادوەیر



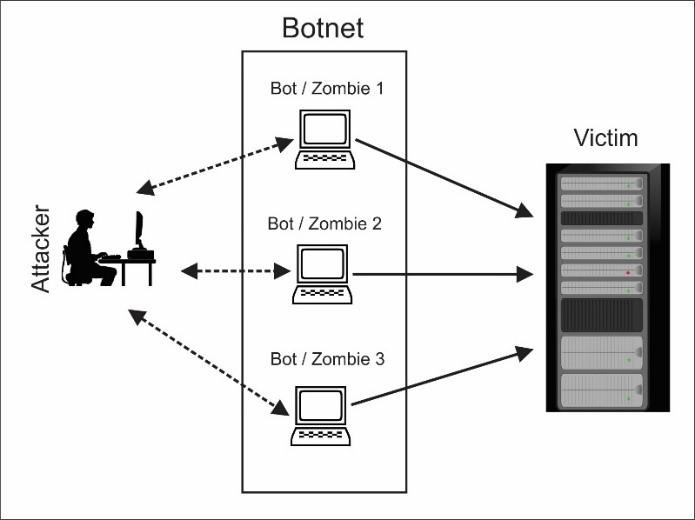
وەک لە ناوەکەیدا دیارە advertisement-supported software کاری ئەم ماڵوەیرە کۆکردنەوەی چالاکییەکانی بەکارهێنەرە لە براوسەر/ وێبگەرەکاندا و پاشان نیشاندانی ڕیکلام لەو بوارەدا، بەنمونە زۆرترین چالاکی کەسێک دەربارەی بەشە جیاوازەکانی هاردوەیری کۆمپیوتەرە، لەم کاتەدا ئادوەیرەکان ئەم چالاکیانە تۆمار دەکەن و دەینێرن بۆ خاوەن ریکلامەکان، پاشان خاوەن ریکلامەکان ریکلامی پارچە جیاوازەکانی هاردوەیری کۆمپیوتەر نیشانی کەسی توش بوو دەدەن تا بابەتەکان بکرێت.

Keylogger – کیلۆگەر



کیلۆگەر هەروەها پێشی دەوترێت چاودێریکاری سیستەم، بەنزیکەی هەموو ئەو شتانەی کە بەکارهێنەر لەسەر کۆمپیوتەر ئەنجامی دەدات تۆماری دەکات و دەینێرێت بۆ کەسی خاوەن کیلۆگەر وەک ئەو وشانەی کە دەینوسین و وشەی نهێنی و هەژمارە خەزنکراوەکانی ناو براوسەرەکانمان و سەردانی کردنی ماڵپەرەکان و ئەو کلیلە وشانەی کە بەرنامەکانمان پێ چالاک کردووە.

Botnet – بوتنێت



بوتنێت کورت کراوەی وشەکانی robot network تۆرێکی کۆمپیوتەری توشبووە بە ماڵوەیر، لە ژێر کۆنترۆڵی تاکە هێرشبەرێکدان کە بە کەسی هێرش بەر دەوترێت bot-herder وە بە کۆمپیوتەرە توش بووەکان دەوترێت زۆمبی، کەسی خاوەن بوت-نێت دەتوانێت زۆمبی کەسانی قوربانی بەکاربهێنێت بۆ هێرشی بەکۆمەڵ بۆ سەر ماڵپەر و سێرڤەرەکان یان بەکاریان بهێنێت بۆ دروستکردنی دراوی ئەلیکترۆنی یان سیخوری بکات بەسەر کەسانی قوربانیەوە.

**بەناوبانگترین ڕانسۆموەیرەکانی ساڵی ٢٠٢١**

Buffalo Public Schools

Acer

CNA Financial

Applus Technologies

Quanta Computer

ExaGrid

Ireland's Health Service Executive (HSE)

AXA S.A.

JBS USA

**پێنج گەورەترین هێرشی ڕانسۆموەیر لە مێژودا**



WannaCry

TeslaCrypt

NotPetya

REvil or Sodinokibi

SamSam

**WannaCry**

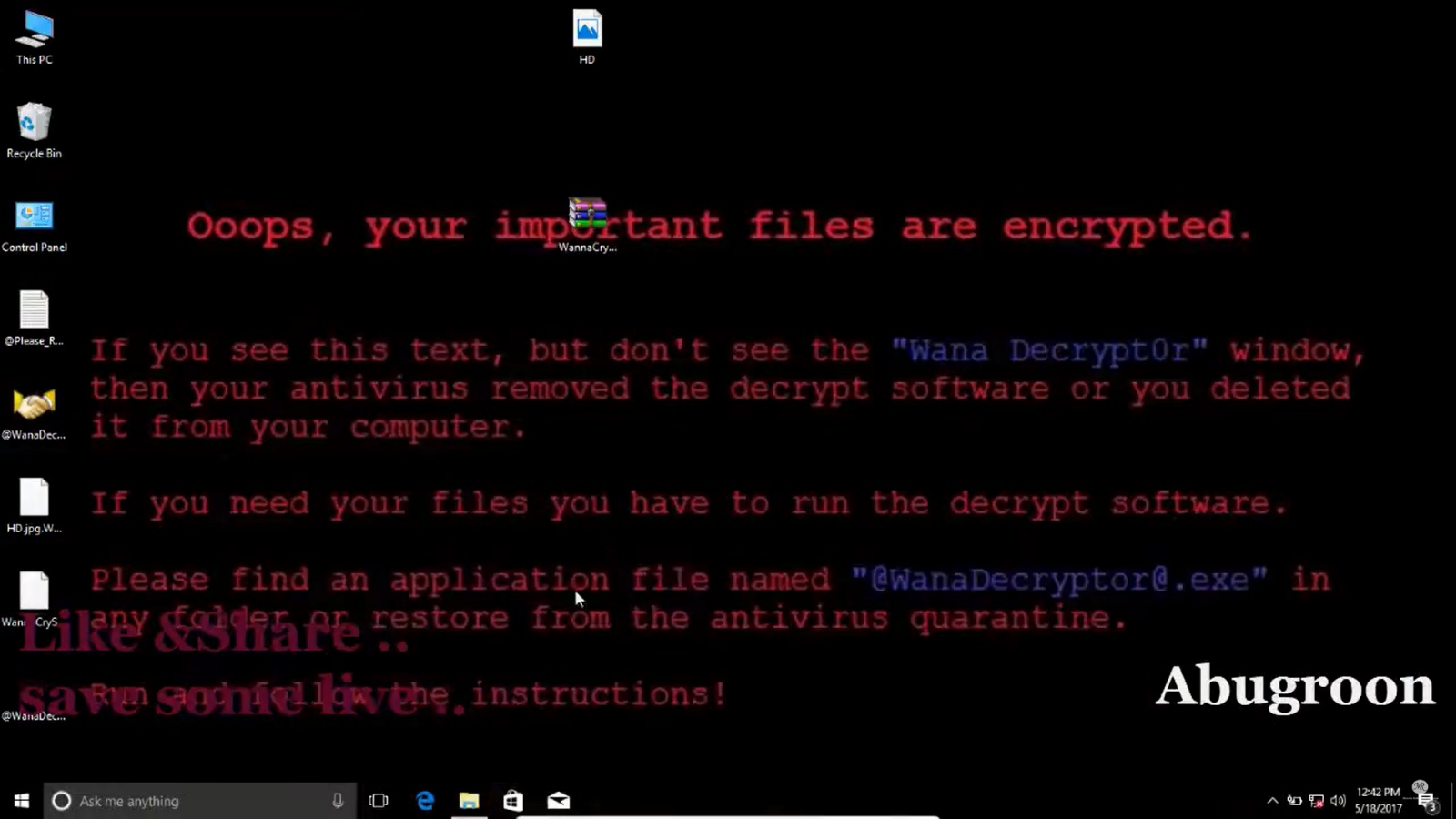
بۆ ئەوەی باشتر لە مەترسی هێرشی ڕانسۆموەیر تێبگەین، زۆر بەکورتی باسی وانە-کرای دەکەین.



