

## TrustDefender demonstrates sophisticated HTML and JavaScript injection of Carberp

**9<sup>th</sup> December 2010:** After revealing the true threat of new Trojan Carberp, TrustDefender Labs has released an in-depth analysis into how the malware infiltrates websites and the details of its operation. Carberp hit the scene with a big bang last month targeting financial institutions with transactional two factor authentication schemes. The new Labs report reveals how cyber criminals have developed sophisticated configuration files and JavaScript methods, which Carberp is using with remarkable skill to target banking websites.

TrustDefender Lab's most recent analysis of the Carberp variant exposes the complex configuration systems used, shows how the website mechanism works and highlights the impressive JavaScript injection code used by cyber criminals.

Andreas Baumhof, CTO of TrustDefender comments, "Today's Trojans are evolving to become more than just an enabler to get sophisticated HTML into the currently viewed website. In this way Carberp follows the same principle as all other transactional Trojans such as Zeus, Gozi, Spyeye and Silon. What makes Carberp so effective is the threat does not come from the malware itself. The real threat comes from the configuration file and the related resources such as the highly modular and sophisticated JavaScript inclusions."

The fraudsters behind Carberp spend considerable time not just on the configuration file, but also making sure they have a flexible and dynamic method in place to compromise even elaborate two factor authentication schemes. Their aim goes beyond just information stealing where the stolen data is sent to a different location. The bad guys employ a forceful method to send and receive information to bypass even dynamic password schemes. Dynamically generated JavaScript will ensure that Carberp is customised for the targeted financial institution and operation (e.g. wire transfer).

What are the sophisticated Javascript characteristics being used by Carberp?

- Carberp features heavily dynamic JavaScript hosted on a valid HTTPS (SSL) websites
- This JavaScript is designed to get around the most sophisticated two factor authentication code (such as transactional hardware tokens)
- Carberp demonstrates how cyber criminals are developing Trojans to create sophisticated configuration files and JavaScript. Theoretically this can be used with any type of Trojan of choice whether that is Carberp, Zeus, Spyeye or Gozi
- The sophistication of the injected HTML is incredibly high. User experience specialists are employed to do this as the key is to make it look legitimate

Andreas Baumhof continues "The evolution of Trojans such as Carberp highlights how Trojans use complex behaviour to employ intelligent guises and commit fraudulent activity. Financial institutions and enterprises need to provide appropriate security, beyond traditional AV software to reduce the risks of fraudulent activity."

**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)

**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.