Ransomware CryptoWall 4.0 là gì? Làm thế nào để dọn sạch Ransomware CryptoWall 4.0?

CryptoWall 4.0 là một dạng ransomware mã hóa các tập tin, ransomware này sẽ mã hóa các tài liệu cá nhân mà nó phát hiện trên máy tính của nạn nhân bằng cách sử dụng key RSA-2048 (thuật toán mã hóa AES CBC 256-bit). Sau đó sẽ hiển thị thông báo nói rằng để giải mã dữ liệu bạn cần thanh toán một khoản tiền.

Nếu phát hiện các tập tin của bạn bỗng dưng biến mất hoặc bị đổi tên bằng các ký tự ngẫu nhiên, chẳng hạn như "*e9fgbb.ie0r", "52lcvn.ifggh" "d3uhgfds.gre8v*",.... Và tất cả thư mục Documents, Pictues và Desktop có chứa các file HTML và file PNG có các tên ngẫu nhiên như "*HELP_FILE_4BAACA128.PNG", "HELP_FILE_4BAACA128.HTML*",... Rất có thể máy tính của bạn đã bị ransomware Cryptowall tấn công.

1. Virus CryptoWall 4.0 tấn công máy tính người dùng như thế nào?

Virus CryptoWall 4.0 được phân phối thông qua: các trang web độc hại hoặc các trang web bị hack, và nó có thể truy cập máy tính của bạn thông qua việc khai thác bộ kit tấn công (exploit kits) sử dụng các lỗ hổng trên máy tính của bạn để cài đặt Trojan mà bạn không hề hay biết.

Ngoài ra cách thức trên, virus CryptoWall 4.0 còn có thể truy cập máy tính của bạn bằng cách sử dụng các email spam đính kèm hoặc link đến các trang web độc hại. Cyber-criminals là email spam có thông tin tiêu đề giả mạo, lừa người dùng để họ tin rằng nó là email từ công ty DHL hoặc FedEx.

Hoặc khi cài đặt một phần mềm nào đó, người dùng vô hình cài đặt thêm các phần mềm giả mạo mà họ không hề hay biết.

2. Ransomware CryptoWall 4.0 là gì?

Ransomware CryptoWall 4.0 nhắm mục đích tới tất cả các phiên bản Windows, trong đó bao gồm Windows 10, Windows Vista, Windows 8 và Windows 7. Loại Ransomware này sử dụng cách mã hóa các tập tin của người dùng khá đặc biệt, nó sử dụng phương pháp mã hóa AES-265 và RSA để đảm bảo rằng nạn nhân sẽ không có sự lựa chọn nào khác.

Khi ransomware CryptoWall 4.0được cài đặt trên máy tính của bạn, nó sẽ tạo ra các tên thực thi ngẫu nhiên trong thư mục "%AppData" hoặc thư mục "%LocalAppData". Thực thi này khởi chạy và bắt đầu quét tất cả các ổ trên máy tính của bạn để mã hóa các tập tin dữ liệu.

Ransomeware CryptoWall 4.0 sẽ tìm kiếm các tập tin có phần đuôi mở rộng cụ thể để mã hóa. Các tập tin nó mã hóa bao gồm các tài liệu và các tập tin quan trọng như .doc, .docx, .xls, .pdf và một số tập tin khác. Khi các tập tin được phát hiện, nó sẽ thêm phần đuôi mở rộng mới vào tên tập tin (chẳng hạn như 3aweno9f.7gt8 , 0hewendfq.p5r hoặc d2121rg.m4).

Một khi các tập tin đã được mã hóa, người dùng sẽ rất khó có thể nhận biết được các tập tin nào cần phải khôi phục và khôi phục như thế nào.

Dưới đây là danh sách các tập tin mở rộng mà ransomware nhắm đến:

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

Trong quá trình mã hóa các tập tin của bạn, ransomware CryptoWall 4.0 còn tạo ra các file văn bản HELP_YOUR_FILES.TXT
và HELP_YOUR_FILES.HTML trong mỗi thư mục có chứa các tập tin đã bị mã hóa và trên màn hình Desktop Windows. Loại ransomware này cũng thay đổi hình nền màn hình Desktop Windows thành HELP_YOUR_FILES.PNG.