وانەکرای کاتێک ئاگاداری کەسی توشبوو دەکات

لە مانگی ٥ ساڵی ٢٠١٧ کۆمپانیاکان لە سەرتاسەری جیهاندا توشی خێراترین هێرشی ماڵوەیر بوون کە ناسراوە بە وانە-کرای، ئەم ڕانسۆموەیرە کە توشی سیستەمی ویندۆز بوو لە یەکەم کاتژمێری بڵاوبونەوەیدا ٧٠٠٠ کۆمپیوتەر توشبوون بەم هێرشە، وە لەماوەی تەنها دوو ڕۆژدا بڵاوبووەوە لە ١١٠،٠٠٠ ناونیشانی ئای پی-دا، وانە-کرای بە یەکێک لە گەورەترین هێرشەکانی ڕانسۆموەیر دادەنرێت لە مێژودا، کە لەتەواوی کار و پیشەسازییە جیاوازەکاندا بڵاوبوویەوە، یەکێک لە دیارترین ئەو کۆمپانیانەی کە توشی ئەم هێرشە بوویەوە کۆمپانیای هۆندای بەرهەمهێنی ئۆتۆمۆبیل بوو، لەسەرەتای توشبوونی ئامێرەکان بەم ڕانسۆموەیرە تا سێ ڕۆژی سەرەتا داوای ٣٠٠ دۆلار دەکات بۆ کردنەوەی فایلە قوفڵ بووەکان وە بۆ شەش رۆژی دواتر داوای ٦٠٠ دۆلار دەکات کە بەشێوەی دراوی بیت-کۆین دەبێت بینێریت بۆ لایەنی هێرشبەر، لەدوای ئەو ماوەیە ئەوا هەموو فایلەکانت بۆ هەمیشە لەدەست دەدەیت.

باوترین ئەو پاشگری فایلانەی کە وانە-کرای کردبوونیە ئامانج



سەرچاوەی وێنە کەناڵی Moawia Abugroon لە یوتیوب

فایلەکانی ئوفیس

ppt – doc – docx – xlsx – sxi

فایلەکانی ئەرشیف و میدیا

Zip – rar – tar – mp4

فایلەکانی داتابەیس

sql – accdb – mdb – odb

فایلەکانی گرافیک و فۆتۆگرافی

Vsd – raw – svg – psd

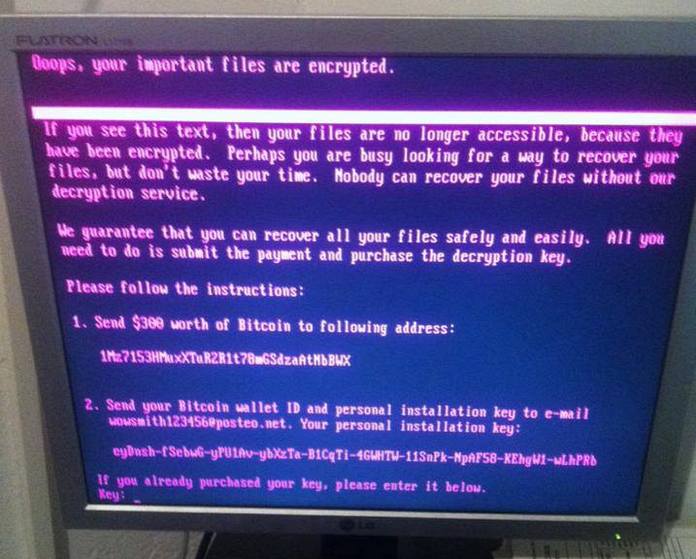
وە جۆرە جیاوازەکانی تری فایل

ئەم ڕانسۆموەیرە لە دوو شوینی هاردی سی دەدا بەزۆری

بەناوی tasksche.exe لە فۆڵدەری ProgramData -ی هاردی سی

بەناوەکانی tasksche.exe و mssecsvc.exe لە فۆڵدەری Windows -ی هاردی سی

**چۆنییەتی خۆپاراستن لە ڕانسۆموەیر**



ئاگاداری ڕانسۆموەیری NotPetya لەسەر شاشەی سیستەمێکی ویندۆز

خۆپاراستن باشترە لە خۆ چارەسەرکردن، بۆ ئەوەی خۆت بپارێزیت لەم هێرشە مەترسیدارە پێویستە زانیاریت لەسەر ڕانسۆموەیر ببێت وە ئەم خاڵانەی خوارەوە جێبەجێ بکەیت.

