

27 September 2008

By: Lucian Constantin, Web News Editor



Intercage is offline again.
Intercage, Inc.

[Lights Out at Intercage - Atrivo, Again](#)

The Intercage depeering whack-a-mole game continues

Only a few days after the UnitedLayer transit provider accepted to strike a peering deal with Intercage, under certain costly conditions, the ISP decided to pull the plug. This is the second time in one week that the infamous malware hosting company finds itself no longer reachable on the Internet.

We have been tracking the whole Intercage - Atrivo story for some time now, but for our readers who haven't followed up all the articles, here is some background information. Intercage, also known as Atrivo in the past, used to offer hosting solutions to the well known cybercriminal group going by the name of the Russian Business Network (RBN). After RBN disbanded in smaller groups and went underground, Atrivo changed its name to Intercage, but kept offering hosting solutions to various groups involved in illegal activities.

This prompted several recent [research papers](#) and reports from security groups showing the extent of malicious files and websites hosted by Intercage or its partners. One such report in particular written by several security researchers, which is referred to as [the HostExploit report](#), is credited with being responsible for creating a media frenzy and raising a virtual lynch mob aimed towards Intercage.

The bad publicity forced Intercage's uplink providers to [terminate their contracts](#) with the San Francisco company. Their first save from going offline came from an ISP called Pacific Internet Exchange (PIE), owned by a friend of Intercage founder and CEO Emil Kacpersky. Following pressure from security groups like Spamhaus, which blacklisted over 1,000 of their IPs, and their own customers, who threatened to leave, [PIE depeered Intercage](#) only after a few days, thus leaving their servers unreachable on the Internet.

Emil Kacpersky moved rapidly and convinced another ISP, UnitedLayer, to take them on board after only 72 hours of downtime. In order to secure this deal, [Intercage had to pay big time](#) by terminating their hosting contract with Esthost, the Estonian hosting company that was considered the biggest source of illegal activity on their network. According to Emil Kacpersky, however, Esthost also amounted for 25% - 50% of Intercage's revenue.

Along with this change, UnitedLayer asked that Intercage set up a functional and responsible ticket-based abuse reporting system and also warned them that they would not hesitate to pull the plug if the company violated the ISPs terms of service. "We have said very unequivocally to Emil that when and if factual evidence is provided to us that puts him in violation of our AUP... then we will terminate them like we would any other client," said UnitedLayer COO, Richard Donaldson at that time.

Soon after, Global Crossing, the first of Intercage's three original ISPs to terminate their arrangement, expressed their concern over this move. "It has come to our attention that United Layer is now routing traffic for Intercage (AS 27595) over the Global Crossing network," said an e-mail sent to UnitedLayer earlier this week. "Intercage was removed from our network for violating our acceptable use policy, and is not welcome to return under any circumstance," added Andrew Ramsey, Global Crossing's manager of information security operations, in the same e-mail.

UnitedLayer, which have peering arrangements with Global Crossing, strongly held their position and refused to take any action as a result of the e-mail. This prompted Global Crossing to set up IP filters on their own network, thus rendering 75% of the websites hosted by InterCage unreachable. This was followed by numerous well documented abuse reports sent to UnitedLayer, which prompted them to reconsider and terminate the contract with InterCage. Richard Donaldson commented for [The Register](#) that in his opinion InterCage was legitimately trying to reform but that "there was just too much to do. In light of that, it was safer to keep them off."

Some professionals have expressed their concern that even if the major hub of cybercrime activity in the US, InterCage, goes down, their questionable clients and partners will just move somewhere else. This idea is backed up by the fact that Esthost and Estdomains have already been back online for some time now, while InterCage is still struggling. What's even more interesting is that their new providers, as reported by [Sandi Hardmeier](#), also have indirect peering with Global Crossing; ZAO Petersburg Transit Telecom (PTT) (AS31353) - upstream from ASN-SPBNIT OJSC North-West Telecom Autonomous System (AS8997) - upstream from RETN-AS (AS9002) - upstream from GBLX Global Crossing Ltd. (AS3549). Donaldson noted that "Esthost is traversing Global Crossing's network as we speak and everybody else's, for that matter."

Mr. Donaldson also drew a pertinent conclusion regarding the consequences of this InterCage ostracizing story - "All you've done is force Esthost go more underground and become less visible, less containable and less capable of even being approached by law enforcement. So the community can certainly cheer that they've in essence targeted this company, but the root of the problem has not been fixed."