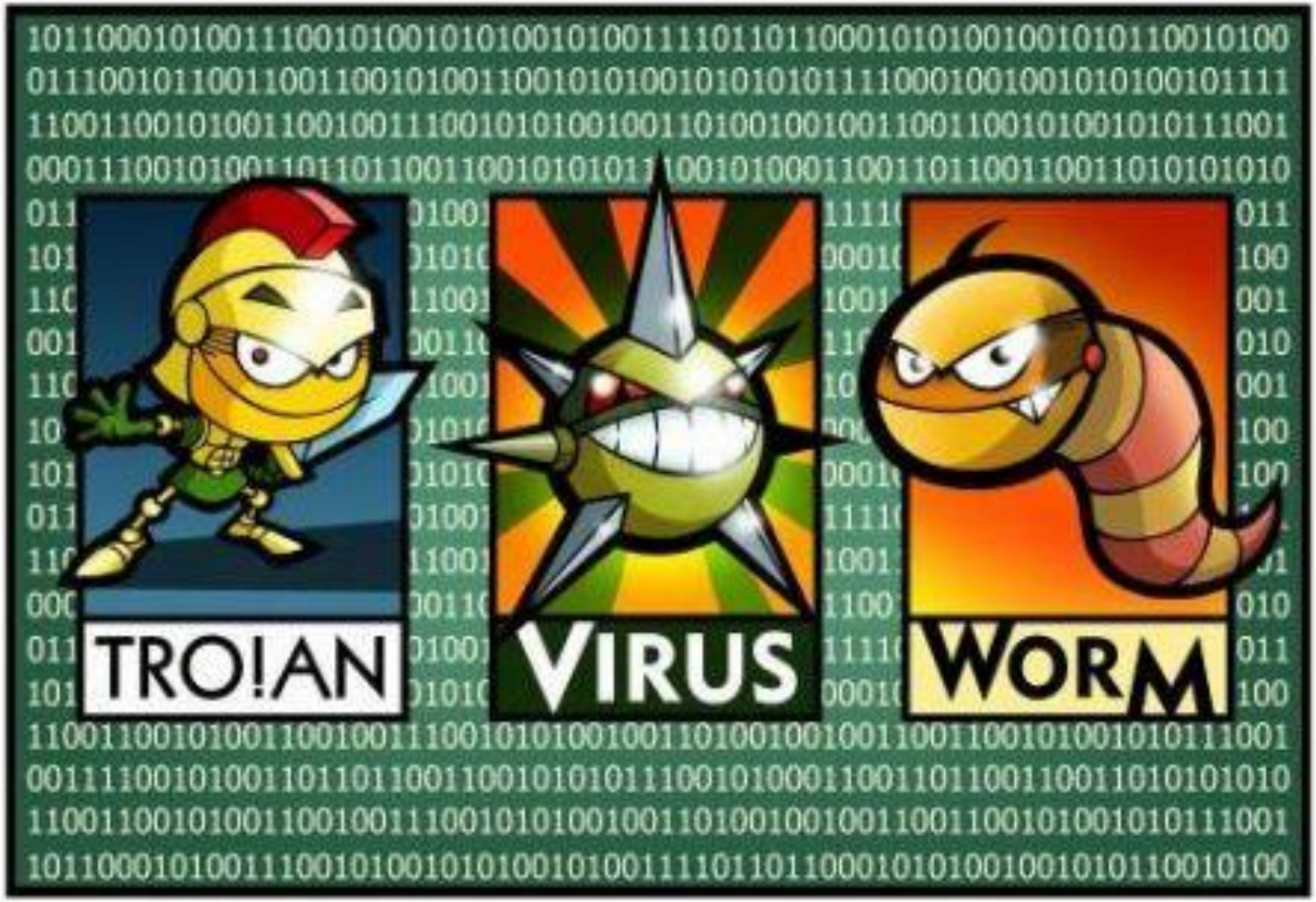
Viruși,viermi și troiani

Au colaborat:Croitori Nicoleta și Senic Ecaterina


TRO!AN
VIRUS
WORM

Ce au fiecare în comun?

Caracteristici:

- Aceștia afectează sistemul de securitate a calculatorului,cauzând activități malițoase pentru acesta.
- Toate 3 se folosesc pentru a fura date personale și informații secrete;
- Pot permite accesul de la distanță neautorizat la un calculator compromis;
- După infiltrare aceștia tind să se ascundă.

