

New TrustDefender Labs report highlights enhancements of the notorious Zeus Trojan to undermine tracking and detection

Sydney, Australia - Wednesday 5th October 2011 – TrustDefender Labs, the research arm of online security and web fraud detection company TrustDefender – has released a new in-depth report covering recent variants of the world’s most successful Trojan that focuses solely on making it harder to be tracked by the good guys.

The Zeus Trojan is one of the most successful Trojans of our times, which can mainly be attributed to the innovation, flexibility, separation of core Trojan and the Man-In-The-Browser configuration (webinjects) plus its stealthy operation that enables the creators to easily distribute the ‘Zeus Trojan as a service’ (SaaS) to many, many fraudsters.

When the source code of the Zeus Trojan was leaked to the public in April this year, it was clear that it would have some serious implication for the security industry. Within a matter of weeks, three new variants of the Zeus Trojan have been found in the wild based on this leaked source code. All new variants have implemented improved Antivirus evasion capabilities and the ability to make sure security researchers and automated security tools cannot easily compile a list of targeted brands (such as financial institutions, payment processors, government agencies or any online retailer).

Andreas Baumhof, CEO of TrustDefender comments that “Currently there are dedicated services offerings available that constantly decrypt known Zeus configuration files to determine which brands are affected and how they are affected. These services try to give financial institutions an early warning that they are being targeted. The disturbing fact is that with the proliferation of many new and different variants of the Zeus Trojan plus new innovative methods of encrypting the configuration file, this method of decryption cannot be done automatically anymore – thus giving the criminals a head start and more time to perpetrate the crime.”

Baumhof proceeds: “We need to change the paradigm from ‘reactive to proactive’. We cannot rely on the fact that we protect against just the things we know; we need to change our thinking to protect the good things we have. The TrustDefender Intelligence Suite is built exactly on this paradigm. For example our clientless Man-In-The-Browser protection in TDzero works by intelligently fingerprinting the website, whereby we know how the genuine website really looks like versus the site the customer or end user is looking at. We don’t need to know a configuration file to protect a brand. This is true protection that is instant, proactive and without delay.”

The recent variants show that the creators of the various malware are constantly improving their work and it is only going to be a question of time before current security countermeasures simply don’t work anymore.

More information on the TrustDefender Intelligence Suite can be found on the website at <http://www.trustdefender.com> and more information on the TrustDefender Labs in-depth report can be found on the blog at <http://www.trustdefender.com/blog>.

-ENDS-

About TrustDefender

TrustDefender delivers security and fraud detection technology to protect enterprises and their customers at the device and transaction level from online fraud. This enables TrustDefender's customers in banking, Government, cloud application providers and online merchants to reduce the cost of online fraud. The company's combination of device and page fingerprinting technologies is a world first and instantly detects the source of any attempts to compromise an organisation's online defences. TrustDefender, founded in 2006, is headquartered in Sydney, Australia with offices in the UK, USA and Asia Pacific and can be found online at www.trustdefender.com