

HELP NET SECURITY Search Help Net Security

NEWS MALWARE ARTICLES REVIEWS Q&As EVENTS SOFTWARE NEWSLETTER

Subscribe for free
Browse archive

HITBSECCONF2016 AMSTERDAM
23-27 MAY 2016

7TH ANNUAL HITBSECCONF
IN EUROPE, NH KRASNAPOLSKY

Featured news

- Endpoint security really can improve user experience
- How email in transit can be intercepted using DNS hijacking
- Unexpected implications arising from the Internet of Things
- Flaw allows malicious OpenSSH servers to steal users' private SSH keys
- 250 Hyatt hotels around the world hit with PoS malware
- OS X's Gatekeeper bypassed again
- Success of the Internet of Things depends on privacy and security
- eBook: Fighting Known, Unknown, and Advanced Threats
- Cheap web cams can open permanent, difficult-to-spot backdoors into networks
- 800 risk experts from 40 countries identify the top global business risks
- Cisco kills hardcoded password bug in Wi-Fi access points
- Microsoft ends support for Windows 8, IE8 through 10: What does this mean for you?
- Have I been hacked? The indicators that suggest you have
- The danger of terror attacks using drones, and possible countermeasures

What you need to know to **earn more** in system administration and **security**

The need for global cooperation on cyber security

Posted on 23 February 2010.



When the Internet was in its teens, it was hard to imagine it evolving as far as it has. Yesterday I was chuckling over an [article](#) from 1995 in which the author adamantly claims that the Internet is a nice enough pastime, but it will never gain the kind of influence it has since then acquired over "real-life".

"The truth in no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works," he wrote. While I might agree with the second assertion and point out that videoconferencing solved that problem, the other two have already been disproved.

It's a fact that only a small minority of visionaries could have predicted that so much of our lives would be tied to the cyber world. Over the years, we have been able to reap the benefits of this state of affairs, but there are some foul things afoot that threaten it. Yes, we are talking about online criminals.

As events have proved, one of the major issues tied to online crime is that of the prosecution of guilty parties. The fact that there are no borders in the cyber world has lengthened considerably their reach. Another thing that allowed them to prosper is the fact that many countries are still years from establishing laws that would criminalize these exploits and from gaining the ability to understand them and gather enough evidence to prosecute them.

Datuk Mohammed Noor Amin, chairman of the U.N.-affiliated International Multilateral Partnership Against Cyber Threats, says that rich countries should help poorer ones find a solution for this problem and clamp down on cyber criminals operating from within their borders.

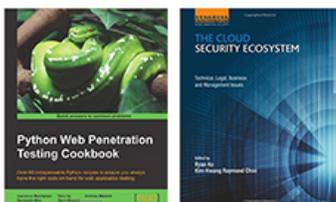
[Reuters](#) reports that there are a lot of people out there who would like to witness the rise of an international organization that would regulate cyberspace, because cyber crime is booming and yearly losses can be counted in billions of dollars.

Most countries still tend to look at the issue at the national level and seemingly fail to realize that the escalating growth of cyber crime is reaching levels that will sabotage the trust needed for economies to develop and grow.

"Nations take for granted the Internet is going to be 'on' for the rest of our lives. It may not necessarily be so," says cyber law expert Pavan Duggal. A disruption in service that would last days or weeks would create havoc with online businesses. "People have realize the Internet is an integral part of every country, politically, socially and business-wise," he says, and because of this it's important not to ignore the issue of cyber security.

Author: **Zeljka Zorz**, HNS Managing Editor

Subscribe to the HNS newsletter and win one of these books.
If you win, we'll e-mail you on February 8.



Spotlight

1 2 3 4 5

Flaw allows malicious OpenSSH servers to steal users' private SSH keys

Qualys researchers have discovered two vulnerabilities in the popular OpenSSH implementation of the secure shell protocol, one of which could be exploited by attackers to extract users' private cryptographic keys.



Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address



Daily digest

Receive a daily digest of the latest security news.

Email @ Address

Email Address

Subscribe

[10 key questions](#) to ask when selecting a cloud services vendor

DON'T MISS

Mon., Jan 18th

Endpoint security really can improve user experience

How email in transit can be intercepted using DNS hijacking

Flaw allows malicious OpenSSH servers to steal users' SSH keys

Cheap web cams can open permanent, difficult-to-spot backdoors

Have I been hacked? The indicators that suggest you have

[Back to TOP](#) ↑



Subscribe for free

Browse archive

HELP NET SECURITY

Search Help Net Security



STAY INFORMED



GET OUR NEWSLETTER

COPYRIGHT 1998-2016 BY HELP NET SECURITY. // [READ OUR PRIVACY POLICY](#) // [ABOUT US](#) // [ADVERTISE](#) //