

Rising tide of ransomware

How criminals abuse encryption to work against us and what we can do to better protect ourselves




Chester Wisniewski
Senior Security Advisor
[@chetwisniewski](#)

SOPHOS

Who am I?



Methods of infection - SPAM




Een koerier had het pakket niet levered
[Zie de informatie](#) over uw pakket, pr

Aandacht!

Als het pakket niet binnen 30 dagen is
van u voor het is houden van in het b

Deze automatisch gegenereerde e-ma



Track & Trace

Reassessment notice

The reason of sending this notice of reassessment is that you have not paid your tax assessment. Interest and penalty tax will be added to your assessment. A 'tax default' under various taxation and regulations will be imposed. It will show that the mistake has been made while it is not intentional disregard of the law, and the penalty will be between 15-80, depending on the amount of the tax. If it is intentional disregard of the law by taxpayer, the penalty will be 70 per cent if the written disclosure is not made. The assessment will commence an investigation. All factors will be taken into consideration when determining reasonable grounds for reassessment.

[More Info](#)

A request for remittance should be made in writing. You should send a remission in writing to us and supply us with information on the reasons why the penalty tax should be remitted.

© Office of State Revenue: ISO 9001 - Quality Certified

RoyalMail

A courier did not deliver the parcel to your address **17 September 2014**, because nobody was home. Please [view information](#) about parcel, print it and go to post office to receive a package.

Attention

If the parcel isn't received within 30 working days Royal Mail will have the right to claim compensation for the parcel. Please [view information](#) about the procedure and conditions of parcel keeping in the nearest office.

This is automatically generated email, please [unsubscribe](#) if you do not want receive email from Royal Mail.

Royal Mail Group Ltd 2014. All rights reserved

Methods of infection – Exploit kits



Cryptowall 4 - What it won't encrypt

Paths to exclude

- windows
- temp
- cache
- sample pictures
- default pictures
- sample Music
- program files
- program files (x86)
- games
- sample videos
- user account pictures
- packages

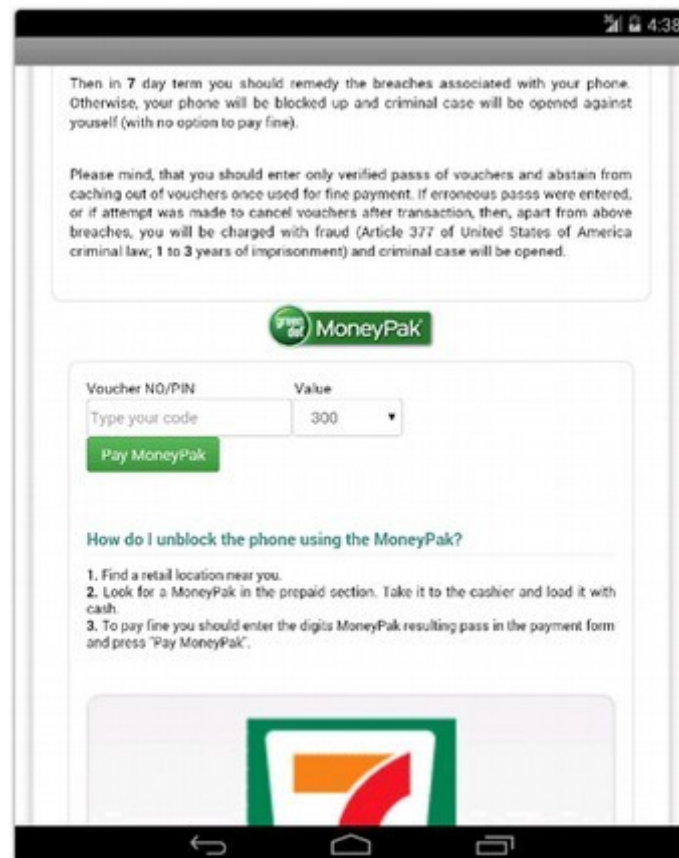
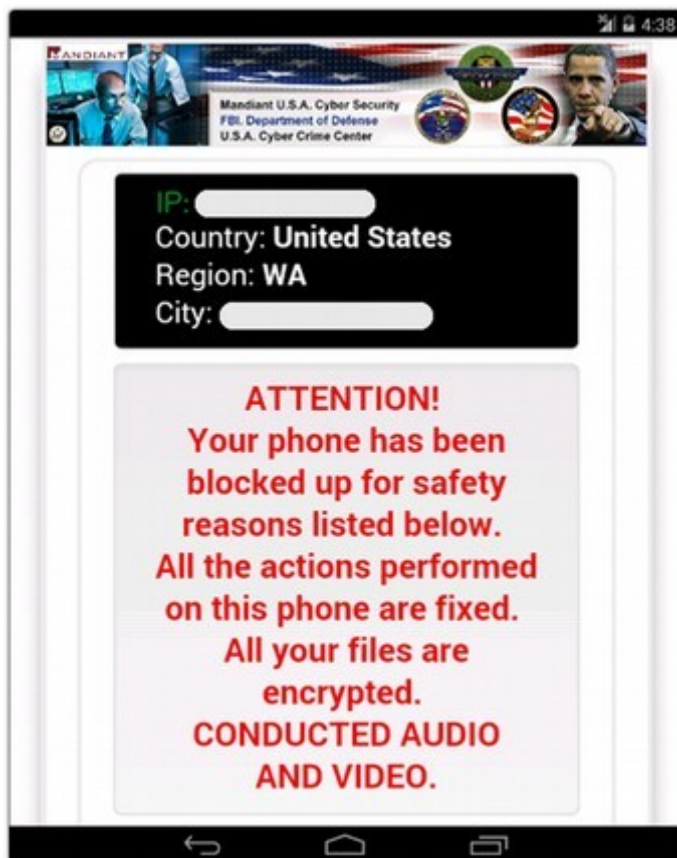
Files to exclude

