

TrustDefender reveals true threat of new Trojan Carberp– the new Zeus!

8th October 2010: Leading online transaction security provider, TrustDefender has analysed the latest new transactional Trojan Carberp, (pronounced Car-ber-‘P’), which is already gaining momentum with cyber criminals in Europe and the US. Financial institutions and enterprises should be wary of Carberp as it is challenging the highly successful transactional Trojans; Zeus, Mebroot and Silentbanker to become a leading malware security threat.

TrustDefender Labs (the research and development division of TrustDefender) has discovered the potential impacts and risks of this new Trojan. While Zeus has been the leading class of malware for security attacks throughout the last 18 months, there are a number of new players entering the market with an extensive new feature-set and distribution network challenging existing Trojan detection software.

Online Security expert and CTO of TrustDefender, Andreas Baumhof comments; “This particular Trojan appears to be purpose built and has evolved in sophistication at a rapid rate. TrustDefender anticipates Carberp will further develop and could morph into a problematic threat from a financial, political and personal perspective. This demonstrates how quickly the bad guys are innovating new sophisticated threats.”

Carberp was first seen in May 2010, however most recently TrustDefender experts have witnessed the increasing sophistication of the Trojan, which is evolving at a very fast rate. Carberp is a promising challenger to Zeus and potentially provides a new class of Trojan for cyber criminals to use.

Why should we be worried about Carberp?

- Ability to disable other Trojans so it does not interfere with its attack and more importantly does not send stolen information to the competition
- Ability to run as a non-administrator
- Ability to infect Windows XP, Windows Vista and Windows 7, which only few Trojans can do. The Browser Hooking also works for Firefox in various versions but still not yet Chrome.
- Sophisticated browser hooking/installation to fully control all internet traffic (including HTTPS with EV-SSL) and the entire internet session
- It will not make any changes to the registry (only in memory modifications)
- Stolen data is transmitted in real-time to a Trojan’s ‘Command and Control’ (C&C) Server
- Carberp also has a configuration file system where it can inject arbitrary HTML into any website
- Ability to inject dynamically HTML overlays into any banking session, similarly to Zeus, Gozi and Spyeeye, with the aim to work around dynamic authentication schemes (such as 2fa authentication)

Andreas Baumhof continues “The evolution of Trojans such as Carberp highlights that the malware problem is here to stay and will only get worse with malware reaching out to new areas such as Windows 7, Apple Mac and mobile devices. This highlights the need for financial institutions and



enterprises to provide appropriate security for their users so the end user's device is fully protected. This obviously also applies for cloud based applications. While Trojans such as Zeus and Mebroot are successful and high profile; the 'bad guys' obviously wish to stay under the radar and with new malware and configuration files they are able to continue to infiltrate in new ways."

END

For more information visit:

www.trustdefender.com and 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 / monique@taurusmarketing.com.au

TrustDefender will fully detect and protect against Carberp. The TrustDefender online transaction security solution was designed to protect the user and the financial institution right from the start.

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.