

HTTP is not secure

Μάριος Μπαλαμάτσιας
Κωστής Καραντίας

Μάρτιος 2015
Τμήμα Μηχανικών Υπολογιστών και Πληροφορικής, Πανεπιστήμιο Ιωαννίνων



Στόχοι της ώρας

- Επίδειξη ζωντανών επιθέσεων
- Υπόβαθρο επιθέσεων: HTTP/HTTPS
- Κατανόηση και **προστασία**
 - Σωστή χρήση **HTTPS**
 - Καλές πρακτικές ασφάλειας
 - Όλα μέσα από παραδείγματα

Εισαγωγή

Τι γίνεται όταν γράφουμε google.gr στον browser μας και πατάμε Enter;

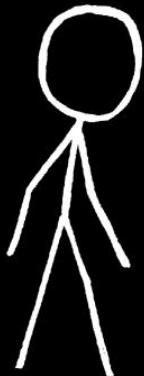
HTTP

Πρωτόκολλο για μεταφορά αρχείων.

Παραδείγματα αιτημάτων:

1. φέρε μου το *kalomoira.mp3*
2. φέρε μου το *vathmologies_sept2015.pdf*
3. φέρε μου το *very_funny_image.jpg*

HTTP



Δώσε μου την αρχική σελίδα

GET / HTTP/1.1
Host: www.google.gr



Εσύ

google.gr

HTTP



Εσύ

Ορίστε η αρχική σελίδα

HTTP/1.1 200 OK

Date: Wed, 25 Feb 2015 22:16:28 GMT

Content-Type: text/html; charset=ISO-8859-7

Accept-Ranges: none

Vary: Accept-Encoding

Transfer-Encoding: chunked

<!doctype html><html[...]



google.gr

Ένα πραγματικό αίτημα

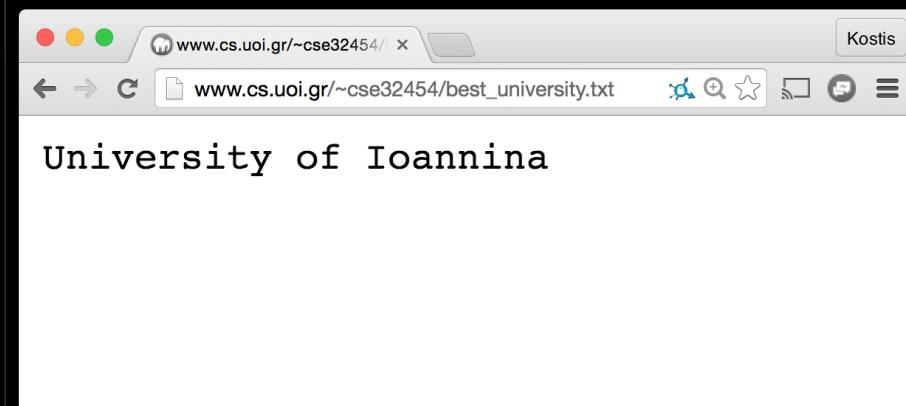
```
	gtklocker@schwarz: ~ ~ ~ zsh
atklocker@schwarz ~ $ nc cs.uoi.gr 80
GET /~cse32454/best_university.txt HTTP/1.1
Host: cs.uoi.gr
```

```
HTTP/1.1 200 OK
Date: Wed, 25 Feb 2015 22:35:41 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Wed, 25 Feb 2015 22:35:06 GMT
ETag: "8280b72-17-50ff13f490990"
Accept-Ranges: bytes
Content-Length: 23
Vary: Accept-Encoding
Content-Type: text/plain
X-Pad: avoid browser bug
```

University of Ioannina

```
gtklocker@schwarz ~ $
```

Αίτημα



Απάντηση

Αποστολή δεδομένων

Είδαμε μόνο πώς να ζητάμε δεδομένα (GET).
Όμως πώς γίνεται να κάνουμε login στο Facebook ή να ανεβάζουμε ένα post;

Είναι μια άλλη μέθοδος του HTTP και λέγεται POST!

POST

Τι συμβαίνει όταν πατάμε
Enter;

The image shows a login form with a blue header bar. The header bar contains the text "Email or Phone" on the left and "Password" on the right. Below the header, there are two input fields: one for "Email or Phone" containing the text "gtklocker" and another for "Password" containing a series of black dots. To the right of the password field is a "Log In" button. At the bottom left of the header bar is a checkbox labeled "Keep me logged in". At the bottom center is a link labeled "Forgot your password?".

Email or Phone	Password
gtklocker
<input type="checkbox"/> Keep me logged in	Forgot your password?
Log In	

POST



Κωστής

Κάνε login με το username και password μου

POST /login/index.php HTTP/1.1
Host: www.facebook.com
Content-Length: 49
Content-Type: application/x-www-form-urlencoded
username=gtklcker&password=123asfaliskwdikos



facebook.com

POST



Κωστής

OK είσαι ο Κωστής, πάρε τη σελίδα σου

HTTP/1.1 200 OK

Date: Wed, 25 Feb 2015 22:16:28 GMT

Content-Type: text/html; charset=ISO-8859-7

Accept-Ranges: none

Vary: Accept-Encoding

Transfer-Encoding: chunked

Γειά σου Κωστή!



facebook.com

Wireshark demo

Capturing from Wi-Fi: en0 [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request.method==POST Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
18163	96.028183000	192.168.1.4	195.24.232.208	HTTP	482	POST /protocol_1.2 HTTP/1.1 (application/x-www-form-urlencoded)
18197	96.181977000	192.168.1.4	195.24.233.57	HTTP	375	POST /np_1.2 HTTP/1.1 (application/x-www-form-urlencoded)
59226	248.780894000	192.168.1.4	195.130.120.101	HTTP	688	POST /login/index.php HTTP/1.1 (application/x-www-form-urlencoded)
72912	323.220955000	192.168.1.4	195.24.232.208	HTTP	430	POST /protocol_1.2 HTTP/1.1 (application/x-www-form-urlencoded)
72973	323.279976000	192.168.1.4	195.24.232.207	HTTP	406	POST /np_1.2 HTTP/1.1 (application/x-www-form-urlencoded)
88119	376.788401000	192.168.1.4	195.130.120.101	HTTP	707	POST /login/index.php HTTP/1.1 (application/x-www-form-urlencoded)