یەکەم/ سەردانی نەکردنی ماڵپەڕی نەناسراو و گوماناوی.

دووەم/ داونلۆد نەکردن و بەکارنەهێنانی بەرنامە و داتا لە ماڵپەڕی نەناسراو و خەڵکی نەناسراوی ناو فەیسبوک و تۆرە کۆمەڵایەتییەکان و ئیمەیڵ..هتد.

سێیەم/ دابەزاندنی دژە ڤایرۆس و دژە ماڵوەیر و بەردەوام نوێکردنەوەیان وە بەکارنەهێنانی بەرنامەی کراک کراو و فایلی گوماناوی.  
چوارەم/ نەگواستنەوەی هیچ داتایەک لەو کۆمپیوتەرەی کە توشی ڕانسۆموەیر دەبێت.

پێنجەم/ ئەگەر تۆر و کۆمپانیای دابینکەری ئینتەرنێت یان تۆری ناوخۆی توشی ڕانسۆموەیر بوو، ئەوا کۆمپیوتەرەکەت پەیوەستی ئەو تۆڕ و کۆمپانیایە مەکە.

شەشەم/ بەکارهێنانی نوێترین سیستەمی بەگەڕخستن (بۆ نمونە ویندۆز یازدە نەک ویندۆز حەوت، ئوبونتوی ٢٢ نەک ١٤) بەردەوام نوێکردنەوەی سیستەمی بەگەڕخستنەکەت، زیادکردنی ئەد بلۆکەر بۆ براوسەرەکەت بۆ ئەوەی فلتەری ڕیکلام و ڤایرۆس بکات بۆت.

حەوتەم/ چالاک کردنی فایەر ۆڵ/دیواری ئاگرینی سیستەمەکەت.

هەشتەم/ گرنگترین فایلەکانت لە هاردی دەرەکی یان کلاودێکی وەک مێگا دابنێ (باک-ئەپ کردنی داتا گرنگەکانت).

نۆیەم/ بەکاری بهێنە وێب براوسەرێکی بەهێزی وەک گۆگڵ کرۆم یان فایەر فۆکس و بەردەوام نوێکردنەوەی.

دەیەم/ دوای تەواو بونی کارەکانت کوژاندنەوەی ئینتەرنێت وە کوژاندنەوەی کۆمپیوتەرەکەت بۆ ئەوەی لە هێرشی هاکەرەکان زیاتر پارێزاو بیت وە بەرنامەکانت بە شێوەیەکی چالاکتر کار بکەن.

یازدەیەم/ خۆشارەزاکردن لە کۆمپیوتەر و تەکنەلۆجیا و ئاگاداربوون لە هەواڵ و مەترسییەکانی ڕانسۆموەیر و ڤایرۆسەکان.

دوازدەیەم/ هاردەکانی دی و ئی ..هتد قوفڵ بکە بە بەرنامەی bitlocker ناو سیستەمی ویندۆز، بەم شێوەیە ئەگەر توشی ڕانسۆموەیر و ڤایرۆس ببیت، ئەوا ئەو هاردانەی کە قوفڵت کردون داتاکانی پارێزراو دەبیت، چونکە قوفڵدانی هارد ڕێگە دەگرێت لە چونەژورەوەی ڤایرۆس بۆ ناو هاردەکەت، بەمەرجێک قوفڵی سەر هاردەکەت نەکەیتەوە کاتێک توشی ڤایرۆس و هاک بوون بویت.

\*ئەگەر لە وڵاتەکانی وەک بەریتانیا و ئەمریکا و ئەڵمانیا...هتد دەژیت دوای ناردنی پارە بۆ هاکەران وە بەدەست هێنانی توڵی کردنەوەی فایلە قوفڵ کراوەکانت، پەیوەندی بە ئەو بانکەوە بکە کە بەشداریت کردووە تێیدا و شکات بکە لەو کەسەی پارەت بۆ ناردووە، ئەگەری هەیە بانک پارەکەت لە گروپی هاکەران وەربگرێتەوە و بۆت بگێڕێتەوە، ئەگەریش لەو وڵاتانە نیت ئەوا سکاڵا لای پۆلیس بکە و لەوانەیە بتوانن پارەکەت بۆ بگێڕنەوە.

**(ئەگەر شێوازی پارە ناردنەکە بیت-کۆین نەبوو)**

**هەنگاوە خێراکان بۆ ئەوەی کێشەکە گەورەتر نەبێت**



یەکەم/ ئەو کۆمپیوتەرەی کە توشی ماڵوەیری ڕانسۆموەیر بووە مەیدە لە ئینتەرنێت، مەگەر زۆر زەرور نەبیت، چونکە هاکیش کراویت ئەگەر هەژمارەکانت بکەیتەوە وەک فەیسبوک و هەژمار بانکی...هتد هەژمارەکانیشت دەبەن، وە لەوانەیە داتای ناو کۆمپیوتەرەکەشت ببەن و دواتر هەڕەشەت لێ بکەن بەوەی کە بڵاوی دەکەنەوە(هاکەرەکان دەتوانن قوفڵی سەر فایلەکان لابدەن، چونکە خۆیان بۆیان قوفڵ داویت)

دووەم/ بەهیچ شێوەیەک فلاش و هارد مەدە لەو کۆمپیوتەرەی کە توش بووە و دواتر بیدەیت لە کۆمپیوتەری تر، با ئامێری تریشت توشی ئەو ماڵوەیرە نەبن و فایل و داتای کۆمپیوتەر و هارد و فلاشەکانت قوفڵ نەبن

سییەم/ ئەگەر لە ڕێکخراو و شوێنێکیت کە تۆڕی ناوخۆیتان هەیە ئەوا کۆمپیوتەرەکەت پەیوەستی ئەو تۆرە مەکە با ڕانسۆموەیرەکە نەدات لە تۆڕ و کۆمپیوتەرەکانی تریش.