- help_your_files.txt
- help_your_files.html
- help_your_files.png
- iconcache.db
- thumbs.db

Extensions to exclude

- exe
- dll
- pif
- scr
- sys
- msi
- msp
- com
- hta
- cpl
- msc
- bat
- cmd
- scf

Andr/Koler



Cryptowall 4 Ransomnote



Image: cryptowalltracker.org

Cryptolocker BitCash

1PgDeMeLLicRZZvZRZnMcRjvyDqX3qhTtL (0.27 BTC - Output)
1LCwEbogmvYRf3MDF9RRgh1Ey4y2wVvp3W (0.15 BTC - Output)
13kL6Uq7kFrtmXbV8avNih9HWjBFXWSgJ (0.18 BTC - Output)
1B6HJpp3hYNNFZLJvNJUMyjSeKYF1uif (0.15161 BTC - Output)
1Kjzv51DeYMR2GBS2KtkmGXCUSX13SSwgU (0.511 BTC - Output)
1KfdzT283ZUuC6cqHsr88GXkDreUSejfn (1 BTC - Output)
15GPMU89kBNwF7hKCaadBacQ9uHf5 (0.15 BTC - Output)

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary

Address [1ACKcumkx4M3aQisMMLq32EubPkUNiUFTC](#)

Hash 160 [64dd4006e5c768d120bb9b5b3afc513877577dcf](#)

Short Link <http://blockchain.info/fb/1ackcum>

Tools [Taint Analysis](#) - [Related Tags](#) - [Unspent Outputs](#)

Transactions

No. Transactions 368 

Total Received **31,734.98886786 BTC** 

Final Balance **1,360.00000001 BTC** 


Request Payment

Donation Button

1FAgu6mmKzoMWbrPAFdoNX8nkaQW94x2Sv (0.3 BTC - Output)
1AnWkzWqftZdFAZumxiNwPnEZZ82T5tAcD (0.2995 BTC - Output)
1CneiANaLPDUXLtkGkusUqVFr2ea9MtxhA (0.08595 BTC - Output)
1FAyYCh4uGCW5y4ekd6YHGChmLduLseisK (0.85826 BTC - Output)
1HeLNEczYAf6tXg36AR19tE4w4AdCChVnd (0.19 BTC - Output)
1CdCNRxq17KWcJmm3iw7ycpwFsZUPrSJou (0.126 BTC - Output)
1G... (0.1 BTC - Output)

No stone unturned





ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΑΤΤΙΚΗΣ

ΔΙΩΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΠΡΟΣΟΧΗ!

Ο υπολογιστής σας έχει αποκλειστεί!

