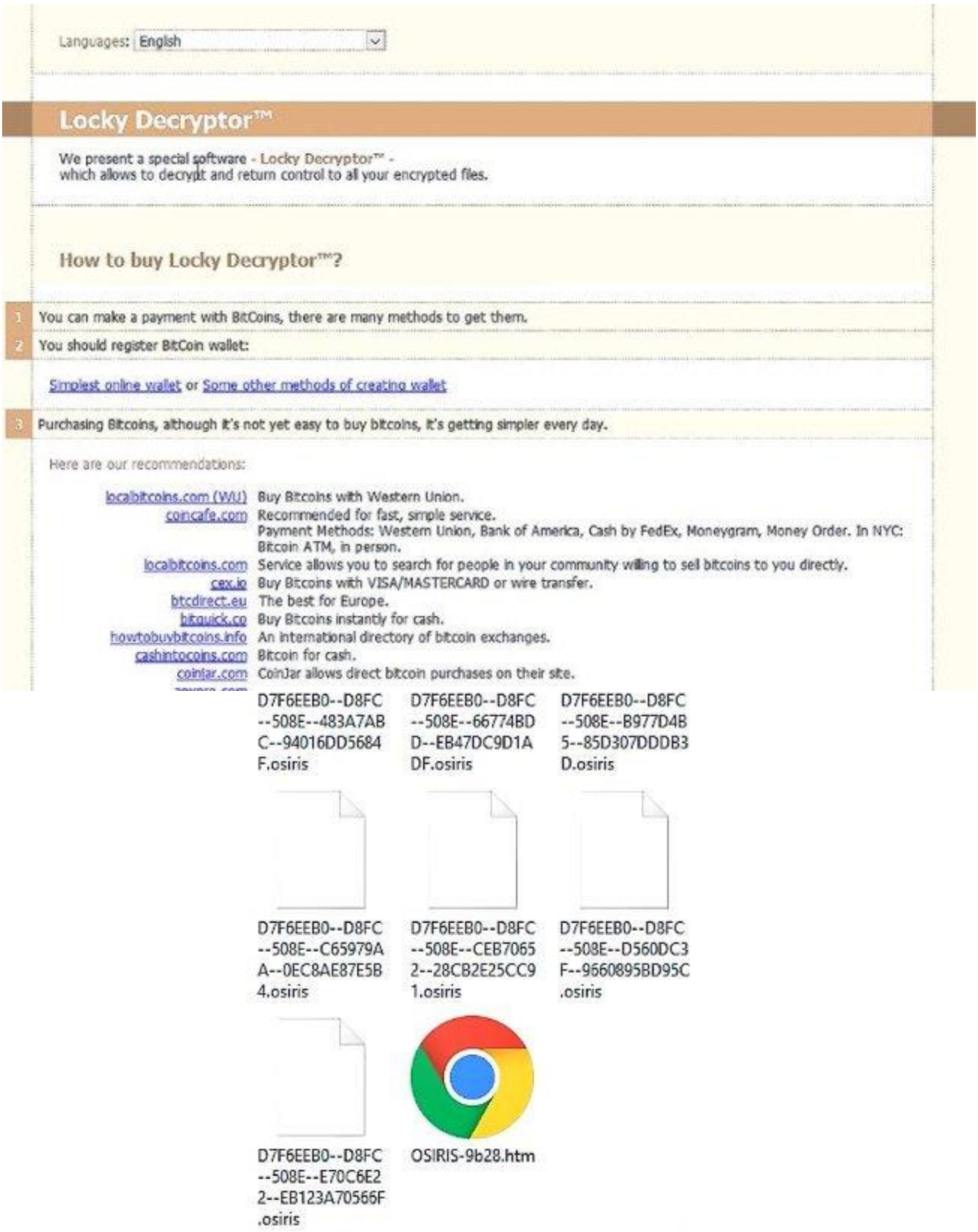
Làm thế nào để loại bỏ tận gốc virus *.OSIRIS - Ransomware Locky ?

Nếu mở bất kỳ một tài liệu cá nhân nào đó và bạn thấy tài liệu đó có phần đuôi mở rộng là **[8_random_characters]-[4_random_characters]-[4_random_characters]-[8_random_characters]-[12_random_characters].osiris**. Rất có thể máy tính của bạn đã bị ransomware Locky rấn công.

Locky là ransomware mã hóa tập tin, nó sẽ mã hóa các tài liệu cá nhân mà nó phát hiện trên máy tính của các "nạn nhân" bị nó tấn công, 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 khoảng 2,5 Bitcoins, hoặc xấp xỉ khoảng 1880$.