[Next sequence number: 642 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
D 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
Window size value: 4117
[Calculated window size: 131744]
[Window size scaling factor: 32]
Checksum: 0x2fd1 [validation disabled]
Urgent pointer: 0
D Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
D [SEQ/ACK analysis]
D Hypertext Transfer Protocol
D HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "gtklcker"
Form item: "password" = "I love spongebob"

0000 54 22 f8 c3 90 e5 b8 e8 56 35 1c 72 08 00 45 00 T*...1.. V5.r..E.
0010 02 b5 c7 72 40 00 40 06 23 d0 c0 a8 01 04 c3 82 ...@. #.....
0020 78 65 c7 65 00 50 b3 87 93 d0 8f ae 1a 09 08 18 xe.e.P..
0030 10 15 2f d1 00 00 01 01 08 0e 3b 50 94 15 bb/.... .;PP...
0040 9c c6 50 4f 53 54 20 2f 6c 6f 67 69 6e 2f 69 66 ..POST / login/in
0050 64 65 78 2e 70 68 70 20 48 54 54 59 2f 31 2e 31 dex.php HTTP/1.1
0060 0d 00 48 6f 73 74 3a 26 65 63 6f 75 72 73 65 26 ..Host: ecourse.
0070 75 6f 69 2e 67 72 0d 0a 43 61 6e 66 65 63 74 69 uoi.gr.. Connecti
0080 6f 6e 3a 20 6b 65 67 70 45 61 6c 66 76 65 0d 0a on.. keep -alive..
0090 43 6f 6e 3a 20 65 65 64 45 61 6c 66 68 3a 20 Content-length:
00a0 ad 04 0d 08 31 61 63 68 65 2d 43 ff 6a 6f 6f 44 ..Call a Contro
00b0 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 08 41 63 l_max-a ge=0 .Ac
00c0 63 65 70 74 3a 20 74 65 78 74 ff 68 74 6d 6c 6c capt.. to xt/html,
00d0 61 70 70 6c 69 63 61 74 69 ff 6e 2f 78 68 74 6d application/xhtm
00e0 6c 2b 79 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml..ap plicatio
00f0 6a 2f 79 6d 6c 3b 71 3d 30 2c 30 2c 60 6d 61 67 n/xml..n ..0 0 imao

Wi-Fi: en0 <live capture in ... | Packets: 90951 · Displayed: 6 (0.0%) | Profile: Default

Τι είδαμε;

Όλα τα δεδομένα που στέλνουμε και
παραλαμβάνουμε περνάνε στο δίκτυο
ακρυπτογράφητα!

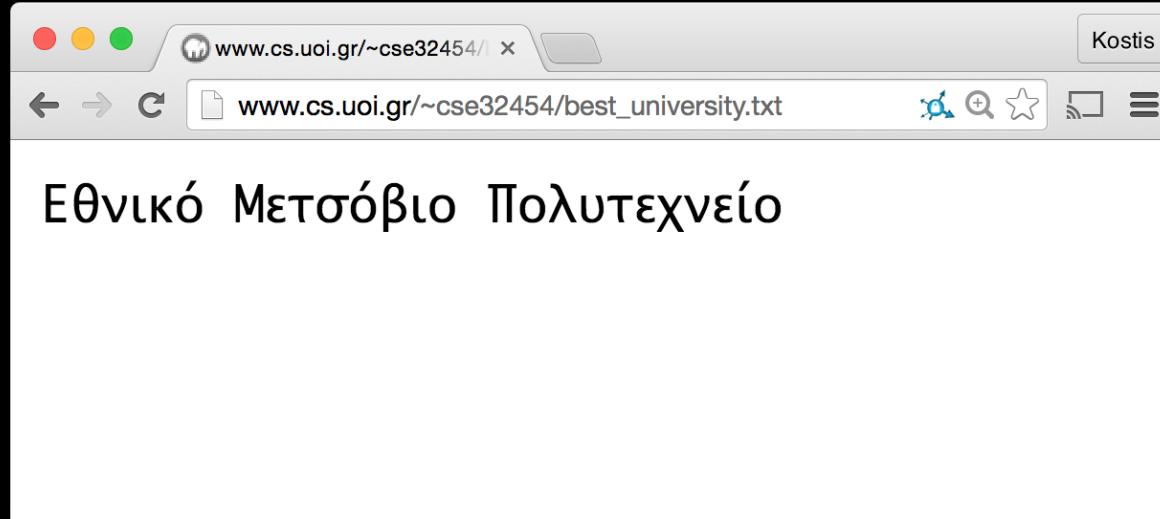
Επιθέσεις τοπικού δικτύου

Το να παρεμβληθούμε θα ήταν αρκετό για να τα διαβάσουμε.

Γίνεται; **ΝΑΙ!**

Επιθέσεις τοπικού δικτύου

Μπορούμε να αλλάξουμε το περιεχόμενο
οποιασδήποτε σελίδας.



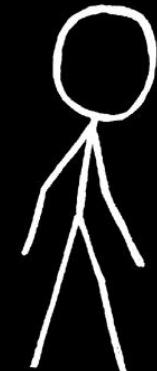
Επιθέσεις τοπικού δικτύου

Μπορούμε να διαβάσουμε οποιοδήποτε αίτημα, GET ή POST, το οποίο όπως είδαμε πριν μπορεί να περιλαμβάνει ευαίσθητα δεδομένα όπως κωδικούς.

Επιθέσεις τοπικού δικτύου

Και για όλα αυτά αρκεί απλά να είμαστε στο
τοπικό δίκτυο!