**تێبینی**

ئەگەر ویستت پارە بدەیت بۆ ئەوەی داتاکانت لەناو نەچن، ئەوا دەبێت ئەنتی ڤایرۆس رابگریت زوو بۆ ئەوەی رانسۆموەیرەکە تێکنەچێت و بتوانیت بەو ئامرازانەی دانراوە تێیدا داتاکانت دیکریپت / قوفڵی سەر فایلەکان بکەیتەوە، دەبێت ئەوەش بڵێم هیچ سەرچاوەیەکی سکویریتی پێشنیاری ناردنی پارە ناکات بۆ کەسانی خاوەن ماڵوەیر، چونکە هیچ گەرەنتییەک کە هاوکاریت بکەن و داتاکانت بۆ دیکریپت بکەن بەڵکو هەندێک جار دەزانن کە پارەداریت ئەوا داوای پارەی ترت لێدەکەن و هیچ هاوکاریەکیشت ناکەن.

**هەنگاوەکانی پاککردنەوەی کۆمپیوتەرەکەت لە ماڵوەیری ڕانسۆموەیر**



یەکەم/ ئەو وێب براوسەرەی بەکاری دێنیت هیستۆرییەکەی بسڕەوە، بۆ ئەوەی ئەو ئیمەیڵ و پاسۆردانەی کە خەزن بووە لە براوسەرەکەتدا بسڕێنەوە، وە بە ئامێرێکی تر/کۆمپیوتەرێک وشەی نهێنی هەموو هەژمارەکانت بگۆرە، چونکە هەرچی هەژماری کراوەی سەر ئامێرە توشبوەکەت هەیە کۆپییەک لە زانیاری"ئیمەیڵ و وشەی نهێنی " هەیە چووە بۆ هاکەر/هێرشبەرەکان.

دووەم-ئەگەری یەکەم/ ئەم دوو بەرنامەیە بەکاربهێنە بۆ سڕینەوەی ڕانسۆموەیر لە کۆمپیوتەرەکەتدا.

سەردانی ئەم ماڵپەڕە بکە و ئەو ئەنتی ڤایرۆسە دابەزێنە

[360totalsecurity.com/en](https://www.360totalsecurity.com/en/)

وە ئەم دژە ماڵوەیرە دابەزێنە

[malwarebytes.com](https://www.malwarebytes.com/)

تێبینی: هەندێک ڕانسۆموەیر ماڵپەڕەکانی ئەنتی ڤایرۆست لێ بلۆک دەکەن و ماڵپەڕەکان ناکرێنەوە، ئەمە واتای ئەوە نییە کە ئەو ماڵپەڕانە کێشەیان تێدایە، بەڵکو کێشە لە کۆمپیوتەرەکەی تۆدایە، ئەو ماڵوەیرەی کە توشت بووە ماڵپەڕەکانی بلۆک کردووە.



دووەم-ئەگەری دووەم/ ئەگەر ماڵپەڕەکانی ئەنتی ڤایرۆس نەکرانەوە، ئەوا بە کۆمپیوتەرێکی تر ئەنتی ڤایرۆسی 360 total security و Malwarebytes داونلۆد بکە، دواتر لەڕێگای میدیا فایەر یان هەر جێگەیەک کە پێت باشە ئەپلۆدی بکە و لە کۆمپیوتەرە توشبووەکەدا ئەو لینکی دوو بەرنامەیە بنوسە کە ئەپلۆدت کردووە و داونلۆدی بکە و دایبەزێنە و چەند جارێک سکان و پشکنینی کۆمپیوتەرەکەت بکە، بەم شێوەیە ماڵوەیری ڕانسۆموەیر لە کۆمپیوتەرەکەتدا نامێنێت و ترست نامێنێت لە ڕێگەی فلاش و هاردەوە بگوازرێتەوە بۆ کۆمپیوتەری تر، پیرۆزە ماڵوەیر نەما لە کۆمپیوتەرەکەتدا، تێبینی دەشتوانی هاردی سی فۆرمات بکەیت و دوبارە سیستەمێکی بەگەڕخستن دابەزێنیت و دواتر سکانی هاردەکانی تر و هاردی سی بکەیت، بەڵام دابەزاندی بەرنامەکانی دوای فۆرمات کاتی زۆرت دەبات، هەر چۆنێک بێت ئەو دوو ڕێگەیە یەکیان ئەنجام بدە، با ماڵوەیری رانسۆموەیرەکە لە ئامێرەکەتدا نەمێنێت، (دەتوانیت ئەنتی ڤایرۆس و ئەنتی ماڵوەیر بکەیتە ناو فلاشێک و دواتر بیگوازیتەوە بۆ کۆمپیوتەری توشبوو، بۆ ئەوەی رانسۆموەیرەکە نەدات لەو تۆڕەی کە پەیوەستی بویت، بەڵام ئاگاداربە ئەو فلاشە مەدە لە هیچ ئامێرێکی تر، دوای پاککردنەوەی کۆمپیوتەری توش بوو، ئەوا ئەنتی ڤایرۆس با لەو کۆمپیوتەرەدا چالاک بێت و فلاشەکە سکان بکە یان فۆڕماتی بکە، بۆ ئەوەی فلاشەکە پاک ببێتەوە لە و رانسۆموەیرەی کە توشی بوویت).

**هەنگاوەکانی چارەسەر کردنی فایلە قوفل بووەکانت/ئینکریپت بووەکانت**

ئێستا دەبێت چارەسەری ئەو فایلانە بکەیت کە قوفڵ بوون



ڕێگای یەکەم/ پارەدان بە خاوەن ڕانسۆموەیر، ئەگەر داتاکان زۆر گرنگن یان هی کۆمپانیا و شوێنی هەستیارە، پارە بنێرە بۆ هێرشبەر/خاوەن ڕانسۆموەیر و با بەرنامەت بۆ بنێرن و قوفڵی سەر فایلەکانت لاببەیت، ئەگەر خاوەن ویشدان بن چونکە هیچ گەرەنتییەک نییە دوای پارە ناردن بەرنامە(کلیلی کردنەوە)ت بۆ بنێرن بۆ چارەسەرکردنی فایلە قوفڵ بووەکانت.  
  