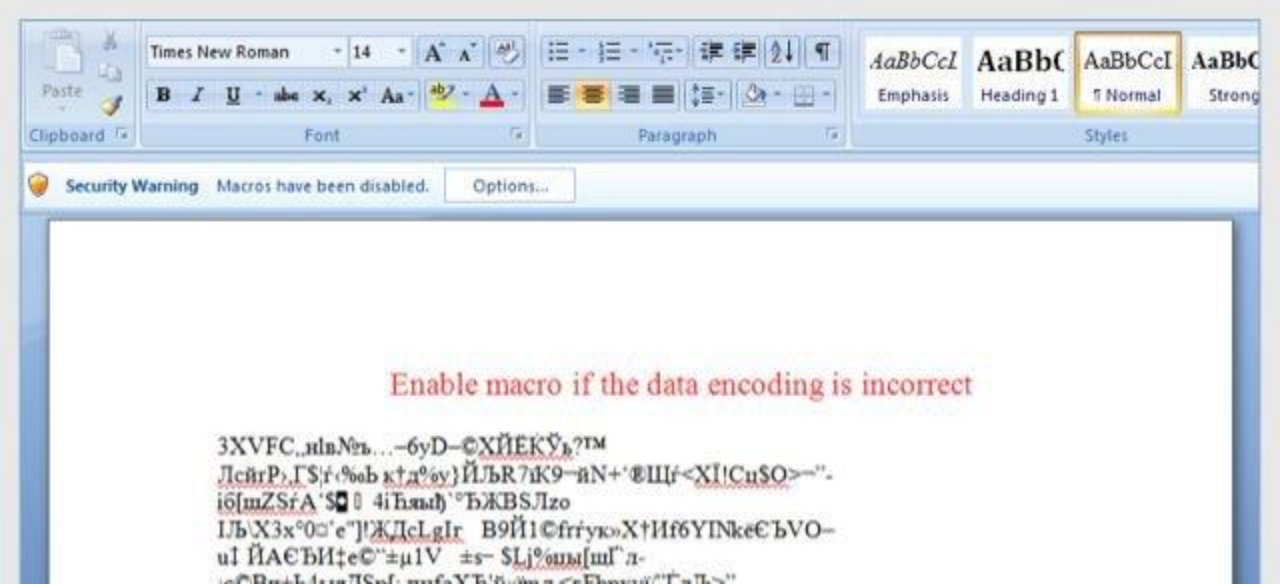
Các hướng dẫn được "gói trọn" trên máy tính các nạn nhân trong 3 file: **OSIRIS.html, OSIRIS_ [4_digit_number] .html,** và **OSIRIS.bmp.**



1. Ransomware Locky OSIRIS tấn công máy tính của bạn như thế nào?

Ransomware Locky được “phân phối” thông qua các thư rác có chứa các file 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. OSIRIS – ransomware Locky là gì?

Locky ransomware 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.

Khi ransomware Locky được 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 Lock 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 (ezz, .exx, .7z.encrypted).

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

Sau khi các tập tin được mã hóa bằng đuôi mở rộng .osiris, ransomeware Locky có thể tạo một tập tin **OSIRIS.html, OSIRIS_[4_digit_number].html**, hoặc **OSIRIS.bmp files**cho mỗi thư mục có tập tin đã được mã hóa và trên máy tính Windows.

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. 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.

Trong hầu hết các trường hợp, ransomeware Locky sẽ chiếm quyền điều khiển phần đuôi mở rộng .EXE, khi bạn khởi động một thực thi nó sẽ cố gắng xóa Shadow Volume Copies trên máy tính.

Sau khi hoàn tất việc mã hóa các tập tin dữ liệu, nó sẽ xóa tất cả Shadow Volume Copies trên máy tính của bạn. Nó không cho phép người dùng sử dụng Shadow Volume Copies để khôi phục (restore) các tập tin đã bị mã hóa.

3. Máy tính của bạn có bị ransomware Locky - OSIRIS tấn công?

Khi ransomeware Lock tấn công máy tính của bạn, nó sẽ quét tất cả các ổ trên hệ thống để tìm các tập tin mà nó nhắm đích đến, mã hóa các tập tin đó và thêm phần đuôi mở rộng .osiris vào các tập tin.

Sau khi các tập tin đã được mã hóa, bạn không thể mở các tập tin này bằng các chương trình như bình thường mà bạn vẫn mở nữa. Ngoài ra khi ransomware Locky kết thúc quá trình mã hóa các tập tin của nạn nhân, nó cũng sẽ làm thay đổi hình nền trên máy tính của nạn nhân.

Ngoài ra nó cũng sẽ hiển thị một ghi chú khoản tiền chuộc dưới dạng HTML trên trình duyệt mặc định của bạn. Những ghi chú này bao gồm cách hướng dẫn làm thế nào để kết nối với các dịch vụ Decrypt Service, nơi bạn có thể tìm hiểu thêm về những gì đã xảy ra với các tập tin của mình và làm thế nào để thanh toán.