Επιθέσεις τοπικού δικτύου



Email or Phone
mbalamatsias@gmail.com

Password

Keep me logged in

[Forgot your password?](#)

[Log In](#)



Email or Phone
mbalamatsias@gmail.com

Password
eimai_mia_mikri_alepou

Keep me logged in

[Forgot your password?](#)

[Log In](#)

Μάριος

Kostis Karanatis
Edit Profile

New Feed

Messages

Events

Saved

GROUPS

- CS Forces
- IEEE UCI SB - Ομαδ...
- Πανελλήνιο Πρωτ...
- Ιωνίων, η Νάξ...
- See New Groups
- Create Group

FRIENDS

- Close Friends
- University of Ioannina
- Ioannina, Greece A...
- Athens, Greece A...
- Athens, Greece An...
- Reinhardt
- Logimus
- GNU Project
- Logimus
- Logimus

APPS

- Games
- Pokés
- Photos
- Notes
- Suggest Edits
- Games Feed

PAGES

- Πηγόρια Μυστικά
- Pages Feed
- Like Pages
- Create Page

Search Facebook

Update Status Add Photos/Videos

What's on your mind?

Luben shared a link.

Kόπι πάτη τελείωση στραβά με αυτή τη φωτογραφία του Κιμ Γιονγκ Όν

Για κίνησης πρωτότυπων της δύσης κάνει ανεύθυνα λόγω η πηγαία του κώματος

LUBENT.V

Like · Comment · Share

The Independent

He was only 34 years old

PAES

Κωστής

Kostis Karanatis
Edit Profile

New Feed

Messages

Events

Saved

GROUPS

- CS Forces
- IEEE UCI SB - Ομαδ...
- Πανελλήνιο Πρωτ...
- Ιωνίων, η Νάξ...
- See New Groups
- Create Group

FRIENDS

- Close Friends
- University of Ioannina
- Ioannina, Greece A...
- Athens, Greece A...
- Athens, Greece An...
- Reinhardt
- Logimus
- GNU Project
- GNU Project
- Logimus

APPS

- Games
- Pokés
- Photos
- Notes
- Suggest Edits
- Games Feed

PAGES

- Πηγόρια Μυστικά
- Pages Feed
- Like Pages
- Create Page

Search Facebook

Update Status Add Photos/Videos

What's on your mind?

Luben shared a link.

Kόπι πάτη τελείωση στραβά με αυτή τη φωτογραφία του Κιμ Γιονγκ Όν

Για κίνησης πρωτότυπων της δύσης κάνει ανεύθυνα λόγω η πηγαία του κώματος

LUBENT.V

Like · Comment · Share

The Independent

He was only 34 years old

PAES



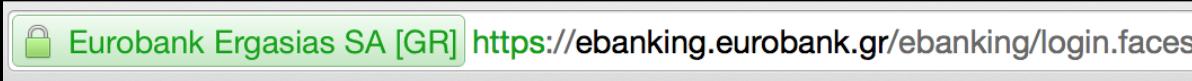
facebook.com

HTTP password stealing demo

HTTPS

Λύνει 2 προβλήματα:

1. Προστασία από κακόβουλους που παρακολουθούν το δίκτυο—τα δεδομένα που στέλνουμε και παραλαμβάνουμε είναι κρυπτογραφημένα.
2. Σιγουριά ότι αυτός με τον οποίο επικοινωνούμε είναι στην πραγματικότητα αυτός που υποστηρίζει.



Πώς φαίνεται στο δίκτυο;

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **tcp.port==443** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
94224	414.174811000	195.130.119.42	192.168.1.4	TCP	1434	LTCP segment of a reassembled PDU
94225	414.174863000	192.168.1.4	195.130.119.42	TCP	66	51184-443 [ACK] Seq=1458 Ack=21149 Win=131072 Len=0 TSval=995156085 TSecr=6809165
94226	414.175182000	195.130.119.42	192.168.1.4	TCP	1434	[TCP segment of a reassembled PDU]
94227	414.175184000	195.130.119.42	192.168.1.4	TLSv1	507	Application Data
94228	414.175223000	192.168.1.4	195.130.119.42	TCP	66	51184-443 [ACK] Seq=1458 Ack=22958 Win=129248 Len=0 TSval=995156085 TSecr=6809165
94238	414.211035000	2a03:2880:f01c:2:face:b00c:2001:648:3034:1300:f555:87:TCP			1484	[TCP segment of a reassembled PDU]
94239	414.211037000	2a03:2880:f01c:2:face:b00c:2001:648:3034:1300:f555:87:TLSv1.2			328	Application Data
94240	414.211037000	2a03:2880:f01c:2:face:b00c:2001:648:3034:1300:f555:87:TLSv1.2			876	Application Data
94241	414.211091000	2001:648:3034:1300:f555:87:2a03:2880:f01c:2:face:b00c:TCP			86	49682-443 [ACK] Seq=36385 Ack=368935 Win=129408 Len=0 TSval=995156119 TSecr=8525105
94242	414.211091000	2001:648:3034:1300:f555:87:2a03:2880:f01c:2:face:b00c:TCP			86	49682-443 [ACK] Seq=36385 Ack=369725 Win=128640 Len=0 TSval=995156120 TSecr=8525105
94641	417.065181000	2a03:2880:f01c:2:face:b00c:2001:648:3034:1300:f555:87:TCP			1484	[TCP segment of a reassembled PDU]
94642	417.065305000	2001:648:3034:1300:f555:87:2a03:2880:f01c:2:face:b00c:TCP			86	49682-443 [ACK] Seq=36385 Ack=371123 Win=131072 Len=0 TSval=995158936 TSecr=8525134
01643	417.065416000	2a03:2880:f01c:2:face:b00c:2001:648:3034:1300:f555:87:TLSv1.2			100	Application Data

Window size value: 65535
[Calculated window size: 65535]
[Window size scaling factor: 1]

▷ Checksum: 0x717c [validation disabled]
Urgent pointer: 0

▷ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

▷ [SEQ/ACK analysis]
TCP segment data (441 bytes)

▷ [6 Reassembled TCP Segments (5924 bytes): #94218(11), #94220(1368), #94222(1368), #94224(1368), #94226(1368), #94227(441)]

Secure Sockets Layer

 TLSv1 Record Layer: Application Data Protocol: spdy
Content Type: Application Data (23)
Version: TLS 1.0 (0x0301)
Length: 5919
Encrypted Application Data: e64609bc81b163af70099fee6521042b9afed0b0e4dbc68d...

Frame (507 bytes) Reassembled TCP (5924 bytes)

Payload is encrypted applica... Packets: 104103 · Displayed: 7370 (7.1%)

Profile: Default

HTTPS

Κάποιος που παρακολουθεί το δίκτυο δε ξέρει
τι στέλνουμε όταν επικοινωνόμε με HTTPS.

