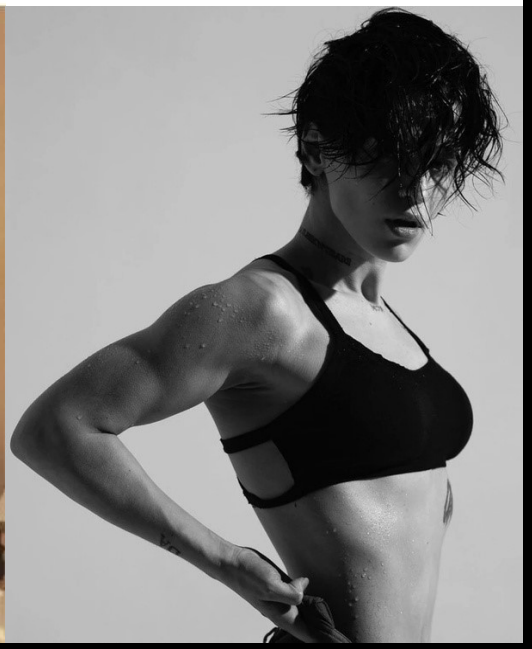
Εισαγωγή στην ασφάλεια και συνηθισμένες επιθέσεις

Fossaegean 2023

Σκοπός

Security Fan

Security Enjoyer



Τι είναι η ασφάλεια;

- Ασχολείται με την προστασία των υπολογιστών και των δικτύων, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.

- Η τεχνολογία της ασφάλειας έχει σκοπό τη δημιουργία συστημάτων που παραμένουν αξιόπιστα απέναντι σε δολιοφθορές και σφάλματα.

- Για να επιτευχθεί ο σκοπός αυτός καταφεύγουμε σε κατάλληλα εργαλεία, κατάλληλες μεθόδους και διαδικασίες σχεδιασμού, πρακτικές υλοποίησης και δοκιμής.

Απαιτήσεις Ασφάλειας (CIA)

- **Εμπιστευτικότητα (Confidentiality):** Στόχος της είναι η εξασφάλιση πως τα δεδομένα δε θα γίνουν διαθέσιμα σε μη εξουσιοδοτημένα άτομα.

- **Ακεραιότητα (Integrity):** Στόχος της είναι τα δεδομένα να μην υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα άτομα ή με μη ανιχνεύσιμο τρόπο.

- **Διαθεσιμότητα (Availability):** Στόχος της είναι το σύστημα να μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια.

Ευπάθειες και Απειλές

- Απειλή είναι η πιθανή αιτία βλάβης ή ανεπιθύμητου αντίκτυπου σε ένα σύστημα. Π.χ. οι χάκερ, οι ιοί και το κακόβουλο λογισμικό.
- Ευπάθεια είναι μια κατάσταση αδυναμίας του συστήματος την οποία εκμεταλλεύονται οι απειλές.

Τρόποι Αντιμετώπησης

- Κρυπτογράφηση
- Έλεγχοι λογισμικού
- Πολιτικές (π.χ. συστηματική αλλαγή κωδικών)
- Ανάλυση επικινδυνότητας
- Cybersecurity Frameworks

Ποιοτική Ανάλυση Κινδύνων

Η ποιοτική ανάλυση των κινδύνων είναι μία τεχνική κατά την οποία επιχειρείται να προσδιοριστεί το επίπεδο ασφάλειας που απαιτείται για ένα πληροφοριακό σύστημα.

Αυτό επιτυγχάνεται με μία συστηματική εξέταση :

- Των περιουσιακών στοιχείων
- Των απειλών
- Των ευπαθειών
- Του κόστους των απωλειών σε περίπτωση που συμβούν
- Του κόστους των αντιμέτρων σε περίπτωση που μπορεί να χρησιμοποιηθούν για την μείωση των απειλών και ευπαθειών

THE CYBER KILL CHAIN

SEARCHLIGHT Security

1 RECONNAISSANCE

HARVESTING EMPLOYEE EMAILS ADDRESSES AND CREDENTIALS, PROBING THE NETWORK IN SEARCH OF VULNERABILITIES.

2 WEAPONIZATION

COUPLING THE EXPLOIT WITH A BACKDOOR TO CREATE A DELIVERABLE PAYLOAD.