Ransomware Locky sẽ hiển thị thông báo:

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:

hxxps://en.wikipedia.org/wiki/RSA_(cryptosystem)

hxxps://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:

[edited]

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser:
hxxps://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: [edited]

4. Follow the instructions on the site.

!!! Your personal identification ID: [edited]

4. Liệu có thể giải mã các tập tin đã được mã hóa bởi ransomware Locky hay không?

Tính cho đến thời điểm này thì không thể khôi phục các tập tin được mã hóa bởi phần đuôi mở rộng .osiris.

Điểm đáng chú ý nhất của ransomware Locky là cách mà nó mã hóa các tập tin của người dùng. Cụ thể là, nó sử dụng phương pháp mã hóa AES-265 và RSA - để đảm bảo rằng người dùng bị "tấn công" không có sự lựa chọn nào khác ngoài việc mua key private.

Key RSA public có thể được giải mã với key private tương ứng của nó. Lí do bởi vì key AES bị ẩn khi sử dụng mã hóa RSA và key RSA private không có sẵn, việc giải mã các tập tin là không khả thi.

Và bởi vì phải có key private để mở khóa các tập tin mã hóa, mà các key này có sẵn thông qua tội phạm mạng (cyber criminal), do đó các "nạn nhân" có thể bị "dụ" để mua và trả một khoản phí cắt cổ.

4.1. Sử dụng phần mềm để khôi phục các tập tin bị mã hóa bởi ransomware Locky

Tùy chọn 1: Sử dụng ShadowExplorer để khôi phục các tập tin bị mã hóa bởi ransomware Locky

1. Tải **ShadowExplorer** về máy và cài đặt.

2. Sau khi tải và cài đặt xong ShadowExplorer, bạn có thể tham khảo các bước hướng dẫn để restore các tập tin bằng ShadowExplorer trong video dưới đây:

Tùy chọn 2. Sử dụng phần mềm khôi phục tập tin để khôi phục các tập tin bị mã hóa bởi phần mở rộng .osiris

Khi phần mở rộng .osiris mã hóa một tập tin bất kỳ nào đó, bước đầu tiên nó sẽ sao chép tập tin đó, mã hóa tập tin mà nó sao chép và xóa tập tin gốc đi. Do đó để khắc phục các tin đã bị mã hóa bởi phần mở rộng .osiris , bạn có thể sử dụng phần mềm khôi phục tập tin như:

- Recuva:

Tham khảo các bước khôi phục tập tin bị mã hóa bằng Recuva trong video dưới đây:

- EaseUS Data Recovery Wizard Free:

- R-Studio:

5. Làm thế nào để gỡ bỏ đuôi mở rộng .osiris?

Bước 1: Sử dụng Malwarebytes Anti-Malware Free để gỡ bỏ virus "Your personal files are encrypted"

Malwarebytes Anti-Malware Free là phần mềm miễn phí hỗ trợ việc phát hiện và loại bỏ dấu vết của các phần mềm độc hại (malware) bao gồm worms, trojans, rootkits, rogues, dialers, spyware (phần mềm gián điệp), và một số phần mềm khác.

Điều quan trọng là Malwarebytes Anti-Malware chạy song song với các phần mềm diệt virus khác mà không bị xung đột.

1. Tải Malwarebytes Anti-Malware Free về máy và cài đặt.

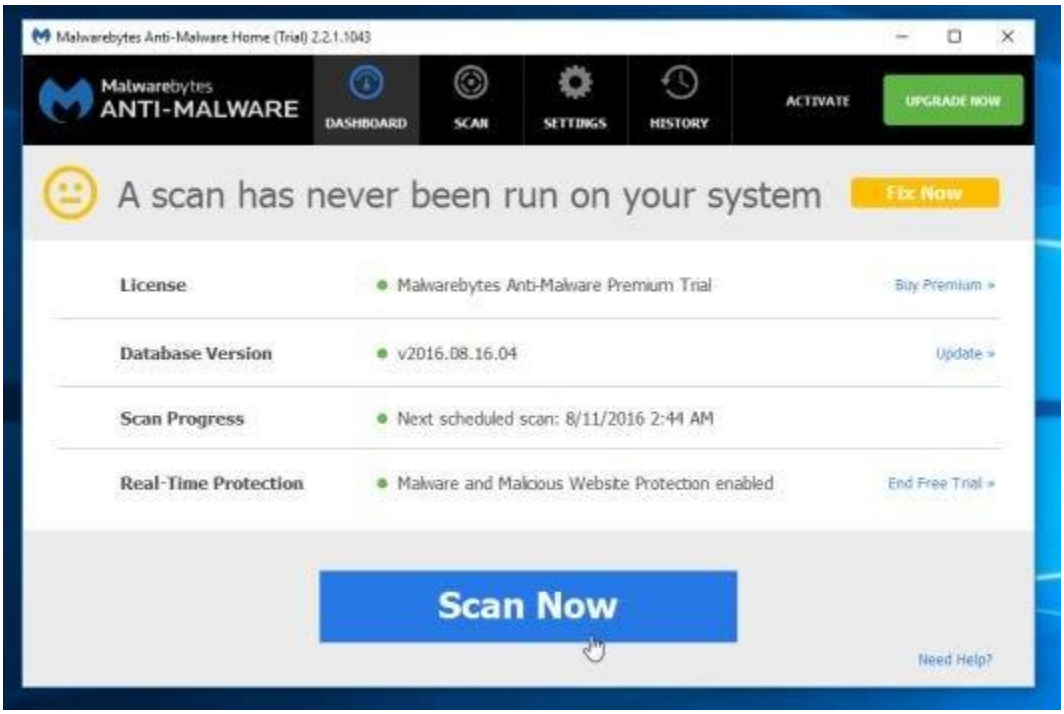
2. Sau khi tải xong, đóng tất cả các chương trình lại, sau đó kích đúp vào biểu tượng có tên **mbam-setup** để bắt đầu quá trình cài đặt Malwarebytes Anti-Malware.