Αρκεί όμως αυτό για να αποφύγουμε μια
επίθεση σα την προηγούμενη;

Πιστοποιητικά

Στο HTTPS έχουμε πιστοποιητικά, που πιστοποιούν ότι όντως επίκοινωνούμε με το σωστό site.

Αυτή η πιστοποίηση γίνεται με κρυπτογραφική σιγουριά.

Έγκυρο πιστοποιητικό

 <https://www.facebook.com/pages/Kane-me>

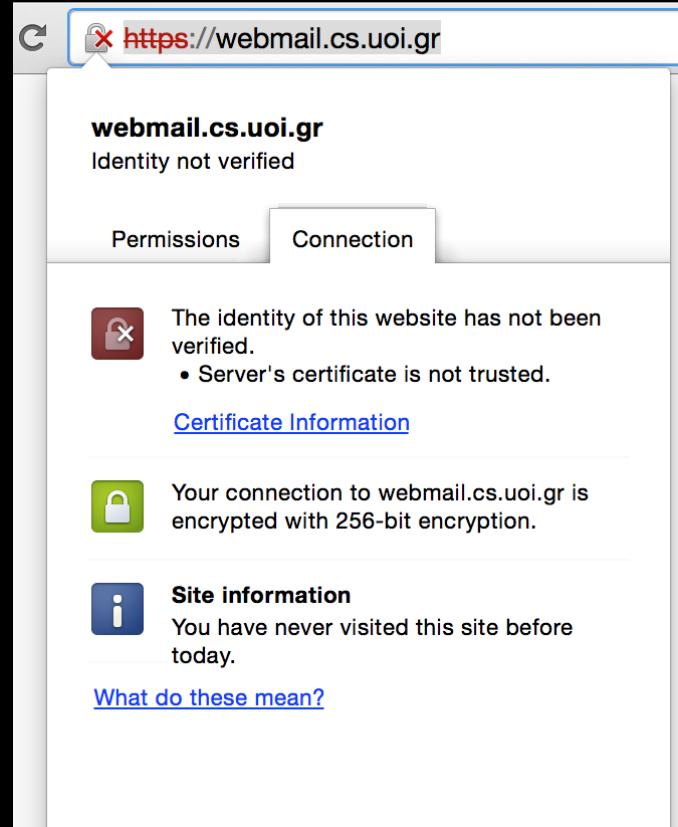
www.facebook.com
Identity verified

Permissions Connection

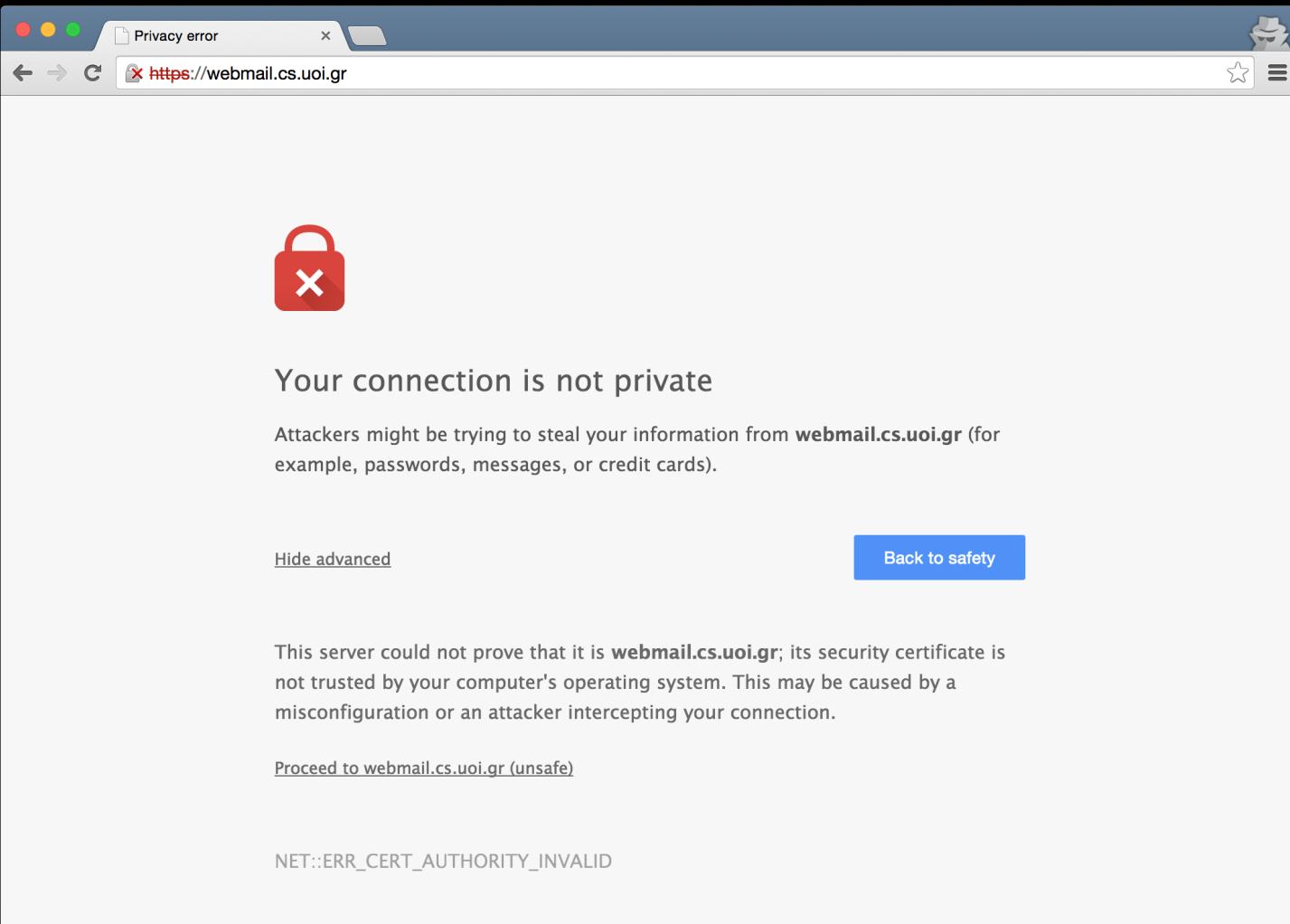
 The identity of this website has been verified by DigiCert High Assurance CA-3 but does not have public audit records.
[Certificate Information](#)

 Your connection to www.facebook.com is encrypted with 128-bit encryption.
The connection uses TLS 1.2.
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as the key exchange mechanism.