Các tập tin này nằm trong mỗi thư mục có chứa các tập tin đã được mã hóa cũng như trong thư mục Startup, thư mục có chứa các chương trình tự động

hiển thị khi người dùng đăng nhập. Và các tập tin này sẽ chứa các thông tin làm thế nào để truy cập các trang web thanh toán và nhận lại các tập tin của bạn.

Các trang thanh toán tiền bao gồm:
3wzn5p2yiumh7akj.partnersinvestpayto.com,
3wzn5p2yiumh7akj.marketcryptopartners.com,
3wzn5p2yiumh7akj.forkinvestpay.com,
3wzn5p2yiumh7akj.effectwaytopay.com, và 3wzn5p2yiumh7akj.onion.

Your files are encrypted.

To get the key to decrypt files you have to pay **700 USD**. If payment is not made before [redacted] the cost of decrypting files will increase **2** times and will be **1400 USD/EUR**

Prior to increasing the amount left:
[redacted]

Your system: Windows 7 (x64) First connect IP: [redacted]

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

bitcoin

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinmr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.56 BTC to Bitcoin address: 1PoebUjR5pdH88tc9ECQ1PCLaCrtPnG9fm

4. Enter the Transaction ID and select amount:

[ ] 1.56 BTC ~= 700 USD Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **700** USD/EUR.

3. Máy tính của bạn có đang bị virus CryptoWall 4.0 tấn công?

Nếu máy tính của bạn bị ransomware CryptoWall 4.0 tấn công, trên màn hình sẽ hiển thị hình nền HELP_YOUR_FILES.PNG che toàn bộ màn hình Desktop. Và một tập tin văn bản sẽ hiển thị trên màn hình Desktop. Các tập tin này có chứa phần hướng dẫn các nạn nhân cách làm thế nào để khôi phục các tập tin đã bị mã hóa.

Và trên màn hình sẽ hiển thị thông báo kèm theo thông điệp:

Cannot you find the files you need? Is the content of the files that you have watched not readable? It is normal because the files' names, as well as the data in your files have been encrypted. Congratulations!!! You have become a part of large community of CryptoWall . If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption? Encryption is a reversible transformation of information in order to connect it from unauthorised persons but providing at the same time access to it for authorised users. To become an authorised user and make the process truly reversible i.e to be able to decrypt your files you need to have a special private key. In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place. I almost understood but what do I have to do? The first thing you should do is to read the instructions to the end. Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are you helpers. After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions. Think logically – we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them. Any of your attempts to restore you files with the third-party tools can be fatal for encrypted files. The fact that changing data within the encrypted files (as 100% of software to restore files do this, except the special decryption software) you break damage to the files and it will be impossible to decrypt the files. This is the same as to collect a mosaic when some mosaics items were lost, broken or not put in its place – the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly. Use the software to restore files can ruin your files forever, only through your fault. Remember that any intervention of the extraneous software to restore files encrypted with the CryptoWall software may be the point on no return. In case if these simple rules are violated we will not be able to help you, and we will not try because you have been warned. For your attention the software to decrypt the files (as well as the private key that come fitted with it) is a paid product. After purchasing the software package you can: 1.Decrypt all your files. 2. Work with your documents. 3. View your photos and other media content. 4. Continue your habitual and comfortable work at the computer. If you are aware whole importance and criticality of the situation, then we suggest you go directly to

your personal page where you will be given final instructions, as well as guarantees to restore your files.

What do you have to do with these addresses? If you browse the instructions in TXT format (if you have instructions in HTML (the file that has an icon of your Internet browser) then for the sake of simplicity it is better to run it). Additional information: Instructions to restore your files are only in the folders where you have encrypted files. For your convenience the instructions are made in three files formats – html, txt and png. Unfortunately, antivirus companies cannot protect and moreover restore your files but they make things worse removing the instructions to restore encrypted files. The instructions are not malware, they have informative nature only, so any claims on the absence of any instructions files you can send to your antivirus company. CryptoWall Project is not malicious and is not intended to harm a person and his/her information data. This project is conducted for the sole purpose of instruction in the field of information security, as well as certification of antivirus products for their suitability for data protection. Together we make the Internet a better and safer place. If you oversee this text in the Internet and understand that something is wrong with your files and you have no instructions to restore files, contact your antivirus support. Remember that the worst has already happened and now the further life of your files depends directly in your determination and speed of your actions.

