

29 October 2008

By: Lucian Constantin, Web News Editor

## [ICANN Terminates Accreditation of Notorious Malware Hosting Domain Registrar EstDomains](#)



*Approximately 281,000 domains registered through EstDomains will be transferred to another registrar*

EstDomains loses  
ICANN accreditation  
EstDomains Inc.

The Estonian-based domain registrar EstDomains was outed a long time ago by numerous security groups for providing domain registration services to cyber-criminals. An [official letter](#) sent a few days ago by Stacy K. Burnette, Director of Contractual Compliance at ICANN, informs the President of EstDomains Inc., Vladimir Tsastsin, that the company's accreditation as a registrar is being terminated.

The EstDomain company was founded in Tartu, the second largest Estonian city, but it has also been registered as a company in Delaware, US. In a [report](#) from KnujOn regarding EstDomain's activity, it is noted that "Delaware is a tiny state that earns its keep by being very business-friendly. Typically, any business incorporated in Delaware is not actually there". This prompted several security professionals to question the ICANN practices of accrediting companies that don't really exist where they were incorporated. Stacy Burnette, responded at that time that ICANN was satisfied with the fact that the registrars were only incorporated in the location listed in their accreditation application.

EstDomains became well known during the past several years for providing domain registration services to various cyber-criminal groups, like the infamous Russian Business Network (RBN), which use the domains in a wide array of cyber-scams and online illegal activities. Some of the domains are used for setting up fake pharmacies used in spam campaigns, others promote rogue applications that are in fact malware, such as Antivirus 2008. A high percentage of the illegal adult content websites are also set up on domains registered through EstDomains.

According to local media reports and official sources in Estonia, Vladimir Tsastsin, the President of EstDomains, was convicted by an Estonian court in February this year to three years in prison for credit card fraud, document forgery, and money laundering. This is also the official reason for which ICANN terminated the company's accreditation as a domain registrar. According to the Section 5.3 of the Registrar Accreditation Agreement (RAA), ICANN can cancel the agreement if "any officer or director of Registrar is convicted of a felony or of a misdemeanor related to financial activities, or is judged by a court to have committed fraud or breach of fiduciary duty [...]; provided, such officer or director is not removed in such circumstances".

According to Stacy Burnette's notification, ICANN received records from Estonia Court that confirm Mr. Tsastsin's conviction at the beginning of this year, but has not received any notification from EstDomains regarding his removal from the position of President. In the opinion of a local journalist, even though Vladimir Tsastsin might still legally be the President of EstDomains, the company has been under the control of the Russian mafia for a long time.

The official e-mail also informs that the approximately 281,000 domains currently sponsored by EstDomains will be transferred to another accredited registrar and that EstDomains has the right to suggest the transfer recipient by 6 November 2008. There is still no clarification whether this decision will remain final or not even if EstDomains eventually sends

documents showing the removal of Vladimir Tsastsin from any administrative position.

This is a significant blow for cyber-criminals and spam gangs and comes after not long ago the number one malware hosting company [Intercage](#) (Atrivo) was depeered by all its uplink providers and was forced to shut down the business. Security experts hope that during the domains transfer, ICANN will take the time to analyze the domains and suspend the ones connected to illegal activities.