Άκυρο ηλεκτρονικό



Quiz: Τι θα κάνατε σε αυτή τη σελίδα;



A man wearing a dark jacket and a light-colored cap is standing in a warehouse filled with stacked wooden crates. He is holding a white iPhone retail box with both hands, pointing his right index finger at the green Apple logo on the front. The box also features the word "iPhone" and the Chinese characters "苹果".

THIS IS AN IPHONE

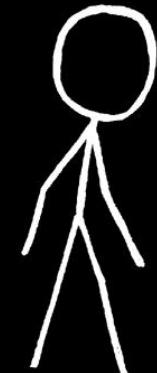
YOU CAN TELL BY THE LOGO

Πιστοποιητικά

Ο καθένας μπορεί να φτιάξει ένα πιστοποιητικό, αλλά μόνο ο πραγματικός κάτοχος του site μπορεί να έχει ένα **έγκυρο** πιστοποιητικό.

Όταν αποδέχεστε κάποιο **μη** έγκυρο πιστοποιητικό, αχρηστεύετε την ασφάλεια που σας προσφέρει το HTTPS.

Επιθέσεις τοπικού δικτύου



<https://www.facebook.com>

Email or Phone
mbalamatsias@gmail.com

Password

Keep me logged in

[Forgot your password?](#)

[Log In](#)

[Search Facebook](#)

Kostis Karanias Edit Profile

Update Status Add Photos/Videos

What's on your mind?

Luben shared a link.
2 mins - v

Kύριο πάτη τελείωση στραβά με αυτή τη φωτογραφία του Κιμ Γιονγκ Όν

Για κίνησης προκάτων της δύσης κάνει ανεύθυνα λόγο η πηγαία του κώματος

LUBENT.VN

Like · Comment · Share

The Independent
25 mins - v

He was only 34 years old

PAGES
ΠΗΓΕΡΩΤΑ ΜΟΥΣΙΚΑ
Like Pages Feed Like Pages Create Page



<https://www.facebook.com>

Email or Phone
mbalamatsias@gmail.com

Password
eimai_mia_mikri_alepou

Keep me logged in

[Forgot your password?](#)

[Log In](#)

[Search Facebook](#)

Kostis Karanias Edit Profile

Update Status Add Photos/Videos

What's on your mind?

Luben shared a link.
2 mins - v

Kύριο πάτη τελείωση στραβά με αυτή τη φωτογραφία του Κιμ Γιονγκ Όν

Για κίνησης προκάτων της δύσης κάνει ανεύθυνα λόγο η πηγαία του κώματος

LUBENT.VN

Like · Comment · Share

The Independent
25 mins - v

He was only 34 years old

PAGES
ΠΗΓΕΡΩΤΑ ΜΟΥΣΙΚΑ
Like Pages Feed Like Pages Create Page



facebook.com

Marios

Kostas

HTTPS password stealing demo

Άλλα θέματα ασφάλειας

Τι άλλο κάνουμε μέσω HTTP;

Κατεβάζουμε λογισμικό που τρέχουμε στον
υπολογιστή μας φυσικά!

Videolan - Official page for VLC media player

www.videolan.org/vlc/index.html

VideoLAN
ORGANIZATION

A project and a **non-profit organization**, composed of volunteers, developing and promoting free, open-source multimedia solutions.

Home News VideoLAN VLC Projects Contribute Support Dev' Zone

g+1 DONATE (why?)

f 4.00 € **d**

t \$ 5.00 **d**

VLC media player

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols.

Features Screenshots Skins

Download VLC
Version 2.1.5 • Mac OS X • 33 MB

Other Systems

Office - Microsoft Downloads

www.microsoft.com/en-us/download/office.aspx

Microsoft

Download Center

Shop Products Categories Support Security

Office

Top picks

Get things done from virtually anywhere
Buy Office 365 and get 1 TB of file storage from OneDrive.
 **Buy now**

Office 365 Business
Get full apps across devices.
 **Buy now**

Popular downloads

<https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CF8QFjAI&url=http%3A%2F%2Fwww.microsoft.com%2Fen-us%2Fdownload%2FOffice.aspx&ei>

Adobe Reader Download

get.adobe.com/reader/

Step: 1 of 3

Optional offer:

Yes, I want to try the free Lightroom 5 trial and learn how to make good shots great. Add to my download.

 Adobe Photoshop Lightroom

Terms & conditions:

By clicking the "Install now" button, you acknowledge that you have read and agree to the [Adobe Software Licensing Agreement](#).

Learn more

Note: Your antivirus software must allow you to install software.

Install now

Total size: 102 MB

uTorrent®

Light. Limitless.

Elegant, efficient torrent downloading.

Free Download
For Mac

Other Platforms

...
o o o
...

Αυθεντικότητα εκτελέσιμων

Θεωρούμε ότι εμπιστεύεστε τους δημιουργούς του VLC, του uTorrent και το Microsoft Office.

Αλλά...



Do you trust me?

Executable altering demo

Αυθεντικότητα εκτελέσιμων

Πώς θα αποφύγουμε μια τέτοια επίθεση;

HTTPS!