4. Làm thế nào để "dọn sạch" ransomware Cryptowall v4.0 trên hệ thống của bạn?

Để "dọn sạch" ransomware Cryptowall v4.0 trên hệ thống của mình, bạn thực hiện theo các bước dưới đây:

Bước 1: Khởi động máy tính ở chế độ Safe Mode with Networking

Bước đầu tiên là khởi động máy tính của bạn ở chế độ Safe Mode with Networking để ngăn virus Cryptowall đang chạy trên hệ thống. Để làm được điều này:

- Trên Windows 7, Vista và Windows XP:

1. Đóng tất cả các chương trình đang mở và **khởi động** lại máy tính của bạn.

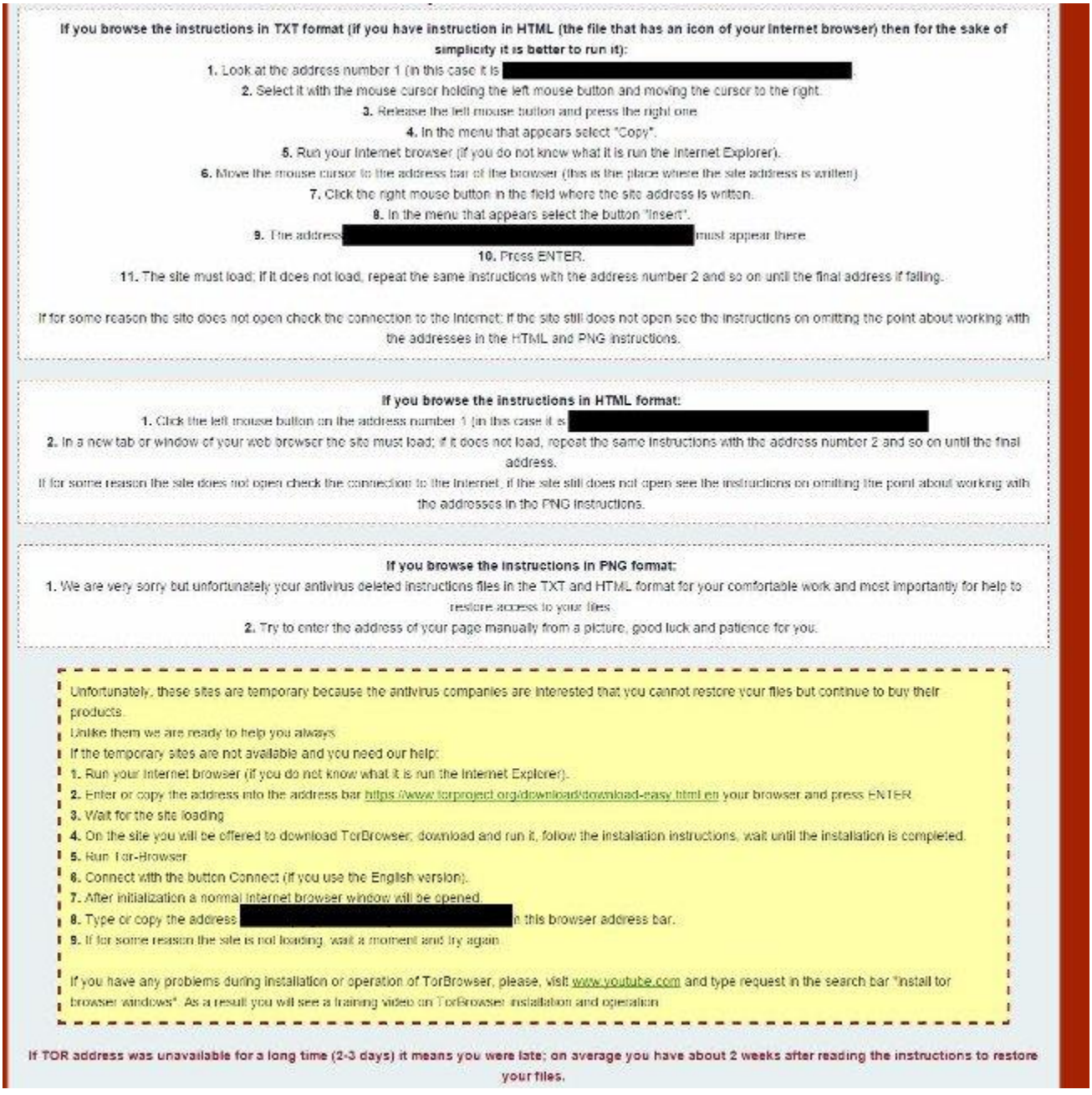
2. Trong quá trình khởi động, nhấn phím **F8** trước khi xuất hiện logo Windows.