ڕێگای دووەم/ گریمان تۆ ئامادە نیت پارە بدەیت بە هاکەرەکان/خاوەن رانسۆموەیر:

ا/ ئەگەر ڤایرۆسی ڕانسۆموەیرەکە تازە دروست کرابێت ئەوە چارەسەری ڕاستەوخۆت دەست ناکەوێت، دەبێت کۆمپیوتەرەکەت و داتاکانت دابنێی ماوەیەک لەوانەیە بگاتە ساڵێک و زیاتر تا چارەسەر دەدۆزرێتەوە و تۆش ئەو بەرنامەی کە دروست کراوە بەکاری دەهێنیت بۆ دیکریپت کردنی فایلەکانت/ لابردنی قوفڵی سەر فایلەکانت.

ب/ بە بەرنامەکانی ڕیکۆڤەری هەوڵبدە و دەتوانیت وێنە و کتێب و فایلی ئۆفیس و فایلی دەنگی لەسەدا هەشتای بهێنیتەوە بە بەرنامەکانی ڕیکۆڤەری

ج/ ئەگەر ئەو ڕانسۆموەیرەی کە توشت بووە زوو دروست کرابێت بۆ نمونە دوو ساڵ پێش ئێستا ئەوا لەوانەیە چارەسەری هەبێت و دەتوانیت فایلە قوفڵ بووەکانت/ئینکریپت بووەکانت قوفڵەکەی سەری لابەیت/دیکریپتی بکەیت.

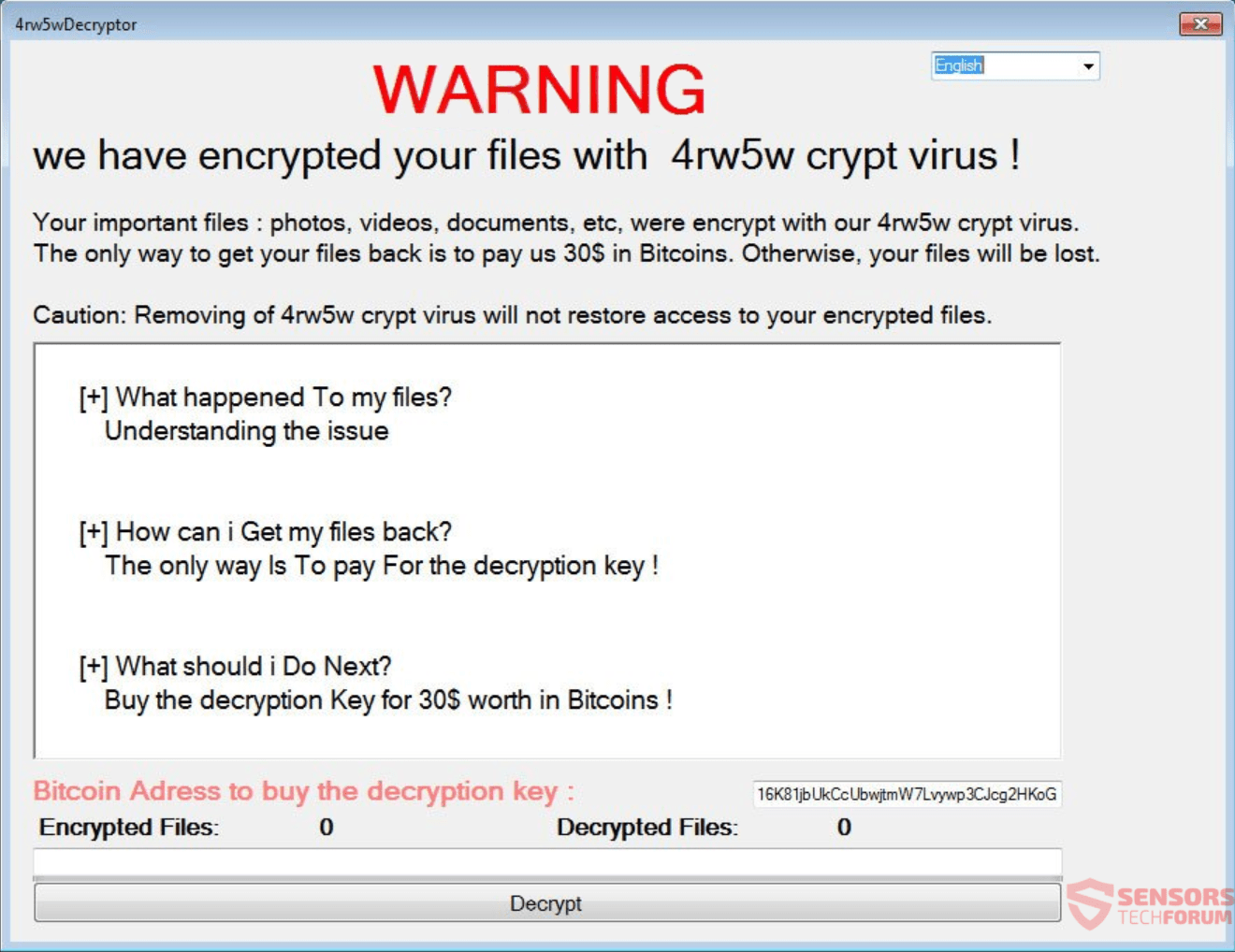
**هەندێک بەرنامەی ڕیکۆڤەری**

بۆ ئەوەی بتوانیت بەشێک لە داتا و بابەتە قوفڵ بووەکانت بەدەست بهێنیتەوە ئەوا بەرنامەکانی ڕیکۆڤەری ڕێگایەکی تا ڕادەیەکی باش بەسودن