3 DELIVERY

DELIVERING THE WEAPONIZED BUNDLE TO THE VICTIM, FOR EXAMPLE THROUGH EMAIL, WEB, USB OR CLOUD APPLICATION.

4 EXPLOITATION

EXPLOITING A VULNERABILITY TO EXECUTE CODE ON THE VICTIM'S SYSTEM.

5 INSTALLATION

INSTALLING MALWARE ON THE ASSET.

6 COMMAND AND CONTROL (C2)

ESTABLISHED A COMMAND CHANNEL TO AN EXTERNAL SERVER FOR REMOTE MANIPULATION OF THE VICTIM.

7 ACTIONS ON OBJECTIVES

FOR EXAMPLE, DATA EXFILTRATION, RANSOMWARE DEPLOYMENT OR CORPORATE ESPIONAGE.

Κακόβουλο λογισμικό

Κακόβουλο λογισμικό (malware) είναι οποιοδήποτε λογισμικό που έχει σχεδιαστεί για να προκαλέσει:

- διαταραχή σε έναν υπολογιστή, διακομιστή, δίκτυο υπολογιστών
- να διαρρεύσει προσωπικές πληροφορίες
- να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και συστήματα
- να στερεί την πρόσβαση στον χρήστη σε πληροφορίες ή να παρεμβαίνει εν αγνοία του στην ασφάλεια και το απόρρητο του υπολογιστή του.