3. Lúc này trên màn hình xuất hiện cửa sổ **Windows Advanced Options Menu**, sử dụng phím mũi tên để chọn tùy chọn **Safe Mode with Networking** rồi nhấn **Enter**.

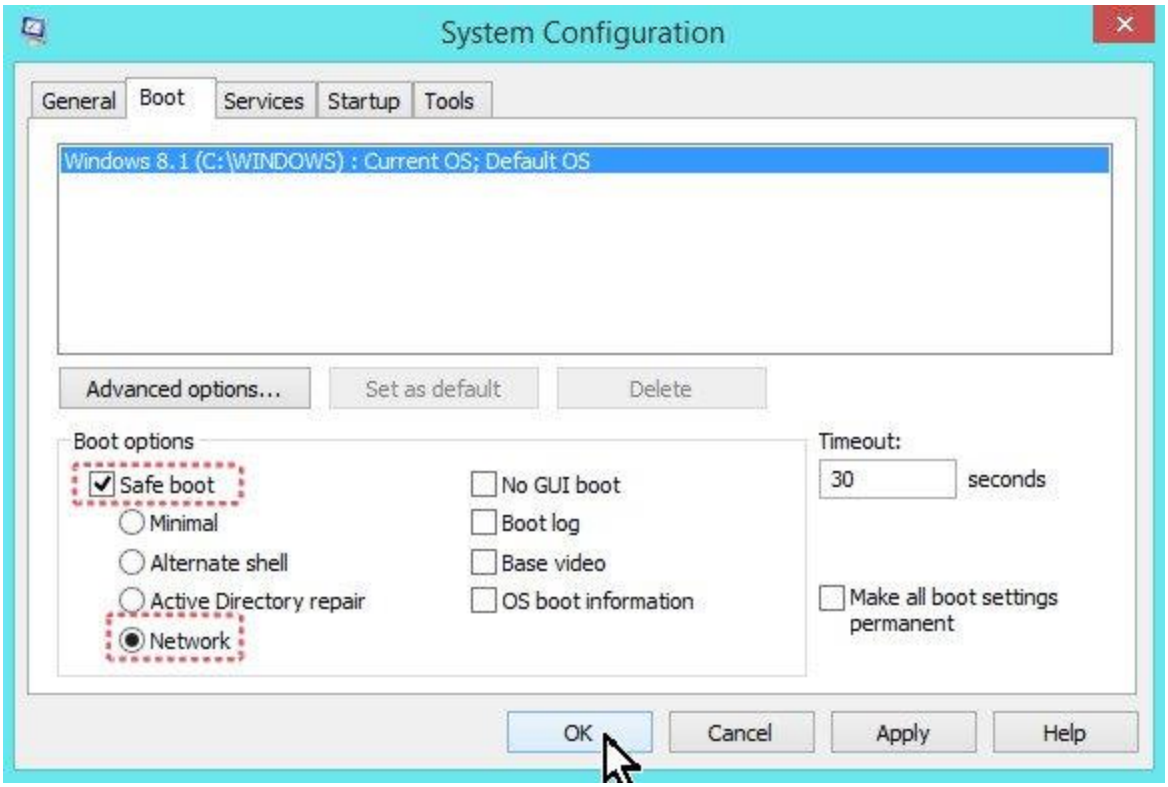
- Trên Windows 8 và Windows 8.1:

1. Nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh **Run**.

2. Trên cửa sổ lệnh Run, bạn nhập **msconfig** vào đó rồi nhấn Enter để mở cửa sổ **System Configuration**.



3. Tại đây bạn click chọn **tab Boot**, sau đó đánh tích chọn **Safe Boot và Network**.



4. Click chọn **OK** rồi khởi động lại máy tính của bạn.

Lưu ý:

Để khởi động máy tính Windows của bạn ở chế độ bình thường (Normal Mode) một lần nữa bạn thực hiện các bước tương tự sau đó bỏ tích mục **Safe Boot** đi là xong.

Bước 2: Tìm và dọn sạch Cryptowall bằng RogueKiller

RogueKiller là một trong những chương trình chống các phần mềm độc hại (malware) hiệu quả. Chương trình có thể phát hiện, ngăn chặn và gỡ bỏ các phần mềm độc hại (malware) nói chung và cả rootkits, rogues, worms,...

1. Tải RogueKiller về máy và cài đặt.

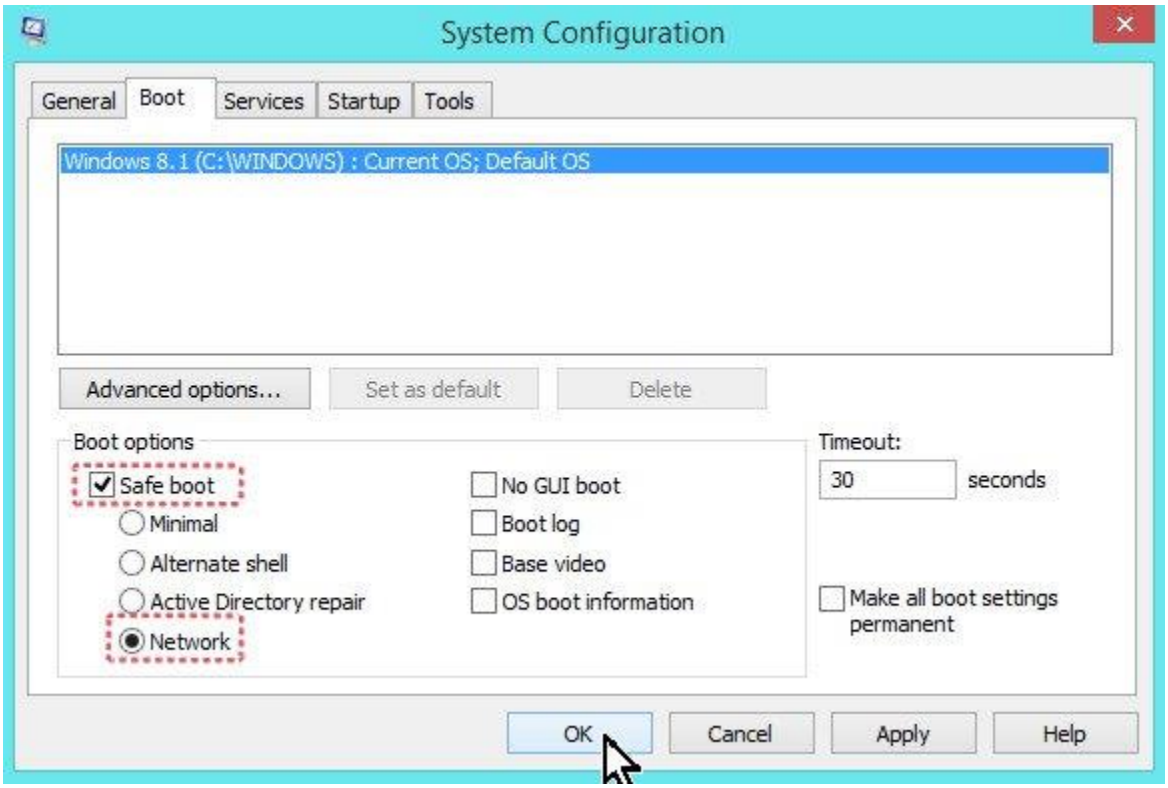
Lưu ý:

Tải phiên bản x86 hoặc x64 phù hợp với phiên bản hệ điều hành của bạn. Muốn biết phiên bản hệ điều hành bạn đang sử dụng, kích chuột phải vào biểu tượng Computer, chọn Properties và tìm kiếm tại mục System Type.