Η διεύθυνση IP σας:
 Όνομα κεντρικού υπολογιστή σας: [redacted]
 Διεύθυνση παραπομπής: [redacted]
 Αυτό το λειτουργικό σύστημα μπλοκάρεται λόγω παραβίασης των νόμων της Ελλάδας! Σημειώθηκαν οι ακόλουθες παραβιάσεις:

Η διεύθυνση IP σας έχει διακρίνεται ιστοσελίδες που περιέχουν πορνογραφία, την παιδική πορνογραφία, κτηνοβοσκία, και τη βία κατά των παιδιών. Ο υπολογιστής σας επίσης περιέχει βίντεο που περιλαμβάνει πορνογραφία, βία και παιδική πορνογραφία! Επιπλέον, από το ηλεκτρονικό ταχυδρομείο σας αποστέλλονται μηνύματα με τη μορφή spam, που περιέχουν προεκρηκτική πρόθεση.

Αυτό το μπλοκάρισμα του υπολογιστή έγινε για να σταματήσουν οι παρόνομοι δραστηριότητές σας.

Για να ξεκλειδώσετε τον υπολογιστή, πρέπει να πληρώσετε πρόστιμο 100 ευρώ. Μπορείτε να πληρώσετε ποινή με δύο τρόπους:

- Μέσω του συστήματος Ukash:**
 Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής 19-ψήφιο κωδικό και να πατήσετε ΟΚ (αν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο ΟΚ).
 Εάν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους κωδικούς στη διεύθυνση email: Qri.r^@hgjlenjcrojce
- Πληρωμή μέσω Paysafecard:**
 Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής ένα 16-ψήφιο κωδικό (αν είναι αναγκαίο, με έναν κωδικό πρόσβασης), και στη συνέχεια κάντε κλικ στο ΟΚ (εάν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο ΟΚ).

Ukash Πού μπορώ να αγοράσω Ukash?
 Μπορείτε να πραγματοποιήσετε Ukash σε εκατοντάδες σημεία παροχής online, από παρπορόκια, καταστήματα ψαλίκων και μηχανήματα αυτόματης ανάληψης.

KIKI - KIKI Αγοράστε την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περφόρο και καταστήματα τροφίμων & ψαλίκων
Kapa - Kapa Αγοράστε την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περφόρο και καταστήματα τροφίμων & ψαλίκων

paysafecard Πού μπορώ να αγοράσω Paysafecard?
 Payzone Hellas είναι η μεγαλύτερη εταιρεία κινητής τηλεφωνίας top-up δικτύου στην Ελλάδα με εγκατεστημένη πάνω από 11.000 μηχανήματα POS. Payzone Hellas πρωταγωνιστεί, επίσης, πληρωμή λογαριασμών και υπηρεσιών κοινής ωφέλειας για την προστασία και τους παρόχους υπηρεσιών στην Ελλάδα.

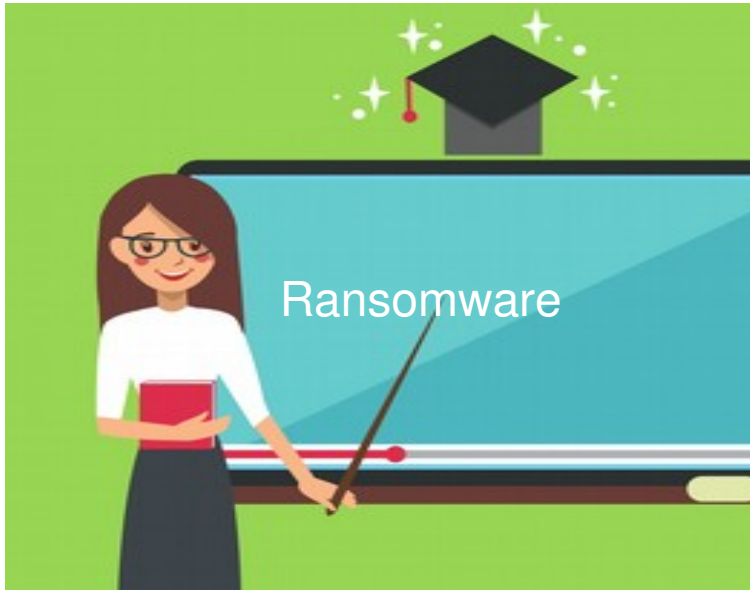
Εισάγετε 100 ΕΥΡΩ
 Paysafecard και Ukash κωδικό:

Εισάγετε τον κωδικό ή Ukash Paysafecard

ΑΓΙΣΤΩΑΝΕ



What to do? Analyze the strategy



SOPHOS