Lúc này trên màn hình sẽ xuất hiện hộp thoại **User Account Control** hỏi bạn có muốn chạy file hay không. Click chọn **Yes** để tiếp tục.

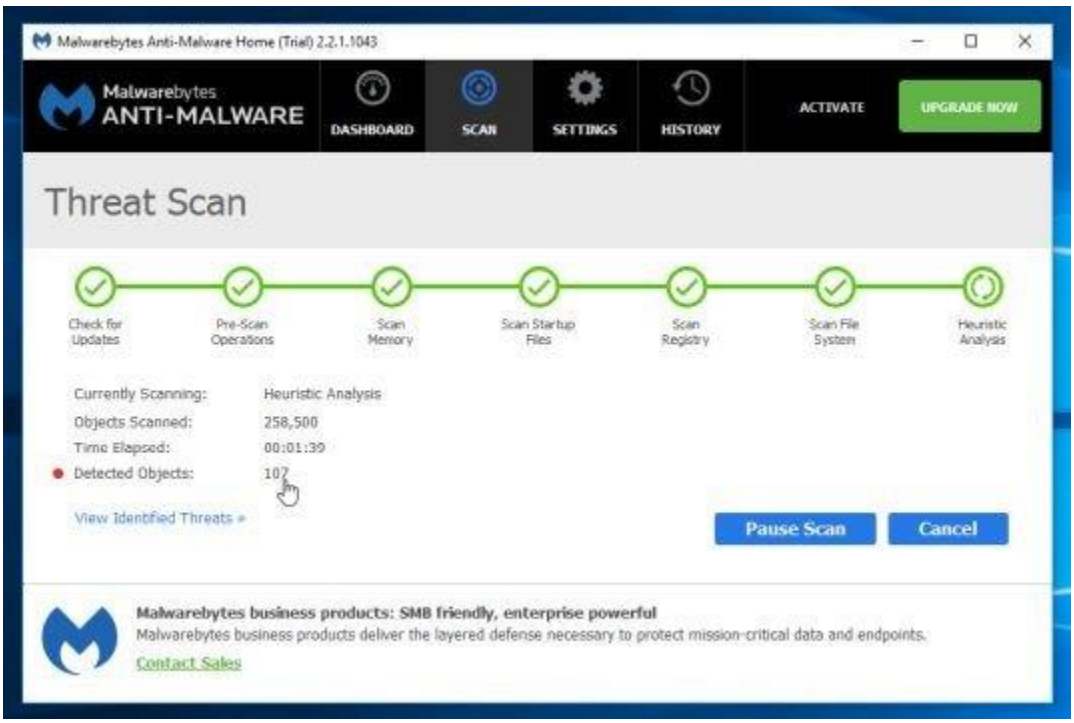
3. Khi bắt đầu quá trình cài đặt, trên màn hình hiển thị cửa sổ Malwarebytes Anti-Malware Setup Wizard, thực hiện theo các bước hướng dẫn trên màn hình để cài đặt Malwarebytes Anti-Malware.

Để cài đặt Malwarebytes Anti-Malware, click chọn nút **Next** cho đến khi xuất hiện của sổ cuối cùng bạn click chọn **Finish.**