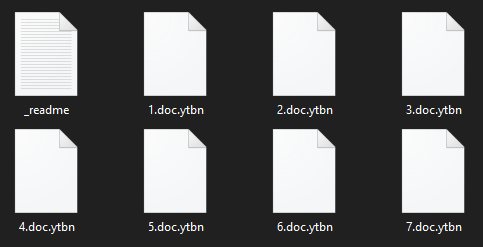


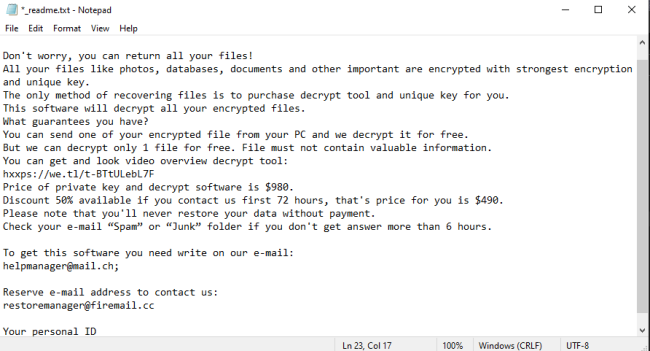
|  |  |  |
| --- | --- | --- |
| [stellarinfo.com](https://www.stellarinfo.com/) |  | STELLAR DATA RECOVERY |
| [wondershare.com](https://www.wondershare.com/) |  | Wondershare Photo Recovery |
| [wondershare.com](https://www.wondershare.com/) |  | Wondershare Data Recovery |
| [getdata.com](https://getdata.com/) |  | GetData Recover My Files |
| [icare-recovery.com](https://www.icare-recovery.com/) |  | iCare Data Recovery Pro |
| [hetmanrecovery.com](https://hetmanrecovery.com/) |  | Hetman Photo Recovery |
| [ashampoo.com](https://www.ashampoo.com/) |  | Ashampoo Photo Recovery |

ئەو بەرنامانە دەبێت پارە بدەیت تا بتوانیت چالاکیان بکەیت و بەکاریان بهێنیت، بۆیە ئەگەر شارەزایت نییە هەوڵمەدە بە کراک کراوی دایانبگریت با دوبارە توشی ڤایرۆس نەبیت، بەڵکو بە شریت بیانکڕە یان برادەرێکی شارەزات بۆت پەیدا بکات.



تێبینی/ بۆ ئەوەی بزانیت ناوی ڕانسۆموە یرێک کە توشی ئامێرێک بووە چییە لە چەندەها شوێنی کۆمپیوتەرەکەدا فایلی تێکست هەیە کە پێت دەڵیت ناوی ئەو ڕانسۆموەیرە چییە، یان بە پاشگر/ئیکستێنشنی فایلە قوفل بووەکاندا دەتوانیت بزانیت ناوی ڕانسۆموەیرەکە چییە بۆ نمونە Ytbn



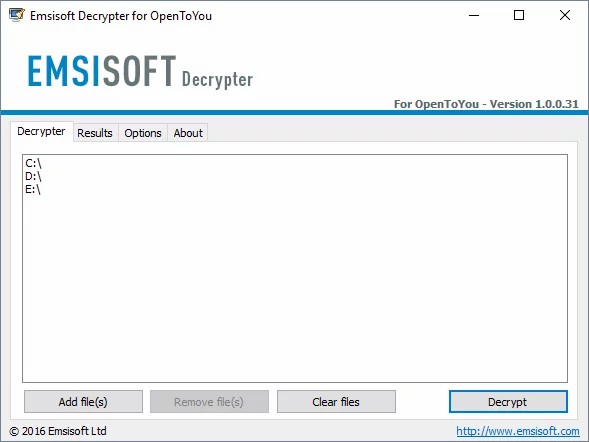


**هەندێک ئامۆژگاری بەسود**

\*هەندێک ڕانسۆموەیر کە دەدات لە کۆمپیوتەر ئەوا بایۆسەکەشت قوفڵ دەکات و ناتوانیت هیچ بە کۆمپیوتەرەکەت بکەیت وەک کردنەوەی سیستەمەکەت یان دابەزاندنی سیستەمی نوێ، لەم کاتەدا دەبێت روم -ROMی کۆمپیوتەرەکەت یان flash memory بگۆڕیت کە پێی دەوترێت ROM BIOS چونکە بایۆس تۆشی قوفڵ بوون بووە.

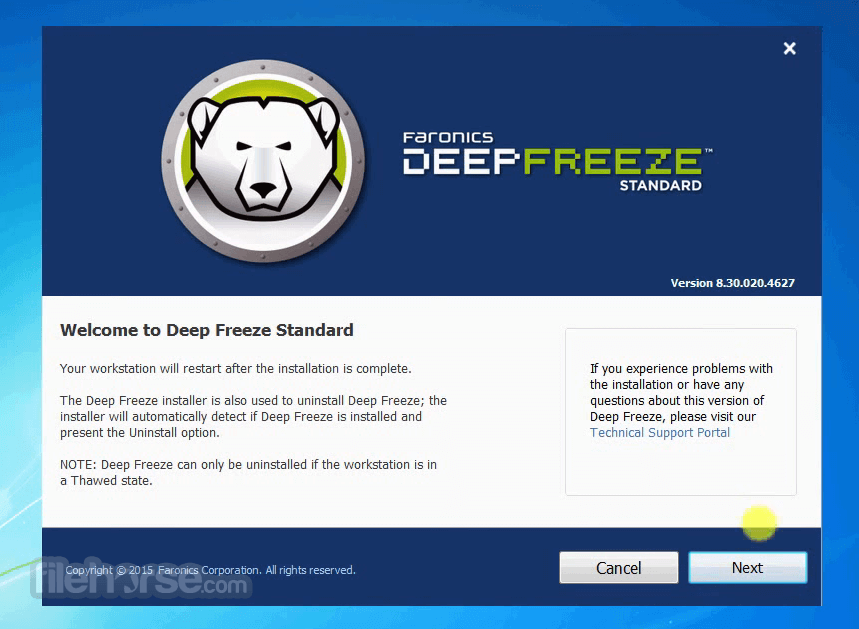
\*ئەگەر کرا کۆمپیوتەرەکەت سیستەمەکەی بگێرەوە/ڕیستۆری بکە بۆ ماوەیەک پێش ئێستا ئەو کات ئەوەی لە هاردی سی دایە، فایلەکانت کێشەی نابێت، چونکە ئەم ڕێگەیە شێوەیەکە لە ڕیکۆڤەری بۆ فایلەکانی هاردی سی.

