

## Nothing's Safe In Cyberspace Says Leo Impact Security

*How cyber criminals (Wikileaks, Antisec, etc.) hack & expose top secret information?*

**Online PR News – 10-October-2011** – New York – Oct 11, 2011: What do the NSA, the Army and Sony Corporation have in common with US embassies around the world? All of them, along with over 2,500 other entities, have been compromised by hackers like Wikileaks and Antisec. The cost of these cyber-crimes has mounted to over \$3 billion a year. And “the little guy” isn’t safe, either. Everyone who uses the internet is at risk, despite the increasing use of antivirus software, IDS/IDP and firewalls in the current security models.

Today Leo Impact Security is exposing top secret methods used by cyber criminal’s also defending preventive methods because today all corporate, personal, and government computers are vulnerable to remote cyber attacks.

How do cyber criminals bypass current security model?

1. Antivirus bypass using crypters and protectors with random encryption methods (ex: cypherx, Themida).
2. Firewall bypass using known ports in malware like port 80 and 8080.
3. IDS/IPS avoid using SSL encryption+ DNS tunneling-based malware (BOTS, RAT).
4. Remote access to any computer using Zero day exploits (.doc, .PPT, and .PDF individual files), Java silent driveway, browser packs, Router DNS MITM, and pen testing tools – Core impact, immunity canvas, Metasploit Pro etc.

For Proof of concepts/Live demos, check our site: <http://www.leoimpact.com>

How to defend against advanced cyber attacks?

Use m2 security model developed by cyber security expert Manish Kumar, chief research officer at Leo Impact. All of the following services are nonprofit as per our Corporate Social Responsibility (CSR).

1. World’s first free antivirus scanning online engine which protects your PC from viruses, trojans, spyware, rootkits, and other malicious programs (zero day exploits) and attachments by using 32+ antivirus on cloud. Visit: [www.balajiplus.com](http://www.balajiplus.com)

2. To protect against unknown malware (rootlets, trojans, BOTS-Zesus, spyeye, Ghostrat, etc.) and zero day exploits attacks using Neutron+ Protection system software in PC.

3. To protect against remote-based attacks like DDOS, Sql Injections, XSS, and buffer overflow, use cloudflare.com on servers and Free VPN providers ([www.usaip.eu](http://www.usaip.eu), [www.vpnreactor.com](http://www.vpnreactor.com), [www.torproject.org](http://www.torproject.org), [www.hotspotshield.com](http://www.hotspotshield.com))

4. To protect against data & information leakage and other attacks, use our two-way authentication and free security analysis and consultancy.

About Leo Impact Security:

Leo impact is a global IT Security consulting, technology and Research company, with more than 14500 clients in more than 75 countries. Legally incorporated in India, USA, Europe (Czech, Italy) . Combining unparalleled experience, comprehensive Innovative capabilities across all IT Security and business functions, and extensive research on the world's most successful companies, Leo impact collaborates with clients to help them become high-secure businesses and governments.

Visit us at: [www.leoimpact.com](http://www.leoimpact.com)

## Media Information

Mark

pr@leoimpact.com

<http://www.leoimpact.com>

616 Corporate Way, Suite 2 #4000, Valley Cottage

new york

new york

10989

United States