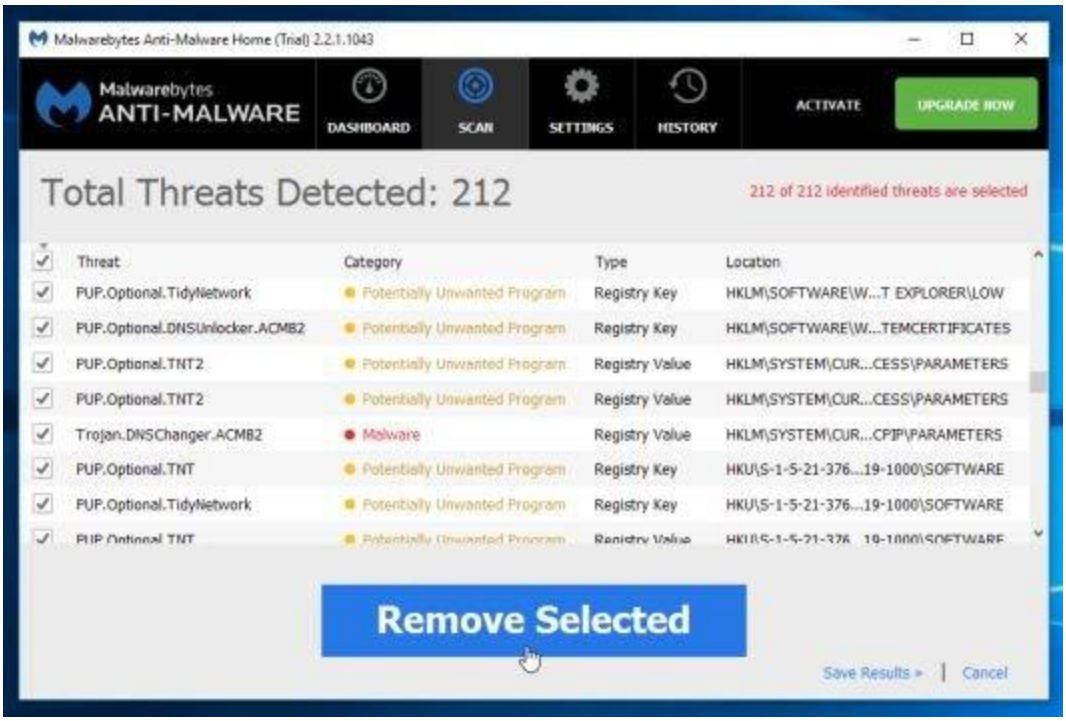
4. Sau khi cài đặt xong, Malwarebytes Anti-Malware sẽ tự động mở. Để bắt đầu quá trình quét hệ thống, bạn click chọn nút **Scan Now.**



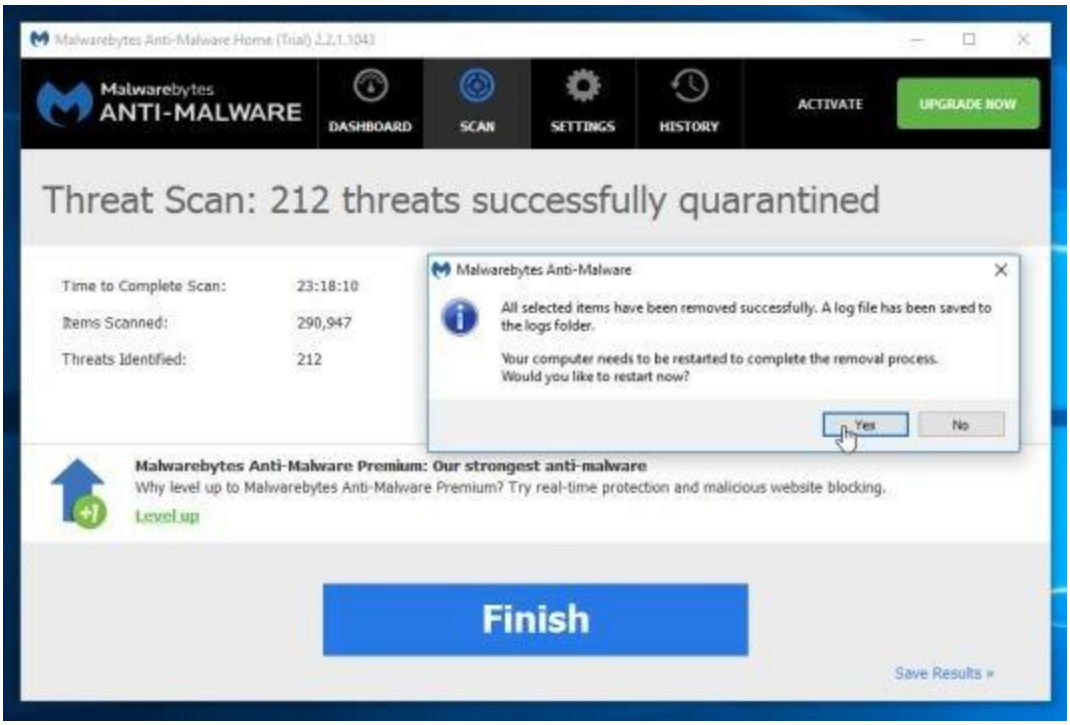
5. Malwarebytes Anti-Malware sẽ bắt đầu quá trình quét máy tính của bạn để tìm và loại bỏ phần mềm độc hại .osiris.