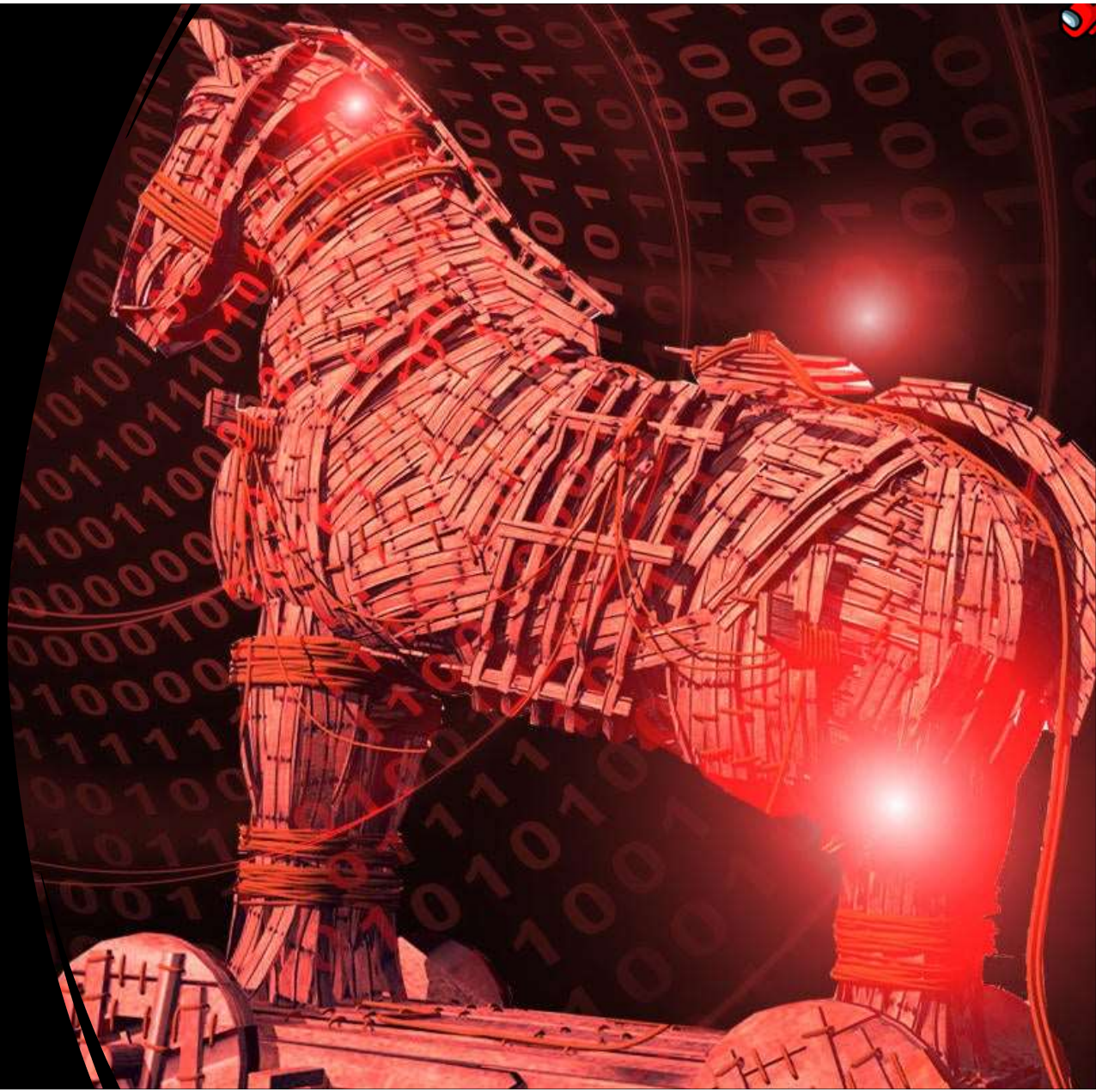
Που εμφανίζεται

Συνηθισμένες επιθέσεις

- Trojan Horse
- Ransomware
- Phishing/Spear Phishing
- DOS/DDOS
- SQL Injection
- XSS

Trojan Horse

Είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.



Ransomware

Το ransomware είναι ένας τύπος κακόβουλου λογισμικού που απειλεί το θύμα καταστρέφοντας ή εμποδίζοντας την πρόσβαση σε κρίσιμα δεδομένα ή συστήματα έως ότου καταβληθούν ρήτρα.

Phishing/Spear Phishing

Το Phishing είναι ενέργεια εξαπάτησης, κατά την οποία ο θύτης υποδύεται μία αξιόπιστη οντότητα. Χρησιμοποιεί τυχόν ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-θύματος, με σκοπό την απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί

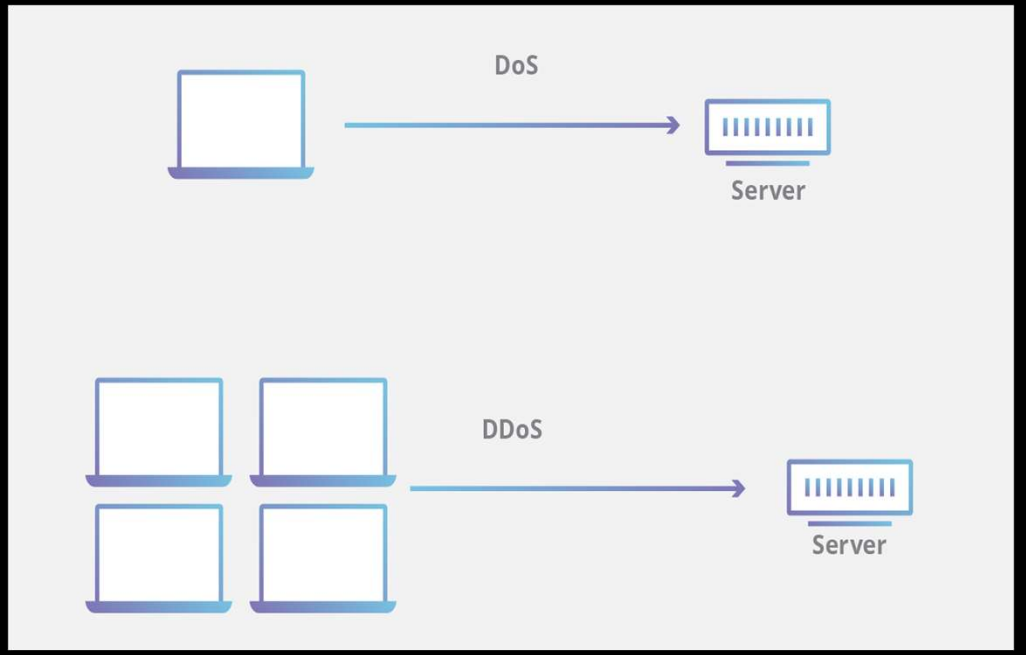
Νιγηριανός Πρίγκηπας ΑΚΑ "The Final Boss"

Αναγνώριση των red flags

DOS/DDOS

- DOS: Η επίθεση DoS είναι μια προσπάθεια να μην διατεθεί ένας συγκεκριμένος πόρος ηλεκτρονικών υπολογιστών στους νόμιμους χρήστες του.