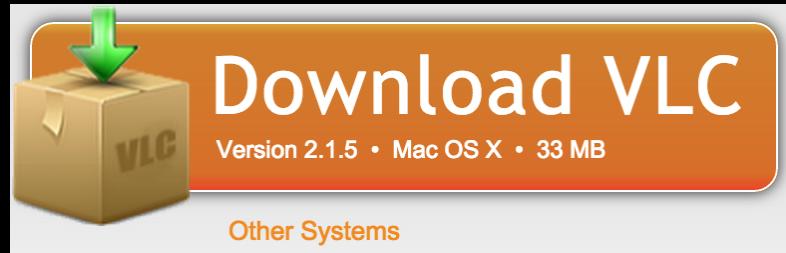
Executable altering demo with HTTPS

Αυθεντικότητα εκτελέσιμων



<https://www.videolan.org/vlc/>

ΝΑΙ



ΝΑΙ

A screenshot of a web browser displaying the official VLC media player website at <https://www.videolan.org/vlc/>. The page features a large orange traffic cone icon in the center. To its left, there are two green checkmarks with red arrows pointing towards the 'Features' and 'Screenshots' sections below. The main content area includes a brief description of VLC's capabilities, links to 'Features', 'Screenshots', and 'Skins', and a prominent orange download button labeled 'Download VLC'. Below the download button are links for 'Version 2.1.5 • Mac OS X • 33 MB' and 'Other Systems'. At the bottom, there are sections for 'Features' (with a link to the simple player) and 'Screenshots' (with a preview of several video frames).

https://www.videolan.org/vlc/

Simple, fast and powerful media player.

<https://get.videolan.org/vlc/2.1.5/macosx/vlc-2.1.5.dmg>

VLC media player

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols.

Features Screenshots Skins

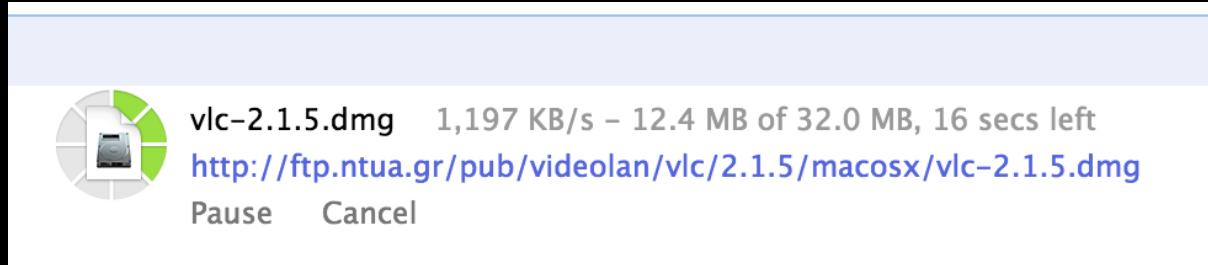
Download VLC
Version 2.1.5 • Mac OS X • 33 MB

Other Systems

Features

Screenshots

Αλλά



Κατεβαίνει από **HTTP**

Ποιο ήταν το πρόβλημα;

Παρ' όλο που η σελίδα ήταν **HTTPS**, το link του αρχείου ήταν **HTTP**, επομένως πάλι μπορέσαμε να το αλλάξουμε.

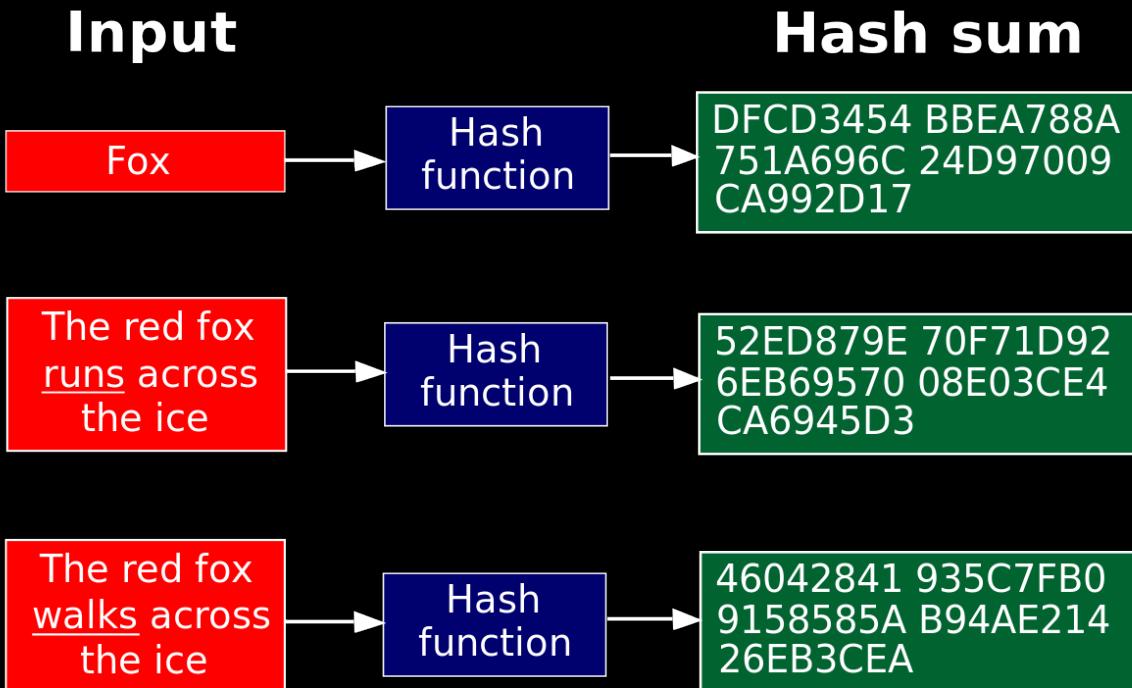
Πώς θα επιβεβαιώσουμε ότι το αρχείο που
κατεβάσαμε είναι όντως αυτό που θέλουμε;

Με Checksums!