6. Sau khi quá trình kết thúc trên màn hình sẽ xuất hiện cửa sổ hiển thị các phần mềm độc hại (malware) mà Malwarebytes Anti-Malware phát hiện được. Để loại bỏ các phần mềm, chương trình độc hại mà Malwarebytes Anti-Malware phát hiện ra, click chọn nút **Remove Seletected**.



7. Malwarebytes Anti-Malware sẽ "*cách ly*" tất cả các tập tin độc hại và key registry mà chương trình phát hiện. Trong quá trình loại bỏ các tập tin này, Malwarebytes Anti-Malware có thể yêu cầu bạn khởi động lại máy tình để hoàn tất quá trình. Nhiệm vụ của bạn là khởi động lại máy tính của mình để hoàn tất quá trình.



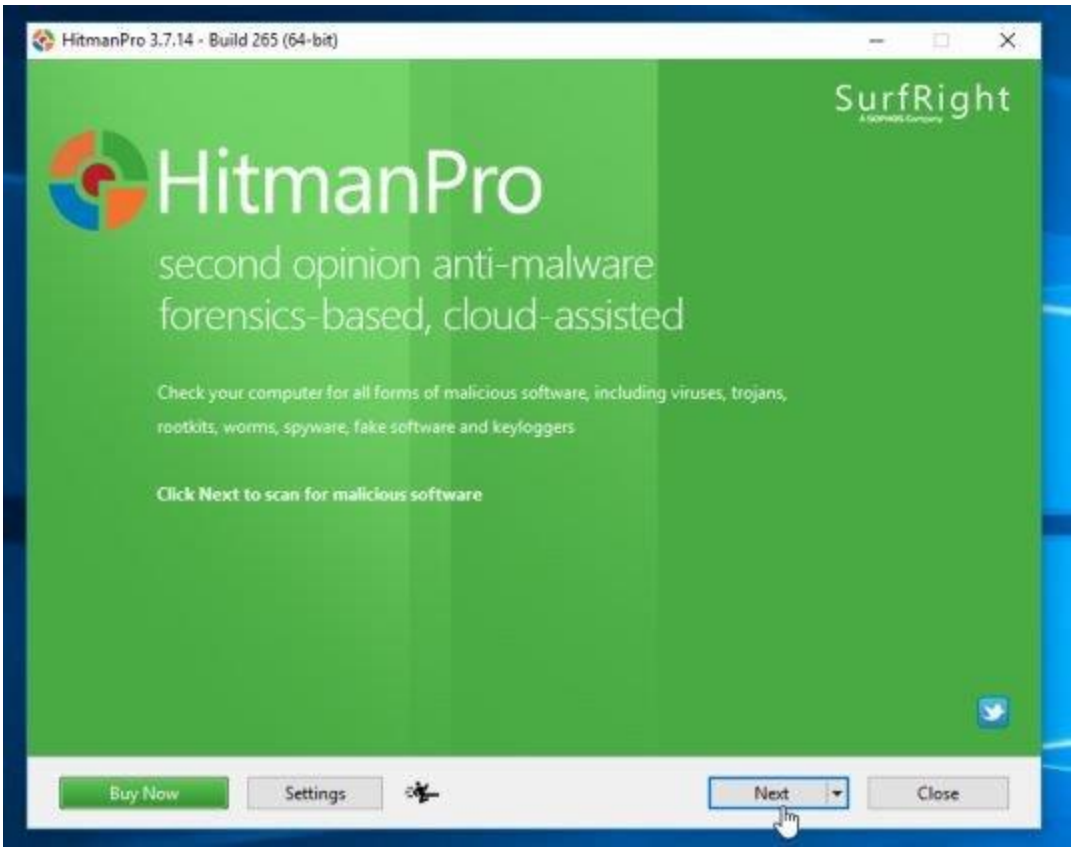
Bước 2: Sử dụng HitmanPro để loại bỏ ransomware Locky

HitmanPro được thiết kế để "*giải cứu*" máy tính của bạn khỏi các phần mềm độc hại như virus, trojans, rootkits, ...) xâm nhập trái phép vào hệ thống. HitmanPro được thiết kế để hoạt động song song với các phần mềm bảo mật khác mà không gây ra lỗi xung đột. Chương trình sẽ quét máy tính của bạn trong vòng 5 phút và sẽ không làm chậm máy tính của bạn.