- DDOS: Μια επίθεση DDoS είναι ένας τύπος DoS στον οποίο η επίθεση είναι αποτέλεσμα αιτημάτων που προέρχονται από πολλά συστήματα (σε αντίθεση με ένα μόνο σύστημα).



SQL Injection

- Οι SQL injection επιθέσεις είναι ο πιο συνηθισμένος τρόπος που οι χάκερ χρησιμοποιούν για να αποκτήσουν πρόσβαση σε ιστοσελίδες και για να κλέψουν ευαίσθητα δεδομένα

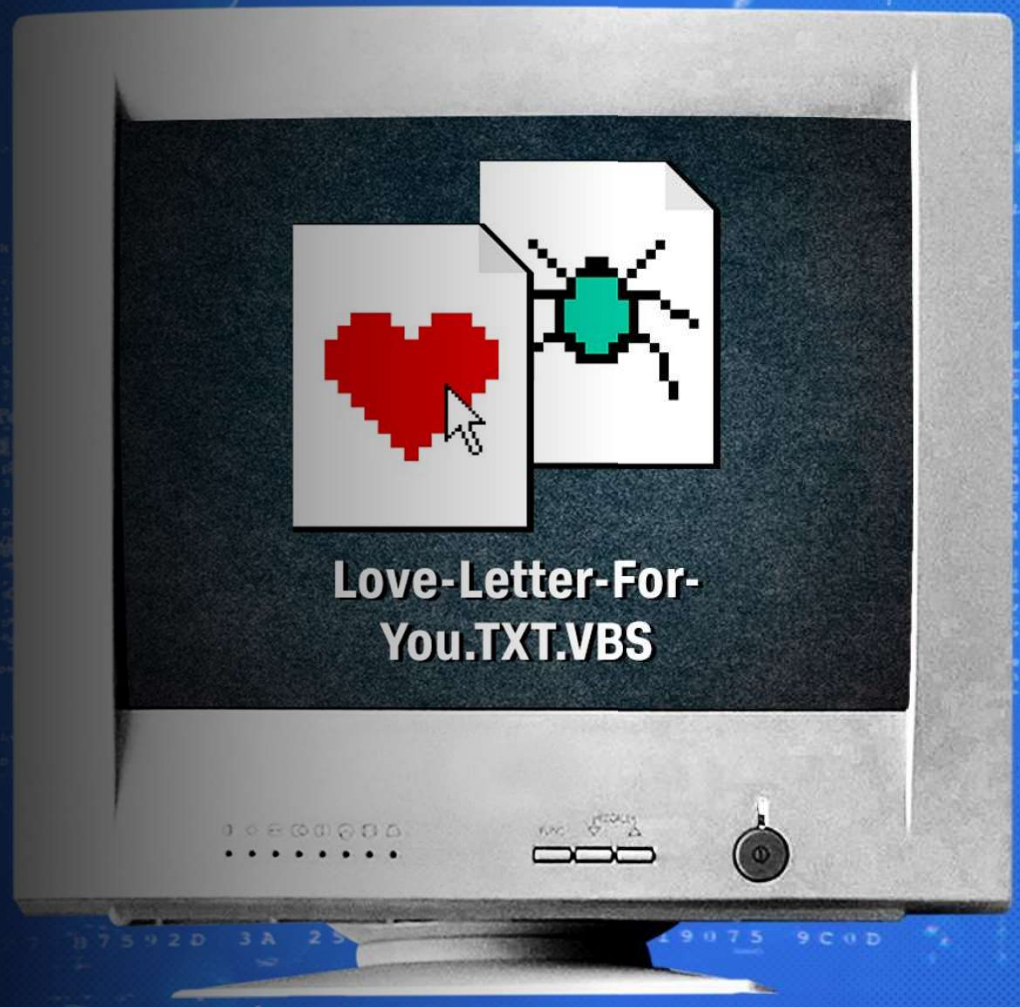
- Μια SQL επίθεση συμβαίνει όταν ο επιτιθέμενος πληκτρολογεί SQL κώδικα σε μια φόρμα στο διαδίκτυο και η web εφαρμογή που επεξεργάζεται αυτόν τον κώδικα δεν τον ελέγχει σωστά και τον εκτελεί, επιτρέποντας με αυτόν τον τρόπο τον εισβολέα να δώσει εντολές στη βάση δεδομένων για να διαρρεύσει αυτή ή τα δεδομένα της.