\*بەرنامەی Emsisoft decrypter دابەزێنە ئەگەر فایلەکانت چاک کرایەوە پێی باشە ئەگەر نا دەبێت چاوەڕێ بکەیت تا چارەسەر دەدۆزرێتەوە و تۆش ئەوکات بەرنامەکە نوێ بکەرەوە و چارەسەری فایلەکانت بکە، ماڵپەری بەرنامە [emsisoft.com](https://www.emsisoft.com/en/)



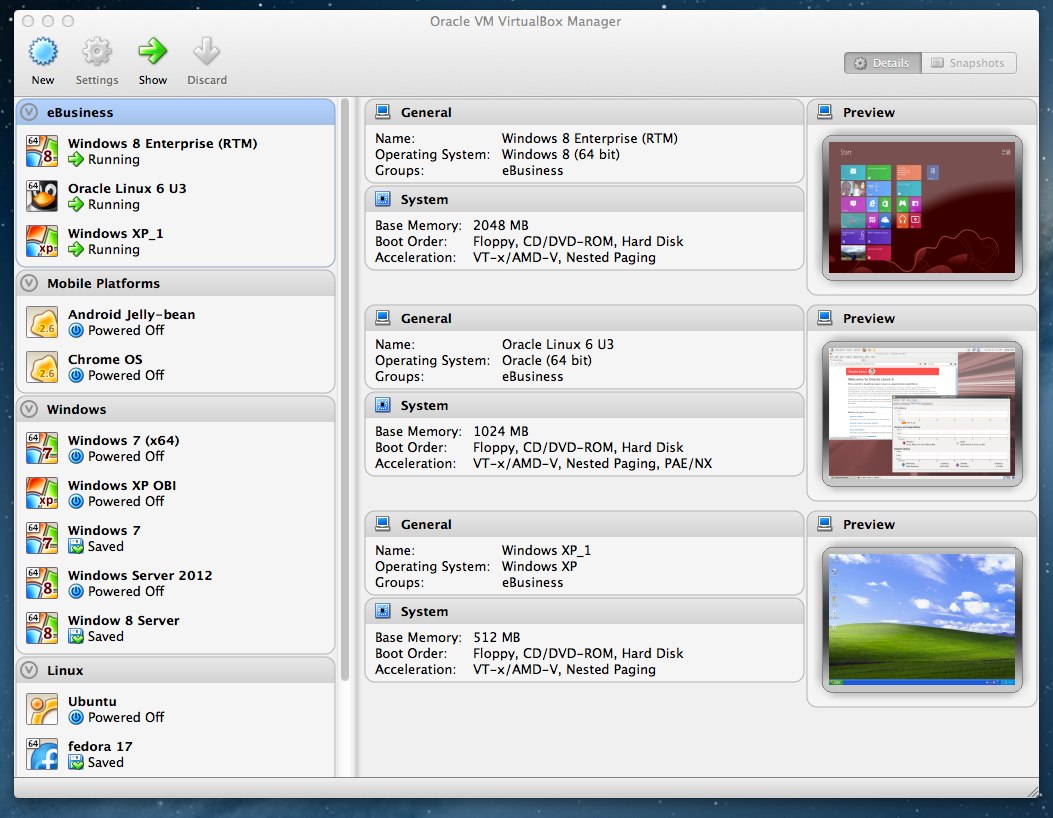
\*ئەم دوو بەرنامەیەش دەتوانیت بەکاربهێنیت بۆ گێڕانەوەی داتاکانت

ShadowExplorer - PhotoRec



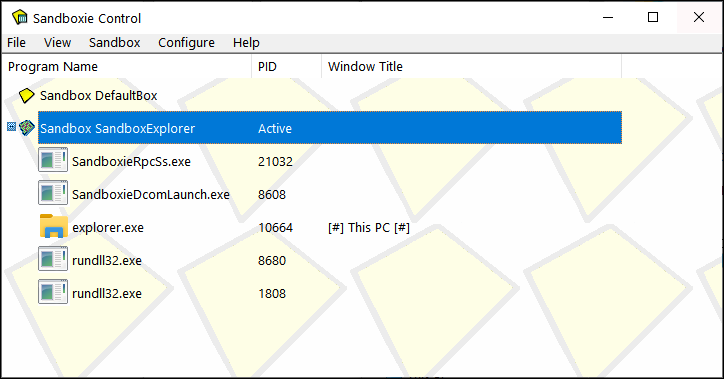
\*دەتوانیت هاردی دی و ئی ..هتد قوفڵ بکەیت و هاردی سی و سیستەمەکەت بە بەرنامەکانی وەک دیپ-فریز و شادۆ-دیفێندەر فریز بکەیت(هەرچی بکەیت و هەر گۆڕانکارییەک لە هاردی سی و سیستەمەکەتدا بکەیت دوای ڕیستارت کردنی کۆمپیوتەرەکەت وەک خۆی لێ دێتەوە، من لە ٢٠١٤ وە هاردی سی واتە سیستەمەکەم بە دیپ فریز و ئێستاش بە شادۆ دیفێندەر فریز کردووە)، ئەوکات ئەگەر رانسۆموەیر بدات لە کۆمپیوتەرەکەت ئەوا بەریستارت کردن هاردی سی وەک خۆی لێ دێتەوە، وە هاردەکانی دی و ئی ..هتد هیچ فایلێکی قوفڵ نابێت و ڤایرۆس لێی نادات ئەگەر هاردەکان نەکرابنەوە، چونکە ڤایرۆس و رانسۆموەیر ناتوانن بیت-لۆکەر/bitlocker تێپەڕێنن.





\*دەتوانیت بە بەرنامەکانی مەکینەی خەیاڵی وەک ڤی.ئێم وەیر و ڤیرچواڵ بۆکس سیستەمی خەیاڵی دروست بکەیت وە فایلی گوماناوی لەوێدا تاقی بکەیتەوە، بەم شێوەیە ئەگەر ڤایرۆسیش بە بەرنامەکانەوە بێت ناتوانێت بپەڕێتەوە بۆ سیستەمە سەرەکییەکەت.

\*دەتوانیت پێش بەکارهێنانی بەرنامە و فایلە نەناسراوەکان سەرەتا لەناو بەرنامەی Sandboxie یان هاوشێوەکانی ئەم بەرنامەیە فایلەکان تاقی بکەیتەوە.



\*پێش دابەزاند یان کارکردن بە هەر فایلێک ئەوا بە ئەنتی ڤایرۆس سکانی بکە، وە لەکاتی کردنەوەی هەر فایلێکدا با ئەنتی ڤایرۆسەکەت چالاک بێت.