Moduri de infiltrare în calculator

- Toți se raspândesc prin e-mail,rețelelor de răspândire fișiere,chat-uri(Aceştia pot veni ca şi ataşamente utile, mesaje instante, link-uri în emal);
- Ei infectează un calculator vulnerabil pe internet, exploatând sistemul de operare ştiut şi vulnerabilitățile programului de securitate instalat.

Viermii

Ce face un vierme în calculatorul meu?

- Utilizarea unui sistem compromis pentru a se răspândi prin email, rețele de răspândire fișiere, instant messenger, chat-uri online sau rețele deschise.

- Infectarea fișierelor, coruperea aplicațiilor instalate, și avarierea întregului sistem.

- Furtul sau dezvăluirea de informații personale sensibile, documente valoroase, parole, nume de autentificare, detalii despre identitate, și contactele utilizatorului.

- Instalarea unui backdoor sau lăsarea unor alți paraziți periculoși.

- Modificarea setărilor de sistem esențiale pentru a scade securitatea generală a sistemului, pentru a-l face mai vulnerabil.

- Să degradeze sever viteza de conectare la internet și performanța generală a sistemului, cauzând instabilitatea software-urilor. Unii paraziți sunt prost programați; risipesc prea multe resurse ale calculatorului și intră în conflict cu aplicațiile instalate.

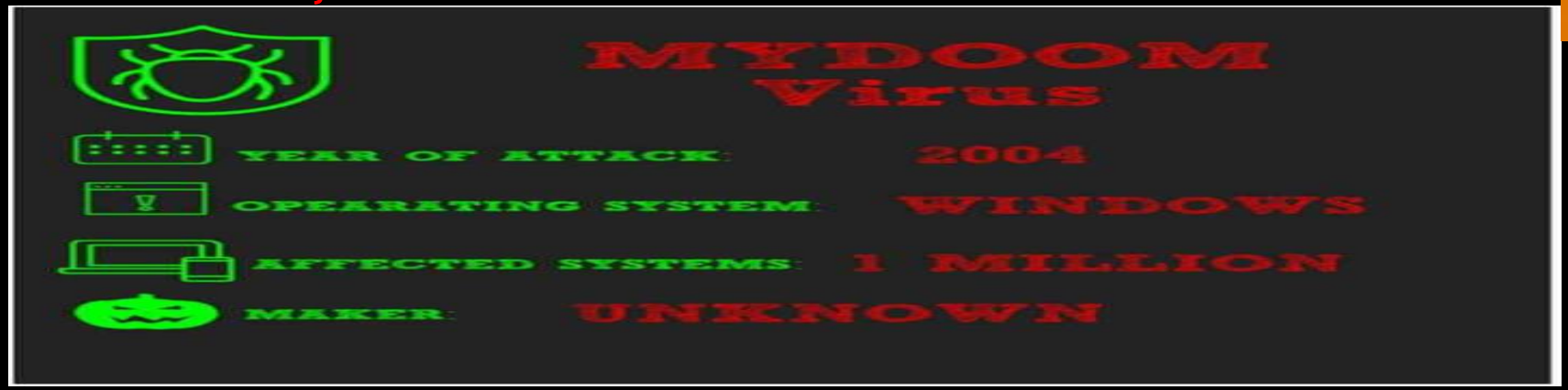
- Nu oferă funcție de dezinstalare, își ascunde procesele, fișierele, și alte obiecte pentru a-și complica eliminarea cât mai mult posibil.

Cele mai periculoase exemple de viermi:

- IIOVE YOU

The Iglamer

MyDoom



VIRUS!

