



How secure is your web site and system?

The UK news was full of details this week about the increase in cyber attacks especially on web sites being attacked by Russian hackers. The same hackers probably attacked thousands of sites in Estonia recently.

The Russian crime ring behind the infamous MPack attack hacked into thousands of Italian Web sites over the weekend and used a one-line snippet of code to redirect surfers from the web site they were visiting to a server rigged with exploits that could steal information including credit card details.

Anti-virus researchers tracking the attacks have found **more than 8,000 hijacked Italian Web sites.**

The sites at risk cover a wide range of Internet interests — from cars and racing (likely to take advantage of the formula one weekend), hotels, sports, music, lottery and pornography were all victims. Even web sites connected to Jon Bon Jovi and Mother Teresa weren't spared.

The MPack exploit kit used in this attack contains a stats counter that spells out in detail the types of exploits used, the number of compromised computers and types of browsers used by the victim (see screenshot below). In this case, it is clear that some newer exploit modules have been added to take aim at flaws in Firefox, Opera and even Apple's QuickTime media player.

The list of compromised sites is huge and from Mpack statistics this attack is working efficiently because the statistic page reports 65,000 unique visitors with almost 7,000 exploited browsers and attacks.

But there is a way to reduce the risk by having your web site and system regularly tested, preferably daily, for vulnerabilities.

encription's services include regular web site and system testing that will identify any vulnerabilities in your web site(s) or IT systems.

Visit

www.encription.co.uk

or call us on

01905 754440



CLH11206





How the attack happened

1



Victim visits hacked website

2



Website redirects part of web page to attacker's server, victim's are unaware of this.

3



Attacker's server downloads trojan virus to victim's machine

4



Further viruses downloaded and installed to victim's computer

5



Internet requests redirected to attackers servers allowing them to intercept confidential information