2. Kích đúp chuột để chạy **RogueKiller**.

3. Click chọn **Accept** để đồng ý với các điều khoản, cài đặt chương trình.

4. Bước tiếp theo là click chọn **Scan** để quét các phần mềm độc hại trên máy tính và trên cổng **startup**.



5. Chờ cho đến khi quá trình quét hoàn tất, click chọn thẻ **Registry**, chọn tất cả các mục chứa các phần mềm độc hại được tìm thấy rồi click chọn **Delete** để loại bỏ tất cả các mục này đi.

6. Đóng RogueKiller lại và thực hiện các bước tiếp theo.

Bước 3: Sử dụng MalwareBytes Anti-Malware để loại bỏ malware Cryptowall

Tải Malwarebytes Anti-Malware Premium về máy và cài đặt.

Lưu ý:

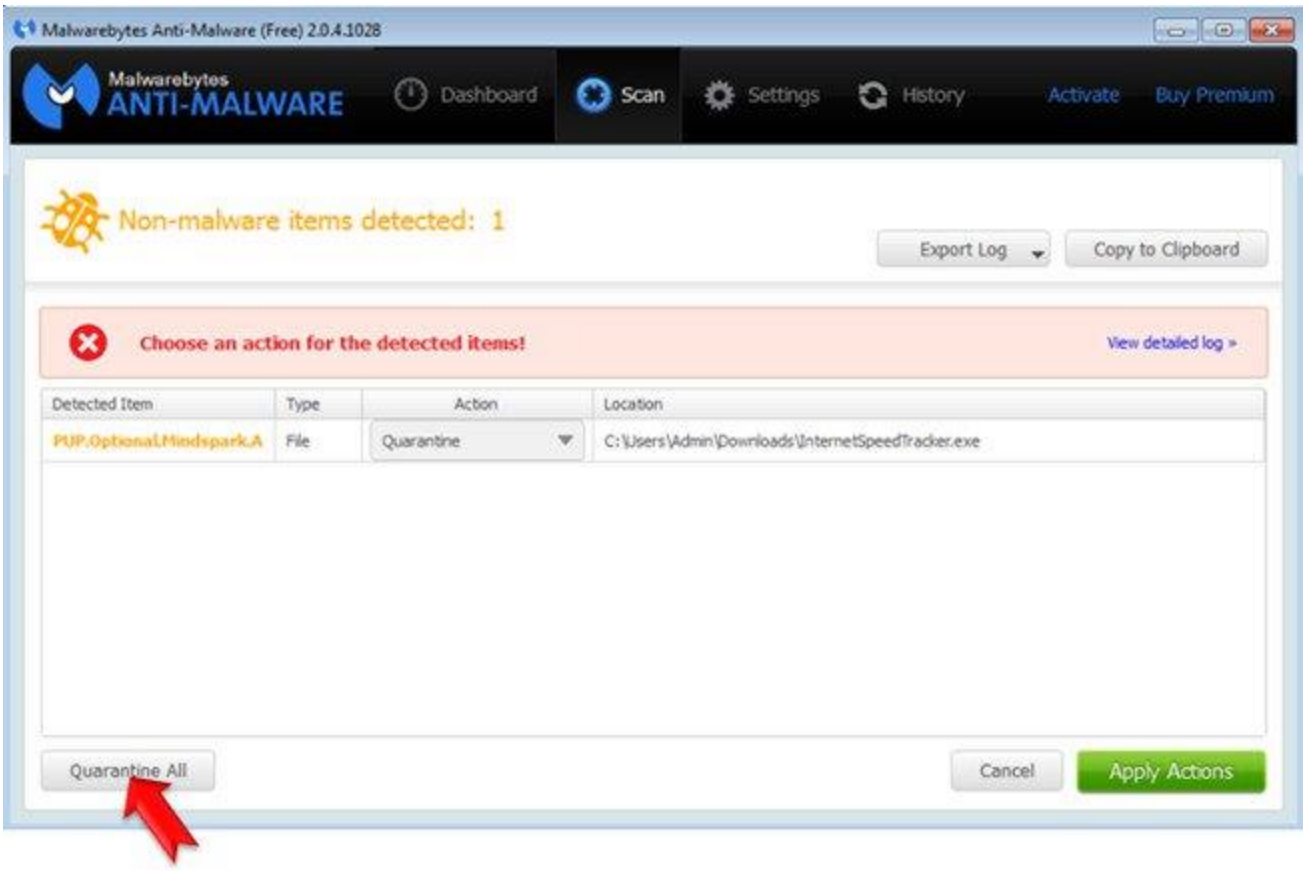
Trên cửa sổ cài đặt cuối cùng, bỏ tích mục Enable free Trial of Malwarebytes Anti-Malware PRO để sử dụng phiên bản MalwareBytes Anti-Malware miễn phí.