- Atunci când un program malițios se va infiltra în sistem, va iniția următoarele activități:
- Va infecta, suprascrie sau şterge fişierele. Poate dăuna documentelor personale, componentelor esențiale din sistem şi aplicațiilor utile. De asemenea, unii viruşi pot distruge întregul sistem prin ştergerea tuturor fişierelor şi dosarelor critice din acesta.
- Poate introduce un cod malițios în registrul master boot (MBR) a unui hard disk pentru a rula o sarcină utilă distructivă înainte ca sistemul de operare să fie încărcat.
- Poate adăuga componente dăunătoare programelor reputabile sau le poate modifica setările astfel încât să infecteze documentele deschise sau create cu aceste programe.
- Poate dăuna sever unui calculator modificând setările esențiale de hardware, ştergând memoria CMOS sau coruptând BIOS-ul. Acest lucru poate conduce la pierderi critice de date şi funcționarea eronată a sistemului de calculator.
- Poate crea mii de fişiere şi dosare la întâmplare care pot consuma foarte mult din resursele calculatorului.
- Poate afişa numeroase mesaje false, să modifice diverse setări de sistem, să cauzeze redirecționări şi să efectueze alte acțiuni enervante pentru a complica sarcinile normale ale utilizatorului.
- Poate infecta sistemul cu troiani, backdoors, keyloggeri şi alți paraziți periculoşi.
- Foloseşte un sistem compromis pentru a răspândi alți malware.
- Fură sau criptează date personale sensitive, documente valoroase, parole, nume de autentificare, detalii despre identitate sau contactele utilizatorului.
- Evită eliminarea prin auto modificare, criptează fişierele infectate, interceptează cereri ale software-ului antivirus şi aduce modificări comportamentului normal de sistem.

er

ew encrypted files

ntill costs raise

:57:21

btc

btc

yment and receive keys

IV

ecrypt using keys

014 3:33:06 PM

30gb of personal documents and files on this computer or device have just been encr
Encypted means you will not be able to access your files anymore, until they are decr
Your original files have been deleted, these can be recovered as described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-128).
The only way to decrypt your files, is to obtain your private key and IV.

The private key, which will allow you to decrypt and get your original files back,
is stored on our server. Each time the timer hits zero, the total costs will raise with th
price.

To receive your private key, you need to pay the amount of bitcoin displayed left of thi
(costs).
You need to send the amount of bitcoins to the bitcoin address at the bottom of this v

After the purchase is made, please wait a few minutes for confirmation of the bitcoins
After the bitcoins are confirmed, click the 'check payment and receive keys' button.
Your keys will appear in the textboxes. After that, you simply click 'decrypt using
keys', your files will be decrypted and restored to their original location.

You can easily delete this software, but know that without it, you will never be able
to get your original files back.

For more information on how to buy and send bitcoin, click 'Next page'.

<< Previous Page

Next Page >>

Send bitcoins to this bitcoin address:

1LrvjACvUfVyNtPedjcyrkgkhzWeZsp

Sp

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:

- **Coin.mx - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- 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 1.19 BTC to Bitcoin address: 16yd1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7 Get QR code

4. Enter the Transaction ID and select amount:

1.19 BTC ~= 500 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 **500** USD/EUR.

Troiani.Modul de raspândire

- Unii troiani pot intra în sistem folosindu-se de vulnerabilitățile browserului web.
- Uneori, troianii pot fi instalați prin intermediul altor paraziți precum viruşi, viermi, backdoors sau chiar spyware.
- Unii troiani sunt deja integrați în anumite aplicații.

Majoritatea cailor troiani pot cauza activități precum:

Infectarea, coruperea şi suprascrierea fişierelor, componentelor esențiale din sistem şi a aplicațiilor instalate. De asemenea, pot distruge întregul sistem prin ștergerea fişierelor critice sau formatarea hard disk-ului.

- Furtul de date financiare, precum numărul cardului de credit, nume de autentificare, parole, documente personale valoroase şi alte informații confidențiale.
- Să urmărească utilizatorul şi fiecare tastare pe care el sau ea o efectuează pe o tastatură. Calul troian poate de asemenea să efectueze capturi de ecran şi să inițieze alte activități pentru a fura informații specifice.
- Să trimită toate datele adunate unei adrese de email predefinite, să le încarce pe un server FTP predeterminat sau să le transfere printr-o conexiune de internet ascunsă unei gazde de la distanță.
- Să instaleze un backdoor sau să îşi activeze propriul component pentru a lăsa atacatorul de la distanță să preia controlul asupra calculatorului compromis.
- Să lase alți paraziți periculoşi.
- Să efectueze Denial of Service (DoS) sau alte atacuri de rețea împotriva unor anumite gazde de la distanță sau să trimită o cantitate excesivă de email-uri pentru a inunda calculatoarele predefinite.

CryptoLocker

Payment for private key

bitcoin

- Choose the amount of payment:

2 BTC

- Send coins to the following address:

Attention!

Make sure that you enter the payment information correctly! Each incorrect attempt will reduce the time to destroy the private key in half!

Are you sure you entered your payment information correctly?