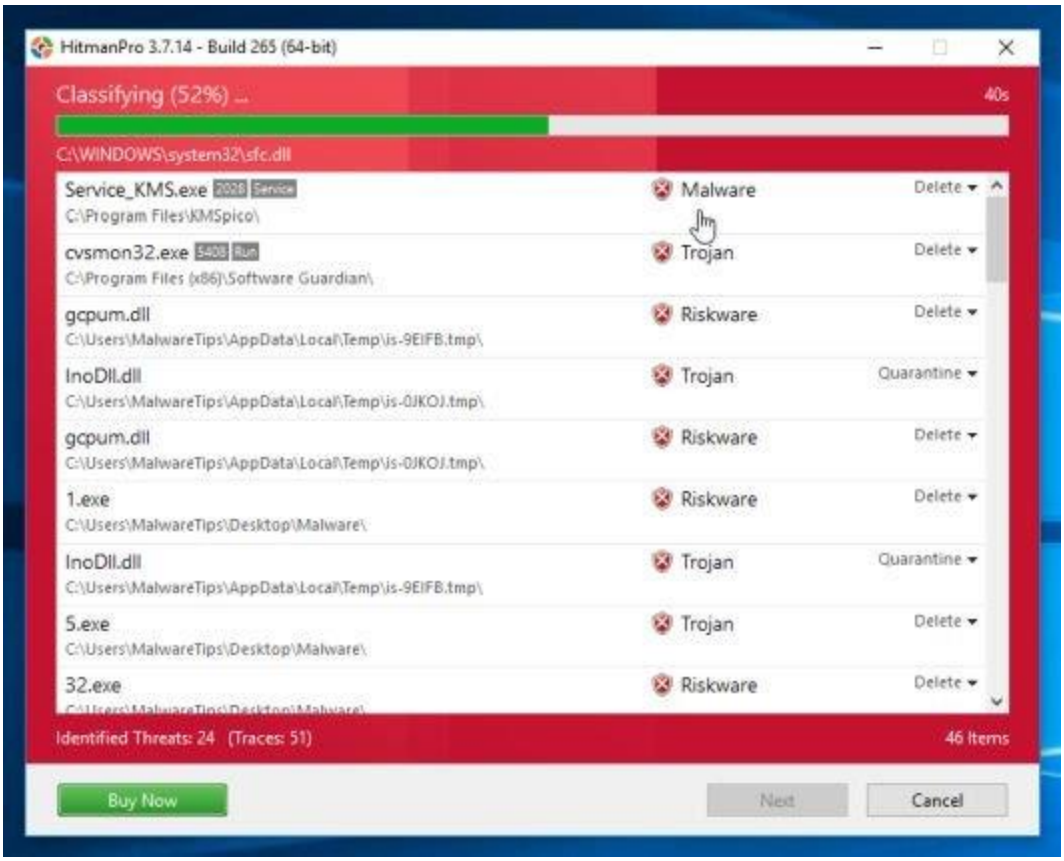
1. Tải HtmanPro về máy và cài đặt.

2. Kích đúp chuột vào file có tên "*HitmanPro.exe*" (nếu sử dụng Windows phiên bản 32-bit) hoặc "*HitmanPro_x64.exe*" (nếu sử dụng Windows phiên bản 64-bit).

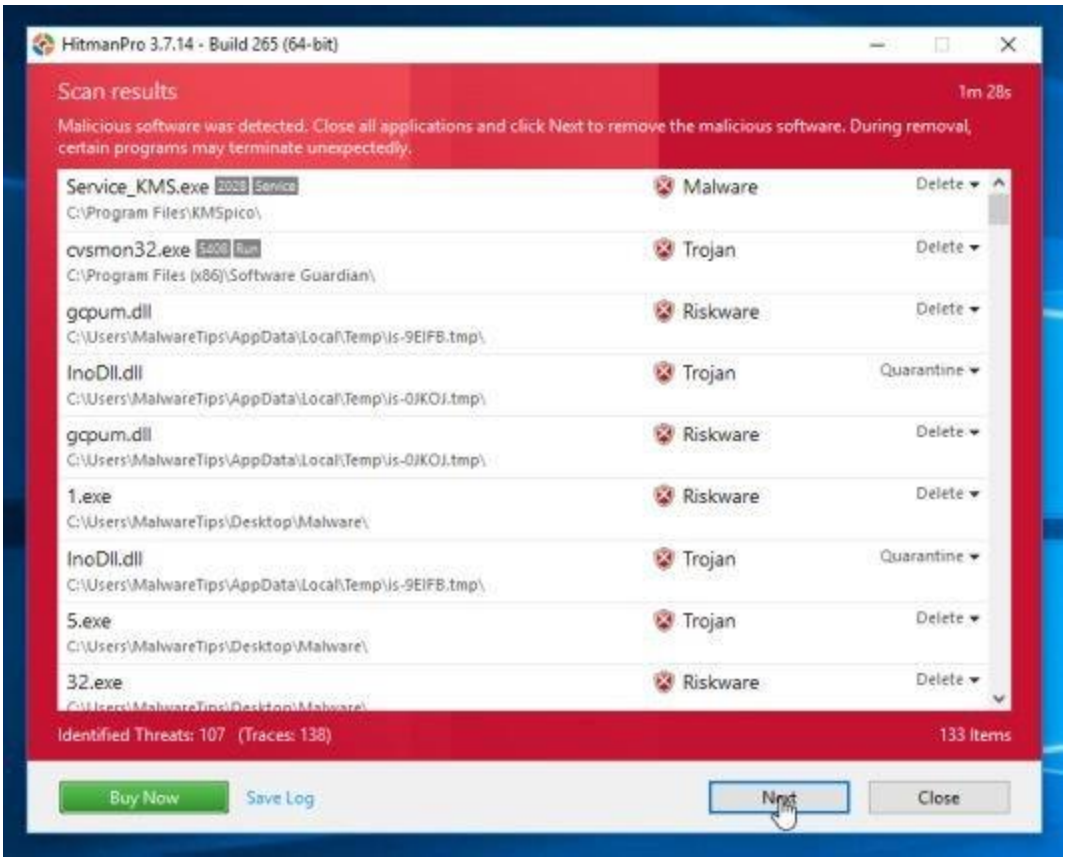
Click chọn **Next** để cà đặt HitmanPro trên máy tính của bạn.