Checksums

- Ένας μοναδικός αριθμός
- Παράγονται από μονόδρομες συναρτήσεις
- Αλλάζουν τελείως εάν μεταβληθεί το αρχικό αρχείο
- Παραδείγματα συναρτήσεων που χρησιμοποιούνται στην παραγωγή των checksums είναι: MD5 (όχι ασφαλής), SHA-1, SHA-2

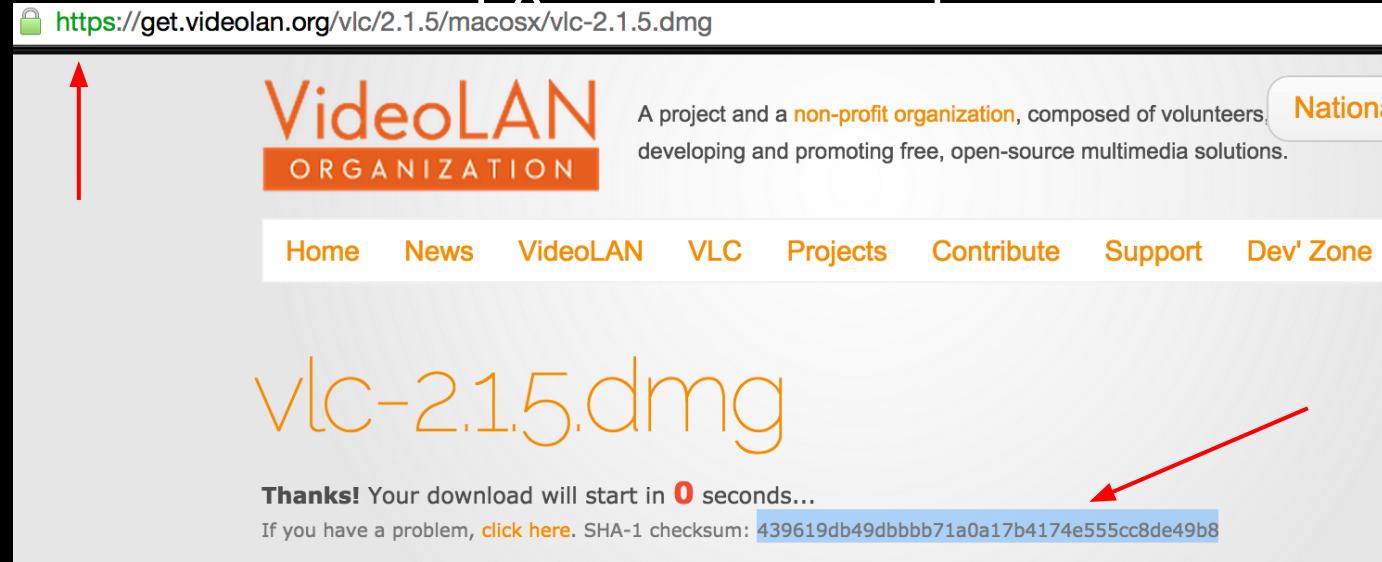
Checksums



Checksums

Πρακτικά σε Mac/Linux

- Βρίσκω από την σελίδα από την οποία κατέβασα το checksum του αρχείου που κατέβασα.



A screenshot of a web browser showing the VideoLAN Organization download page for VLC 2.1.5 on macOS. The URL in the address bar is <https://get.videolan.org/vlc/2.1.5/macosx/vlc-2.1.5.dmg>. A red arrow points from the top-left towards the logo. Another red arrow points from the bottom-right towards the SHA-1 checksum value at the bottom of the page.

https://get.videolan.org/vlc/2.1.5/macosx/vlc-2.1.5.dmg

 VideoLAN
ORGANIZATION

A project and a [non-profit organization](#), composed of volunteers, developing and promoting free, open-source multimedia solutions. [National](#)

Home News VideoLAN VLC Projects Contribute Support Dev' Zone

vlc-2.1.5.dmg

Thanks! Your download will start in **0** seconds...

If you have a problem, [click here](#). SHA-1 checksum: 439619db49dbbbb71a0a17b4174e555cc8de49b8

Checksums

Πρακτικά σε Mac/Linux

- Παράγω το Checksum του αρχείου που κατέβασα με:

```
➔ Downloads shasum vlc-2.1.5.dmg  
439619db49dbbbb71a0a17b4174e555cc8de49b8 vlc-2.1.5.dmg
```

- Συγκρίνω με το checksum από τη σελίδα κατεβάσματος

Checksums

- Επιλέγω κάθε φορά τον σωστό αλγόριθμο για την παραγωγή τους

Αν μου δίνεται για έλεγχο ένα sha256 checksum πρέπει να παράγω το sha256 του αρχείου (αντίστοιχα για sha512)

```
→ Downloads shasum -a 256 vlc-2.2.0-1.dmg
```

```
c8ac6d03336712ced3a6bdc063440bc58740749d75c0a28ea210fba312f74519 vlc-2.2.0-1.dmg
```

```
→ Downloads shasum -a 512 vlc-2.2.0-1.dmg
```

```
9078d22fd92a10ea2bc4b7283407a46f818b772e6dac19009b3f7848e450c8b0d360864f12c336566  
ea3bf5f1dfc9792476df29b5bd222713506e638e0428f63 vlc-2.2.0-1.dmg
```

Checksums

- Αν είναι ίδια τα Checksums τότε όλα **OK!**
- Αν όχι τότε:
 - ή το αρχείο δεν γράφτηκε σωστά οπότε
ξανακατεβάζω και ελέγχω
 - ή κάποιος κακόβουλος χρήστης **άλλαξε**
το αρχείο που κατέβασα

Checksums in Windows

Ακριβώς η ίδια διαδικασία αλλά χρειάζομαι το
Microsoft File Checksum Integrity Verifier

<https://www.microsoft.com/en-us/download/details.aspx?id=11533>

```
C:\>fciv -sha1 vlc-2.3.9.exe
//
// File Checksum Integrity Verifier version 2.05.
//
b5c8c15845a8eff88b95d23da4d7868647e775ef vlc-2.3.9.exe
```

Checksums

- Επιλέγω κάθε φορά τον σωστό αλγόριθμο για την παραγωγή τους

Αν μου δίνεται για έλεγχο ένα sha256 checksum πρέπει να παράγω το sha256 του αρχείου (αντίστοιχα για sha512)

```
→ Downloads shasum -a 256 vlc-2.2.0-1.dmg
```

```
c8ac6d03336712ced3a6bdc063440bc58740749d75c0a28ea210fba312f74519 vlc-2.2.0-1.dmg
```

```
→ Downloads shasum -a 512 vlc-2.2.0-1.dmg
```

```
9078d22fd92a10ea2bc4b7283407a46f818b772e6dac19009b3f7848e450c8b0d360864f12c336566  
ea3bf5f1dfc9792476df29b5bd222713506e638e0428f63 vlc-2.2.0-1.dmg
```