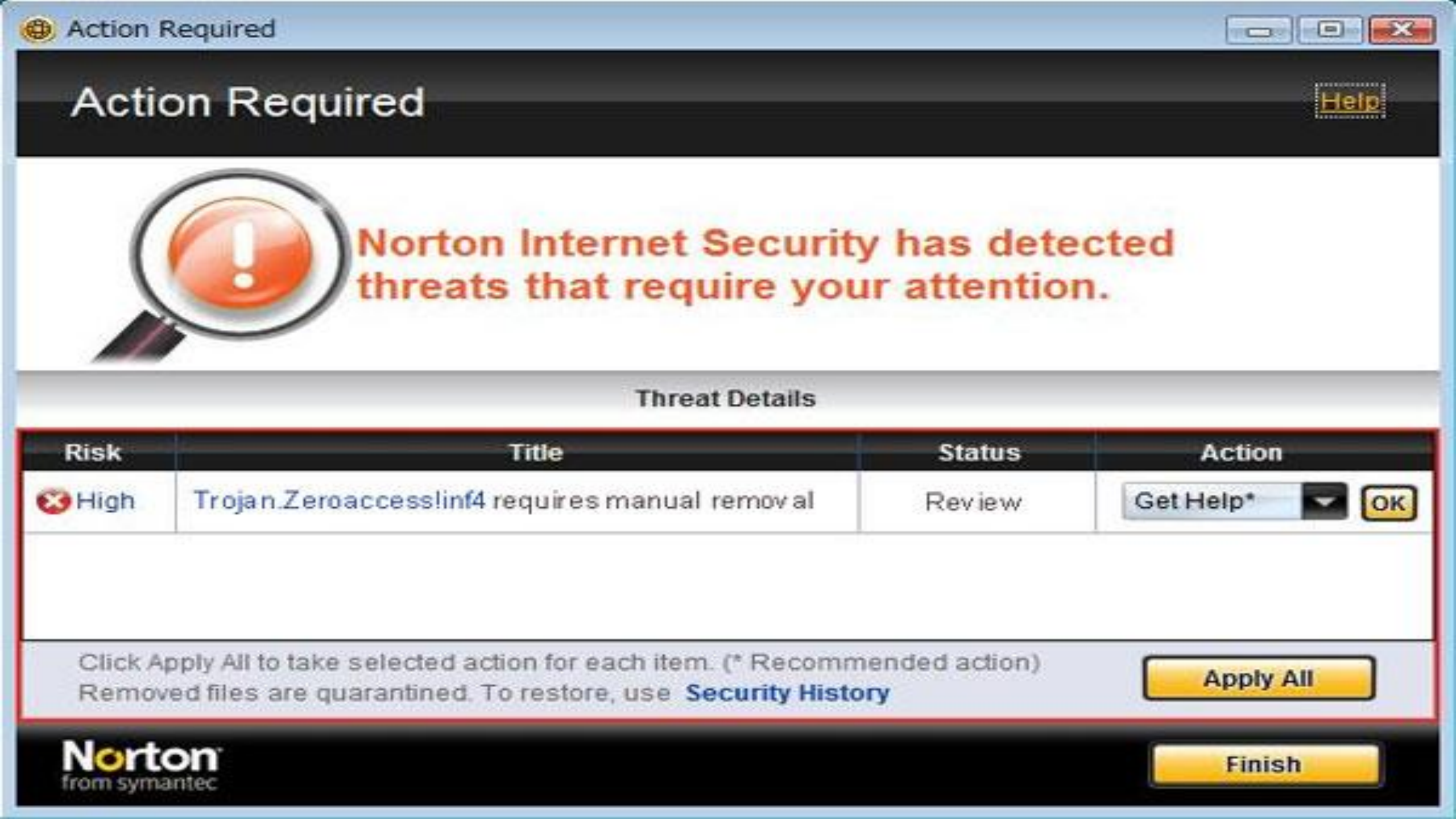
Yes | No

Time left

43 : 30 : 40

<< Back

PAY


Action Required
Action Required
Help
Norton Internet Security has detected threats that require your attention.
Threat Details
Risk
Title
Status
Action
High
Trojan.Zeroaccess!inf4 requires manual removal
Review
Get Help*
OK
Click Apply All to take selected action for each item. (* Recommended action)
Removed files are quarantined. To restore, use Security History
Apply All
Norton from symantec
Finish

Roblox virus

Programe de eliminare a virusurilor,virmilor și troianilor: Reimage, Malwarebytes(Plumbytes Anti-Malware)!!!