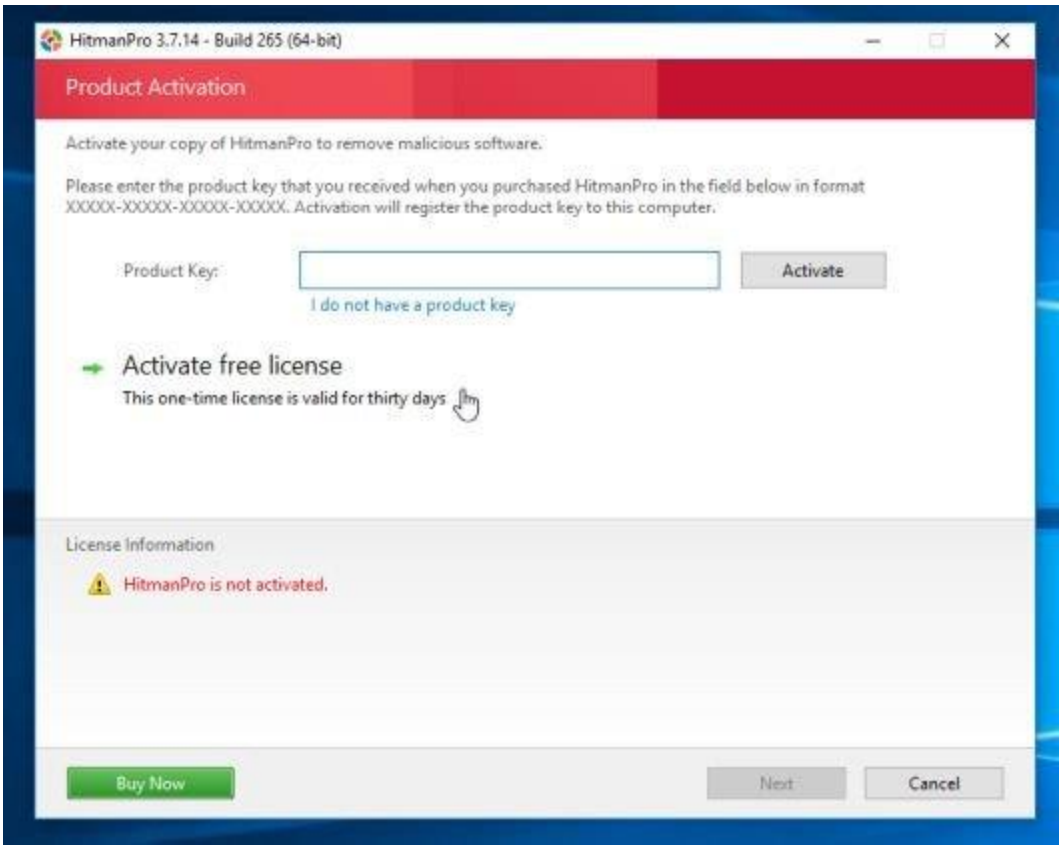
3. HitmanPro sẽ bắt đầu quá trình quét máy tính của bạn để tìm và loại bỏ các tập tin độc hại.



4. Sau khi quá trình kết thúc trên màn hình sẽ hiển thị cửa sổ có chứa danh sách tất cả các chương trình độc hại mà HitmanPro tìm thấy. Click chọn **Next** để loại bỏ phần mềm độc hại trên hệ thống của bạn.



5. Click chọn nút **Activate free license** để dùng thử chương trình miễn phí trong vòng 30 ngày và để loại bỏ tất cả các tập tin độc hại khỏi máy tính của bạn.



6. Làm thế nào để bảo vệ máy tính của bạn khỏi ransomeware Locky ?

Để bảo vệ máy tính của bạn khỏi ransomeware Locky, tốt nhất bạn nên cài đặt các **chương trình diệt virus** trên máy tính và thường xuyên sao lưu các dữ liệu cá nhân của mình. Ngoài ra bạn có thể sử dụng một số chương trình như HitmanPro.Alert để ngăn chặn các chương trình, phần mềm độc hại (malware) mã hóa các tập tin trên hệ thống.