



## 2011 - The year of malware attacks TrustDefender predictions for year ahead

**16 December, 2010:** 2010 has been the year of cybercrime. From data theft and internal breaches, to WikiLeaks and virus based cyber warfare; businesses and governments around the globe have been affected through stolen intellectual property and illegal transactions. A survey conducted earlier this year found, on average businesses in the U.S spend \$3.8 million alone coping with cyber attacks, with some organisations overtly inflicted with costs of up to \$52 million.<sup>1</sup> The UK is devoting more energy to understanding and developing weaponry (to the cost of £650 million) for cyber warfare, more than any other military area<sup>2</sup> and in Australia 69% of adults having been subjected to cyber crime.<sup>3</sup>

TrustDefender predicts 2011 will see a strong increase in cyber activity including malicious malware threats, stolen identities and data infiltration. The move of applications and work environments into the cloud, along with the growing use of mobile devices and online transactions, poses a growing risk to enterprises and makes individuals more vulnerable online. Without adequate attention to online security malware attacks will continue to become more sophisticated and targeted to take advantage of these channels.

Ted Egan, CEO TrustDefender comments, "We have seen a dramatic shift in the way criminals exploit and do business this year – everyone is now at risk. The evolution of IT infrastructure through Smartphone, USB, tablet devices and cloud computing integration has increased online vulnerabilities. Enterprises and end-users do not have the tools or key knowledge of real-time security to address these potential risks. As we continue to rely on the internet throughout our daily lives, the need for real-time solutions is essential."

"The emergence of cyber warfare and cyber espionage foresees some dramatic threats to government protection. Stuxnet is just one example of the impact cybercriminals can have, with over 44,000 computers having been infected with the Stuxnet virus worldwide. The recent events around WikiLeaks address the need to protect personal and corporate data. For the first time governments around the world are listing cybersecurity at the top of their agendas." Ted Egan concludes.

TrustDefender's key predictions for malware advancements in 2011 are:

- 1) **Man-in-the-mobile malware will dominate the year** – The advancement of Smartphone technology from Androids to iPhones provides a valuable opportunity for cyber criminals. The advancement of Smartphone technology from Androids to iPhones provides a valuable opportunity for cyber criminals. There are limited security offerings for Smartphone's and with the increasing growth of mobile banking and shopping this contributes to these devices being targeted and their vulnerability. Malicious activity running in the memory of mobile devices ('man-in the mobile') can go undetectable



while having the ability to infiltrate internet transactions, hack professional email accounts and steal personal data and identification.

- 2) **Malware to increase in sophistication-** Malware will utilise capabilities such as anti-researcher tricks incorporating capabilities using detection of virtual machines and anti-tamper technology capabilities. They will also begin using geo-location tools to identify researchers.
- 3) **Malware activism** –more criminals and “regular” individuals will use customised malware to target specific government and corporate internet activities. Likewise incidences of corporate espionage are set to grow in 2011. Some malware will continue to experiment with embedding itself in hardware. This will not be particularly successful for widespread use, although it might be very effective for the growing espionage market purposes.
- 4) **Specific capabilities to target corporates-** As more and more governments, corporate enterprises and online business move their Information Technology infrastructure into the cloud. There is a serious requirement to have flexible technologies that can reach out to the edge of the cloud and secure the cloud while building trust in the online relationship and the provider.
- 5) **Advanced Trojans and Old Techniques are back** - As we have seen in 2010, we will see an alarming increase in the more sophisticated Trojans escaping detection from traditional anti-virus – increased zero-day attacks. Many of these sophisticated Trojans will incorporate old techniques phishing, spear phishing and SMiShing activities in 2011

-END-

For more information visit: [www.trustdefender.com/blog](http://www.trustdefender.com/blog)

For any further media information or an interview contact:

Sharon Ghatora or Monique Jones Taurus Marketing

Phone: +61 2 9415 4528 or +61 416 890 648 / +61 413 689 343

Email: [sharon.ghatora@taurusmarketing.com.au](mailto:sharon.ghatora@taurusmarketing.com.au) / [monique@taurusmarketing.com.au](mailto:monique@taurusmarketing.com.au)

Notes:

1. <http://www.networkworld.com/news/2010/072610-cybercrime-costs.html>
2. <http://uk.reuters.com/article/idUKTRE6AL6BP20101123>
3. <http://www.smh.com.au/technology/security/cyber-crime-hits-almost-7-in-10-aussies-report-20100909-151yf.html>
4. [http://www.pcworld.idg.com.au/article/368460/experts\\_stuxnet\\_changed\\_cybersecurity\\_landscape/](http://www.pcworld.idg.com.au/article/368460/experts_stuxnet_changed_cybersecurity_landscape/)



### **TrustDefender explained:**

- TrustDefender solves the issues facing financial institutions where an increasing percentage of their customer base connects to online banking services with malware infected computers.
- Furthermore financial institutions have no visibility in real-time to see whether their customers have taken care of their computers and therefore the enterprise cannot distinguish between an infected or clean computer. This leaves the financial institution and the user at risk.
- TrustDefender's unique technology, evaluates the security health risk of a computing device, allowing the business to detect the ever increasing sophistication of malware, immediately act and stop a potential threat through the application of business rules and policies in real-time before any authentication process begins.
- TrustDefender provides key information to online enterprises including financial institutions, while giving the enterprise risk manager a real-time risk profile of the endpoint computers access their website.
- TrustDefender can be easily integrated with existing and older risk management engines to enhance the capabilities of these technologies.
- TrustDefender provides the enterprise with the ability to not only protect the customer but also notify the customer of any security threats and advise them how to deal with any potential risk. The Safe&Secure Mode will make sure a customer can always securely login and fix the problem at a later date.

### **About TrustDefender**

TrustDefender is the worldwide leading provider of 'real-time risk based online transaction security solutions' to safeguard consumer, financial institution and business online transactions. TrustDefender's revolutionary technologies enable users to verify its security health state, perform a memory forensics analysis and secure their mobile computing device in real-time - before and during any Internet transactions.

At the same time, TrustDefender provides real time feedback on the security health of their computer. Best yet, the user does not need to be a security expert to use this technology. Most importantly, for the first time, the financial institution has real-time information that they can use to better protect transactions from compromise and also allows the enterprise risk managers to finally get a real time risk profile of their customer base.

The Enterprise Server incorporates a real-time risk-scoring engine that together with the rules and policy engine is always in control and can give the financial institution a server-side tool to mitigate the risk on both ends and includes an extensive Auditing and Reporting module. TrustDefender is the world's first security solution which enables online businesses to integrate the home user or end user's PC into one overall security chain.



TrustDefender was founded in December 2005 after the founders discovered the traditional security model was broken – and decided to fix it.

DRAFT