

# “Why are we here”?

## WORDPRESS HACKED






**The site ahead contains harmful programs**

Attackers on [this site](#) might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#) [Back to safety](#)

 **Account Suspended**

**This Account has been suspended.**

Contact your hosting provider for more information.

Today, Safe Browsing shows people more than 5 million warnings per day for all sorts of malicious sites and unwanted software, and discovers more than 50,000 malware sites and more than 90,000 phishing sites every month. If you're interested, you can see information about the dangerous sites that are detected by this technology anytime in our [Safe Browsing Transparency Report](#).



YOU HAVE BEEN HACKED !

Specially Dedicated To My Sweet Wife

**Dracula**



Is Here

**You HaVe BeeN HaCkEd By ArabAttack**

تم الاختراق من قبل حزب اناك تحت اواء الجيش السوري الإلكتروني

— syria for ever



My hostgator sites were hacked



Marked readable & junked by @markandit

UNLOCKed Forum

Marked readable & junked by @markandit. You will find us in the corner of all the games. You can play.

Marked readable & junked by @markandit. You will find us in the corner of all the games. You can play.

**2017 UPDATE**

# 15 VULNERABLE SITES TO (LEGALLY) PRACTICE YOUR HACKING SKILLS



# Egroup Services

Christos Pashiardis CEO – Egroup – “White hat hacker”  
Information Security Experts since 1997  
Pen Tests & Ethical Hacking  
Info. Sec. Policies  
Website Security Services



# Site Guarding Int.

Dmitry Baranov CEO – “White hat hacker”  
Website Security Experts  
R & D Lab for Websecurity  
“Cleaning & Monitoring Services”



# What are the of a website' s

- Reputation loss
- Business interruption (Emails etc...)
- Penalized by Google etc.
- Penalized by Hosting provider (all sites down) – (Host Gator, Blue Hosting etc.)
- Liable to Lawsuits
- Time wasted...

# “Damages compromise”?

- Reputation Recovery
- Business Recovery
- Google recovery procedure
- EU directive
- **Cyber Liability Insurance Cover (CLIC) ?**

“EU Member states have until May 2018 to translate it into national laws”




# How do they do it???

Nuke ver 2.3 by [ATS]

Enter IP and Msg: **Nuke the son of a bitch**

194.73.192.100

DIC SUCKER!!!



NetBus 1.70, by cf

Server admin

Open CD-ROM

Host name/IP: [ ] Port: 12345

in interval: 60

Function delay: 0

Buttons: About, Add IP, Connect!, Memo, Del IP, Scan!

Port Redirect, App Redirect, Server setup, Play sound, Exit Windows, Send text, Active wnds, Control mouse, Mouse pos, Listen, Sound system, Go to URL, Key manager, File manager

About Nuke and Nuke Sp'y is activated

L0phtCrack Trial Version

This program is shareware. See readme.txt for licensing information or visit <http://www.l0pht.com/l0phtcrack/>



© 1998 LHI Technologies, LLC. All Rights Reserved

15 Days until trial version will expire.

Buttons: OK, Register

File Help

RedButton



Select Server

Help

```
2/11/1998 3:14 PM
es
p
ever
LogonHours
LogonHours: All
Groups: Administrators (Local)
Guest
FullName: Built-in account for guest access to the computer/domain
Comment:
HomeDrive:
HomeDir:
Profile:
LogonScript:
Workstations:
PsudCanBeChanged: No
PsudLastSetTime: 8/10/1998 7:38 PM
PsudRequired: Yes
AcctDisabled: Yes
AcctLockedOut: No
AcctExpiresTime: Never
LastLogonTime: Never
```

Found 2 users

00001

# Type of attacks in Cyprus:

- **Spam attacks** spam scripts (contact us forms...) HTTPS ....
- **Hidden links**, fake SEO (hacker inserts in the text with hidden color links to other sites like casino, pharmacy , porn etc )
- **Phishing** (to collect the passwords) or cc from your visitors.
- **Bruteforce scripts** (to attack admin, email accounts).

A screenshot of a Chrome Safe Browsing warning message. The message is displayed in a red box with a white 'X' icon. The text reads: "The site ahead contains harmful programs". Below this, it says: "Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit)." There is a checkbox labeled "Automatically report details of possible security incidents to Google. [Privacy policy](#)". A "Details" link is visible on the left, and a "Back to safety" button is on the right. Below the red box, there is a paragraph of text: "Today, Safe Browsing shows people more than 5 million warnings per day for all sorts of malicious sites and unwanted software, and discovers more than 50,000 malware sites and more than 90,000 phishing sites every month. If you're interested, you can see information about the dangerous sites that are detected by this technology anytime in our [Safe Browsing Transparency Report](#)."



# Reduce the Risks of your Website's compromise

1. Purchase a website firewall... as low as 235 euros/year.  
<https://www.siteguarding.com/>
2. Update patches on Servers
3. Use Current Versions of CMS Software
4. Use reliable hosting companies. Ask your developer. It matters, for Google, for Security, for Speed, etc.
5. Always Update Scripts and Remove Installation Files
6. Never Underestimate Your Site's Importance to Hackers
7. CYTA is probably your best choice...



# What to do in case of emergency?

## 1. Website penetrated?

1. Have the mobiles & emergency phones of your ISP to close down your site ASAP.
2. Contact your website firewall suppliers.
3. Contact your website developers.

## 2. Have a clean back up of your website.

## 3. Change all admin passwords

## 4. Check for strange super admin members in your site.

## 5. Κάνε και ένα αγιασμό του γραφείου...



# Finally who is responsible for my website's security?

**ISP** – Internet Hosting Provider(Non os update or patch upgrade)? No IDS in place? No root kit scans?

**Website Design / Developer company?** (Did not update the CMS, or its components, or your version of CMS is incompatible? etc... or bad copy or copy of template or component? Or bad employee etc?)

**Customer?** (Sharing his admin/login password etc.)

Test your website's security



And now SiteGuarding in action...



Thank you.

Christos Pashiardis [christos@egroup.com.cy](mailto:christos@egroup.com.cy)

Dmitry Baranov [ceo@siteguarding.com](mailto:ceo@siteguarding.com)



# What is it to you?

Point	Benefit
You have a professional Info. Sec. business partner in Cyprus that you can trust.	Yes.
Your client's website is up in less than a few hours.	Yes.
Google & other S.E. delisting procedures	Yes
You are within the EU directives guidelines.	Yes
You have a recurring fee every year.	Yes
You are promoted free of charge at <a href="https://www.cyprusbestcompanies.com/">https://www.cyprusbestcompanies.com/</a>	Yes
You are part of the selected web dev. Firms that can have access to 72.000 potential clients	Yes.
You have a hosting company that you can trust.	Yes.