Quét và làm sạch máy tính của ban với Malwarebytes Anti-Malware:

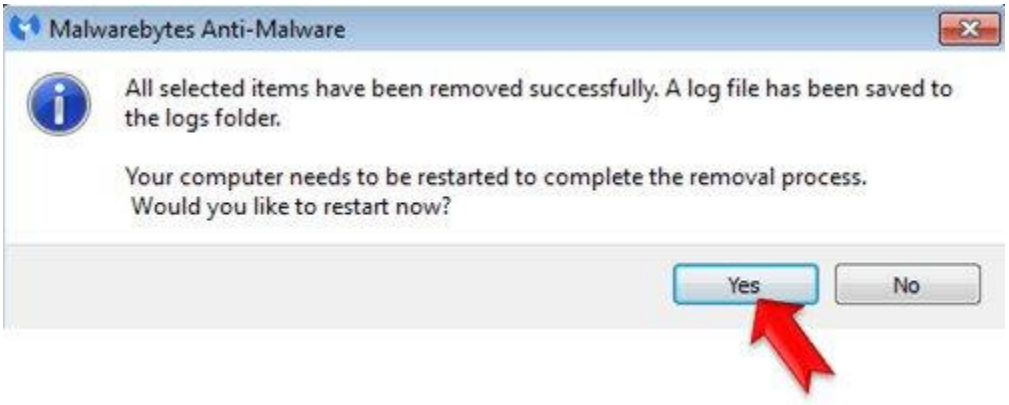
1. Chạy **Malwarebytes Anti-Malware** và cho phép chương trình update (cập nhật) phiên bản mới nhất (nếu cần).

2. Sau khi quá trình cập nhật kết thúc, click chọn nút **Scan Now** để bắt đầu quá trình quét hệ thống của bạn, loại bỏ **malware** và các chương trình không mong muốn.

3. Chờ cho đến khi quá trình quét hệ thống kết thúc. Khi quá trình quét hoàn tất, click chọn **Quarantine All** để loại bỏ các mối nguy hại được tìm thấy.



4. Sau khi quá trình kết thúc, tiến hành khởi động lại máy tính của bạn để hoàn tất quá trình.



Bước 4: Quét hệ thống bằng Eset Online Scanner

1. Chạy Eset Online Scanner. Nếu bạn sử dụng trình duyệt khác chứ không phải trình duyệt Internet Explorer, click chọn Eset Smart Installer để tải chương trình về máy và cài đặt.

2. Chấp nhận các điều khoản rồi click chọn **Start**.

3. Chờ ESET Online Scanner tải các "thành phần" cần thiết, sau đó tiến hành:

- Đánh tích chọn Enable detection of potentially unwanted applications.
- Đánh tích chọn tất cả các tùy chọn tại mục “advanced settings”.
- Click chọn nút Start để quét và loại bỏ virus cũng như các chương trình độc hại trên máy tính của bạn.

4. Chờ cho đến khi ESET online scanner loại bỏ tất cả các mối nguy hại mà công cụ phát hiện trên hệ thống của bạn.