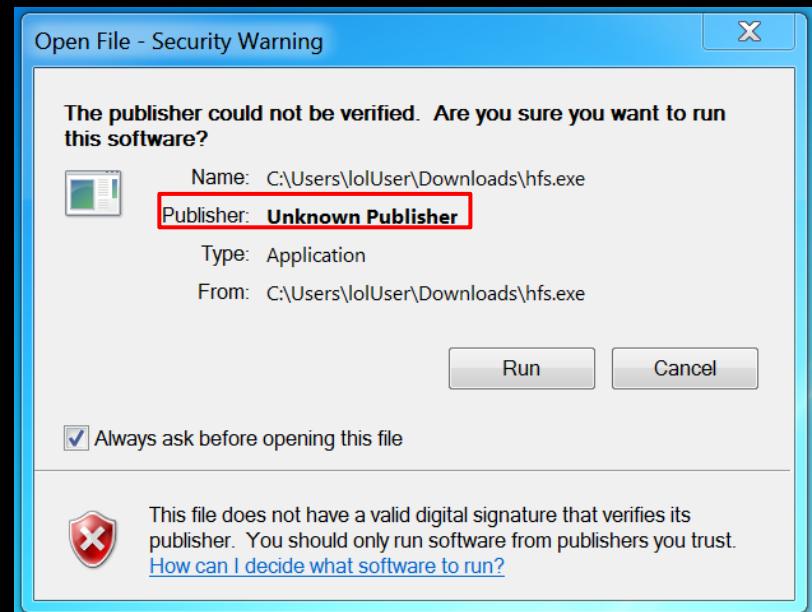
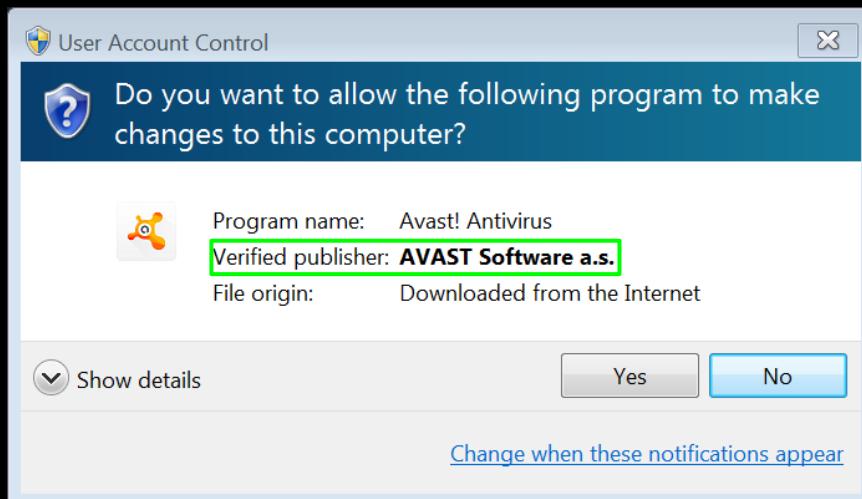
Ψηφιακά Υπογεγραμμένο λογισμικό

Είναι λογισμικό το οποίο μπορώ να:

- επιβεβαιώσω τον συγγραφέα του
- ή να ξέρω ότι δεν έχει μεταβληθεί από κάποιον κακόβουλο.

**Quiz: Γιατί να βρω το Checksum
μέσω **HTTPS**;**

Ψηφιακά Υπογεγραμμένο λογισμικό



Checksums

Κάποιος κακόβουλος θα μπορούσε να πειράξει το checksum που λαμβάνουμε μέσω **HTTP**.

Λίγα λόγια για Linux

Αν χρησιμοποιείτε Linux, η διανομή σας φροντίζει για την ασφάλεια σας.

Όταν κάνετε apt-get install vlc, το apt-get:

1. κατεβάζει το πακέτο του VLC
2. φροντίζει για την αυθεντικότητα του με τρόπους πολύ πιο προηγμένους από αυτούς που προλαβαίνουμε να συζητήσουμε σε μία ώρα

**Quiz: Εμπιστεύομαι οττοιονδήποτε
έχει ένα **έγκυρο** πιστοποιητικό και
κατεβάζω λογισμικό από αυτόν;**

Παράδειγμα

The screenshot illustrates a phishing attack against the VLC media player. The URL in the browser's address bar is <https://mbalamat.github.io/vlc-seems-legit/vlc.html>, which is a forged version of the official VLC website (<https://www.videolan.org/>). The page content is identical to the official site, including the VLC logo, download links, and sections for Features and Screenshots. A red arrow points to a donation form on the right side of the page, which is clearly fake.

<https://mbalamat.github.io/vlc-seems-legit/vlc.html>

VideoLAN
ORGANIZATION

A project and a [non-profit organization](#), composed of volunteers, developing and promoting free, open-source multimedia solutions.

g+1 DONATE (why?) PayPal

4.00 € [donate](#)

\$ 5.00 [donate](#)

[Features](#) [Screenshots](#) [Skins](#)

 Download VLC

Version 2.1.5 • Mac OS X • 33 MB

Other Systems

Features

Simple, fast and powerful media player.

Plays everything: Files, Discs, Webcams, Devices and Streams.

Plays most codecs with no codec packs needed:
MPEG-2, DivX, H.264, MKV, WebM, WMV, MP3...

Screenshots



Αυθεντικότητα εκτελέσιμων

ΠΡΟΣΟΧΗ

HTTPS = πιστοποίηση domain name. π.χ. αν κατέβαζα το VLC από το audiolan.org δεν θα ήταν ok ακόμη και με HTTPS

Τροφή για σκέψη:

- Εκτός από εμάς μήπως θα μπορούσε ο πάροχος της σύνδεσης σας να κάνει ακριβώς την ίδια επίθεση;
- Μήπως η κυβέρνηση σας;

Τι μάθαμε;

- Αποφεύγουμε τη χρήση HTTP για login και για να κατεβάζουμε λογισμικό

Ευχαριστούμε για την προσοχή σας!

Ερωτήσεις:

Βρείτε μας:

- cse32454@cs.uoi.gr Κωστής Καραντίας
- cse32492@cs.uoi.gr Μάριος Μπαλαμάτσιας



This work is licensed under a [Creative Commons Attribution 4.0 International License](#).