\*ئەو بەرنامە و فایلانەی کە بەپارەن بیانکڕە یان هاوشێوەیان هەیە کە فرین/بەخۆراین بەکاریان بهێنە، ئەگەریش هەر زۆر پێویستت بە بەرنامەیەکی کراک کراو هەبوو، سەرەتا ناوی ئەو ماڵپەڕەی کە دەتەوێت بەرنامە و داتای بەشێوەیەکی نایاسای لێوە دابگریت لە گۆگڵ بینوسە و بزانە بابەتەکان چی دەربارەی ئەو ماڵپەڕە دەڵێن، وە دوای داگرتنی بابەتەکان با ئەنتی ڤایرۆست چالاک بێت.

\*دەتوانیت هاردی کۆمپیوتەرەکەت دەربکەیت کە توشی ماڵوەیری ڕانسۆموەیر بووە و دای بنێیت تا چارەسەری بۆ دێت و هاردێکی نوێ بخەیتەسەر کۆمپیوتەرەکەت.

\*مەرج نییە تەنها بەدابەزاندنی بەرنامە و فایلی کراک کراو و نایاسای توشی هێرشی ڕانسۆموەیر ببیت، هەندێک جار لایەنی هێرشکار ڤایرۆس دەدات لە تۆڕی ناوچەیەک و تۆش توش دەبیت کە لەناو ئەو تۆڕەدایت، یان هەڵەیەک لە سیستەمی کارپێکردن یان بەرنامەیەک دەدۆزنەوە و هێرش دەکەنە سەر ئەو خاڵە لاوازە و تۆش توشی ئەو هێرشە دەبیت، بۆیە هەمیشە بەرنامە و سیستەمەکەت نوێبکەرەوە و ئەگەر بیستت هێرشی ڤایرۆس و ماڵوەیر کراوەتە سەر تۆڕێک ئەوا بەکاری مەهێنە، تا چارەسەری ئەو هێرشە دەدۆزرێتەوە و هێرشەکە رادەگیرێت، یان ئەو کەلێنەی کە لە سیستەم و ئەو بەرنامەیەدا هەیە نوێکردنەوەی بۆدێت و هێرشەکە رادەگیرێت.

\*لەوانەیە ماڵوەیری ڕانسۆموەیر بدات لە کۆمپیوتەرەکانی هەندێک کەسمان ئەوا کێشەمان نەبێت و تەنها چەند بەرنامەیەکی کراک کراو لەناو کۆمپیوتەرەکانماندا هەبێت یان چەند وێنە و ڤیدیۆیەکی پێکەنین و دوبارە لە ئینتەرنێتەوە دایانبگرینەوە یان پێشتر داتاکانمان هەڵگرتبێت لە نێو هاردێکی دەرەکی یان کلاودێکدا، بەڵام تۆ حسابی ئەوە بکە ئەگەر ڕانسۆموەیر بدات لە کۆمپانیا گەورەکان بە سەدان تێرابایت داتایان قوفڵ دەبێت، ئەو داتایانە کۆکراوەی هەزاران کارمەند و زانایە و ١٠ یان ٢٠ ساڵ و زیاتری خایاندووە تا ئەو زانیارییانەیان کۆکردۆتەوە، بە سەدان و بگرە هەزاران کۆمپیوتەریان هەیە، ئەو کات دەزانرێت کە زیان و مەترسی ڕانسۆموەیر چەندە گەورە و مەترسیدارە.



سەرچاوەی وێنە ماڵپەری japantimes.co.jp

**وتەی کۆتایی**

ماڵوەیری ڕانسۆموەیر زیانەکانی زۆر گەورەیە وە رۆژ لە دوای رۆژ هێرشی ڕانسۆموەیر لە زیادبوندایە، زۆر گرنگە بابەت لەسەر ئەم جۆرەی ماڵوەیر بنوسرێت، ئەم بابەتەی بەردەستت ڕاپۆرتێکە لەسەر ئەم بابەتە بۆیە ناتوانین زۆر درێژە بەم باسە بدەین، لە خوارەوە چەند سەرچاوەیەک دادەنێین تا بتوانن باشتر لێکۆڵێنەوە لەسەر ڕانسۆموەیر بکەن...

What Is Malware?

[cisco / what is malware](https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html)

[malwarebytes / malware](https://www.malwarebytes.com/malware)

[techtarget / malware](https://www.techtarget.com/searchsecurity/definition/malware)

What is Ransomware?

[proofpoint / ransomware](https://www.proofpoint.com/us/threat-reference/ransomware)

[trellix / what is ransomware](https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html)

[A full analysis of the BlackMatter ransomware](https://resources.infosecinstitute.com/topic/a-full-analysis-of-the-blackmatter-ransomware/)

[HugoLB0 / Ransom0](https://github.com/HugoLB0/Ransom0)

[i created malware with Python (it's SCARY easy!!)](https://www.youtube.com/watch?v=UtMMjXOlRQc&ab_channel=NetworkChuck)

[Reverse Engineering Microsoft Exchange DearCry Ransomware | Brief Analysis](https://www.youtube.com/watch?v=s75edLEbPJc&ab_channel=MotasemHamdan)

[reverse engineering wannacry in computer and tracking all ips and process | 0xDarkgw](https://www.youtube.com/watch?v=2GCYEG8bjo0&ab_channel=BlackBird)

**سەرچاوەکان**

[wikipedia.org](https://en.wikipedia.org/" \t "_blank)

[mcafee.com](https://www.mcafee.com/)

[YouTube/Kaspersky](https://www.youtube.com/user/Kaspersky)

[YouTube/LinusTechTips](https://www.youtube.com/user/LinusTechTips)

[techtarget.com](https://www.techtarget.com/)

[swisscyberforum.com](https://www.swisscyberforum.com/)

[1877.krd](https://1877.krd/)

سوپاس بۆ ئەم بەڕێزانە ئەرکی پێداچونەوەی ڕاپۆرتیان گرتە ئەستۆ

محمد جەبار

بینەر فەریق

ناوەندی شیکار

[t.me/Shikar\_Center](https://t.me/Shikar_Center)



بەرواری بڵاوکراوە

١-٨-٢٠٢٢