XSS

- Η επίθεση XSS εισάγει κακόβουλο κώδικα στον ιστότοπο, έτσι ώστε ο κώδικας να εκτελείται στους χρήστες αυτού του ιστότοπου από το πρόγραμμα περιήγησης.
- Η πιο κοινή γλώσσα για το XSS είναι το JavaScript.
- Συνήθως τα δεδομένα στέλνονται μέσω κακόβουλων web requests.

ILOVEYOU

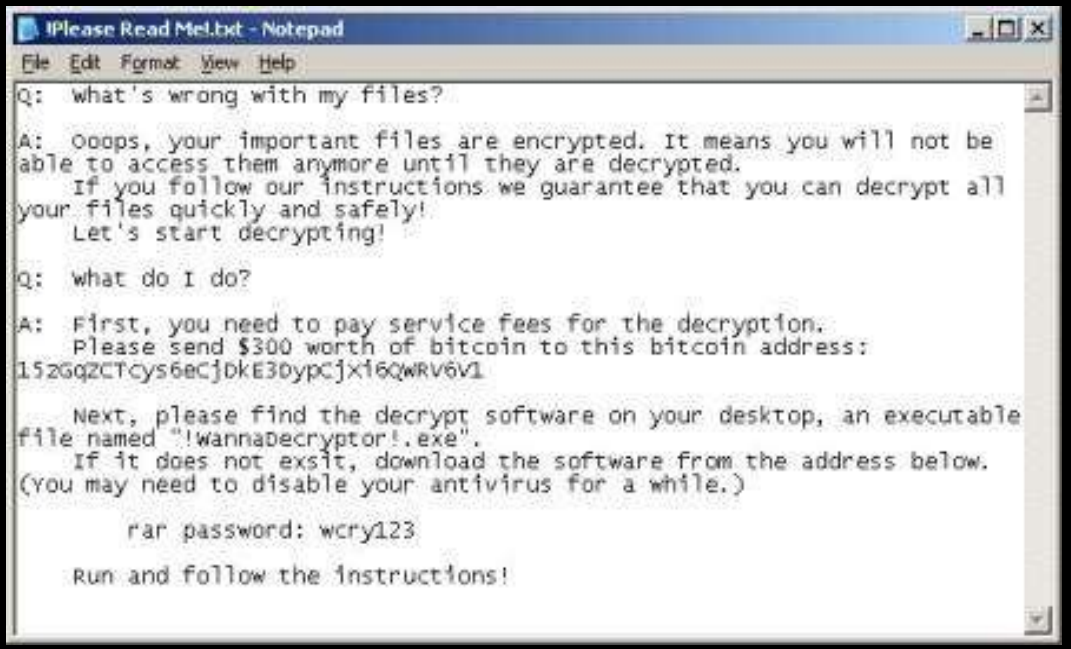
- Μια από τις μεγαλύτερες καταστροφές που έχει προκληθεί από social engineering. Μόλυνε περίπου 50.000 συστήματα.
- Πρόκειται για worm το οποίο δημιουργούσε αντίγραφά του σε πολλά διαφορετικά directories του υπολογιστή
- Έστελνε mail από τον υπολογιστή και τον λογαριασμό του θύματος με θέμα "ILOVEYOU" σε συνεργάτες του, το μήνυμα έγραφε: "Kindly check the attached LOVELETTER from me." και το αρχείο LOVE-LETTER-FOR-YOU.txt.vbs



WannaCry

- Το WannaCry είναι βασισμένο στο EternalBlue της NSA, ένα exploit του πρωτοκόλλου SMB των Windows.
- Πρώτα ο ιός ελέγχει αν υπάρχει το kill-switch domain και, εάν δεν βρεθεί, αρχίζει και κρυπτογραφεί αρχεία σε υπολογιστές θυμάτων. Στη συνέχεια προσπαθεί να σπάσει το SMB(server message block) κάθε υπολογιστή για να διαδώσει τον ιό σε τυχαίους υπολογιστές, αλλά και σε όλο το δίκτυο του θύματος.
- Τέλος εμφανίζει ένα μήνυμα το οποίο ζήταγε ένα ποσό πληρωμής με το ποσό να ξεκινά από τα 300 δολάρια. Μετά από τρεις ημέρες, το ποσό αυξάνεται κατά 300 δολάρια. Επτά μέρες μετά την επίθεση του θύματος, ο ιός διαγράφει τα αρχεία που βρίσκονται στον υπολογιστή. Ο τρόπος πληρωμής γίνεται μέσω Bitcoin.

