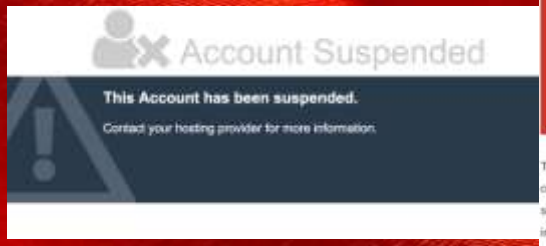
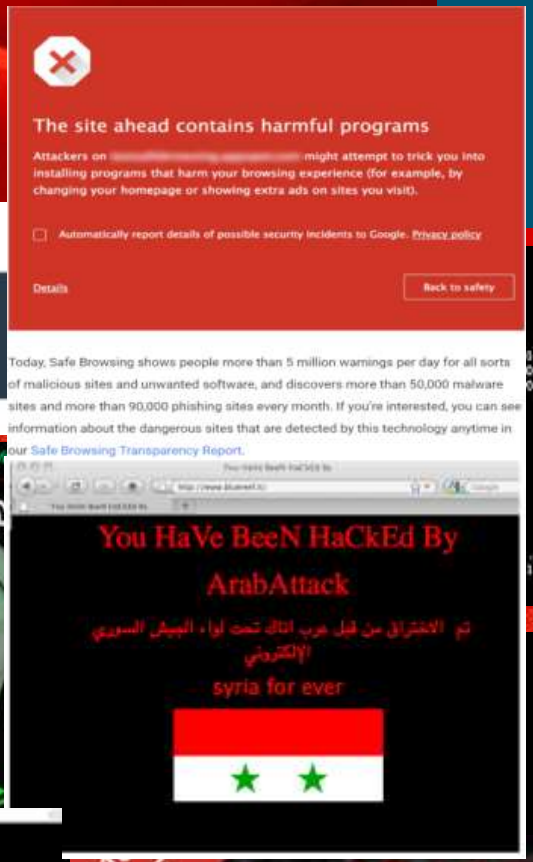
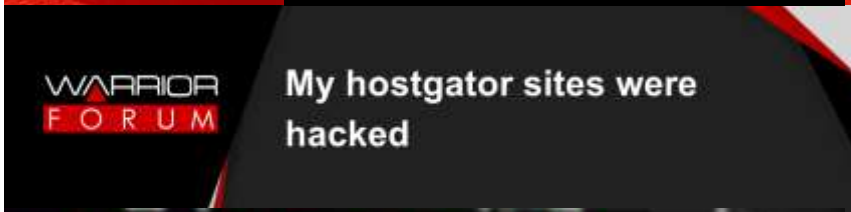
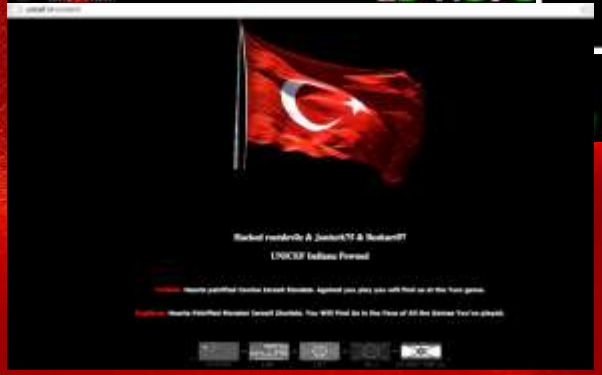
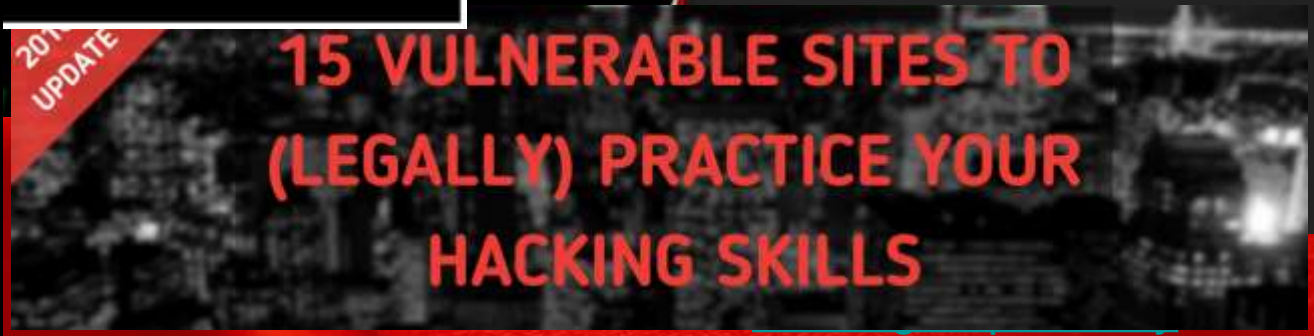
“Why are we here”?











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 "Damages of a website' s compromise"?

- 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…

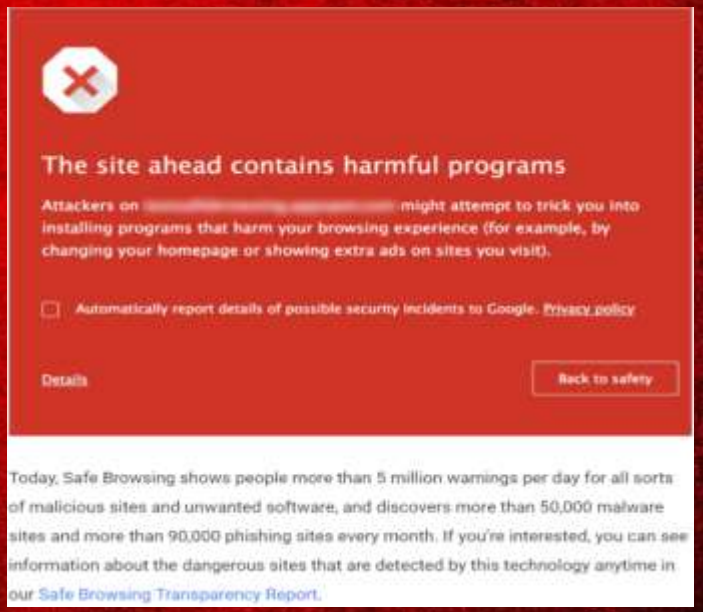
- Reputation Recovery
- Business Recovery
- Google recovery procedure
- EU directive
- **C**yber **L**iability **I**nsurance **C**over (CLIC) ?

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

How do they do it???

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).



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

Dmitry Baranov 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 https://www.cyprusbestcompanies.com/	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.