Πως έμοιαζε


!Please Read Me!.txt - Notepad
File Edit Format View Help
Q: What's wrong with my files?
A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
If you follow our instructions we guarantee that you can decrypt all your files quickly and safely!
Let's start decrypting!
Q: What do I do?
A: First, you need to pay service fees for the decryption.
Please send $300 worth of bitcoin to this bitcoin address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Next, please find the decrypt software on your desktop, an executable file named "!WannaDecryptor!.exe".
If it does not exsit, download the software from the address below.
(You may need to disable your antivirus for a while.)
rar password: wcry123
Run and follow the instructions!

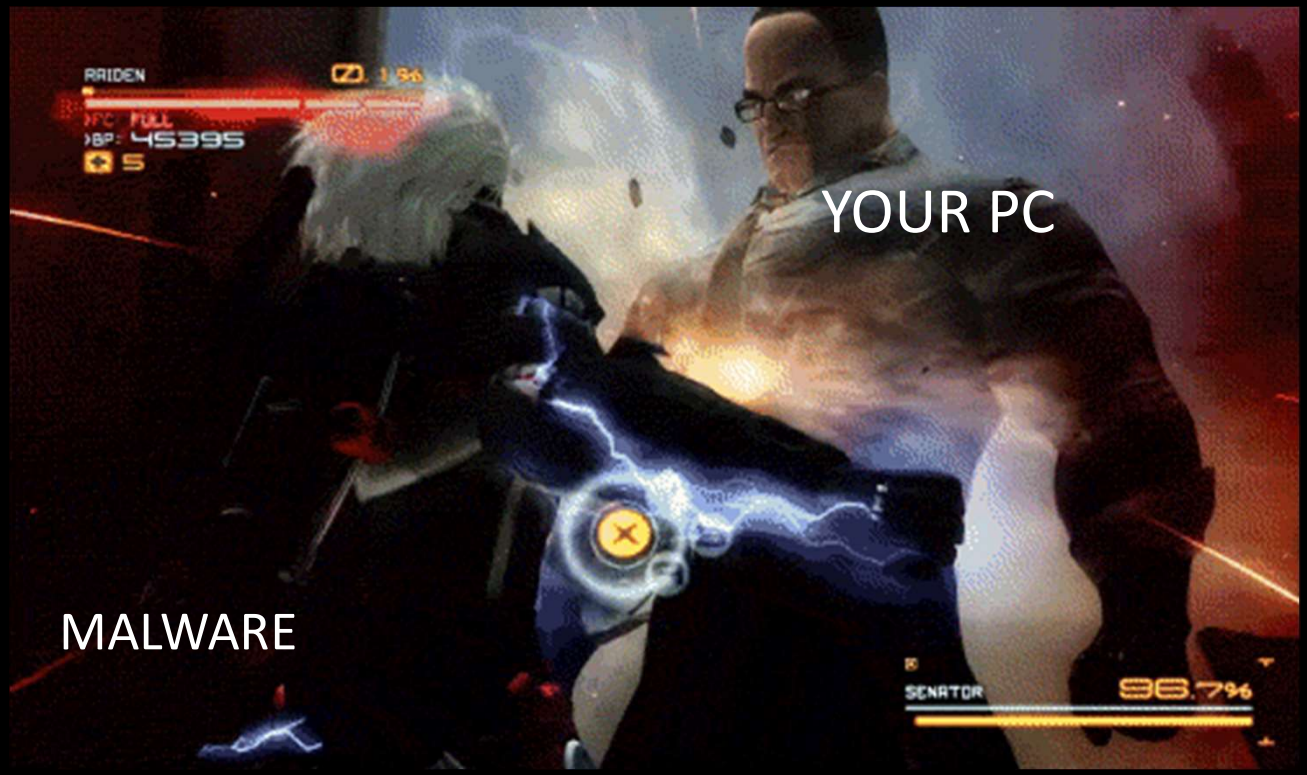

Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy


10 10
1110
0101 01
01 010
01
CVE®
Useful Websites

Useful tools

Useful Extensions

Τελικά αποτελέσματα



Ευχαριστώ για τον χρόνο σας

Ερωτήσεις;
και feedback