# Case Study Ultrascan-AGI Anti Corporate ID Theft Program

**Cyber-Crime Targeting a Multi National Company (real name changed in to MNC)**
Over the last three years we detected an exponential increase in the volume of online traffic by cybercriminals using the name of the MNC in Advance Fee Fraud (AFF) schemes. The inherent openness and anonymity of the internet are creating unprecedented challenges for the Company. Crimes of fraud, brand abuse and unauthorized use of MNC intellectual property have moved online and are increasingly dangerous to the reputation of all international institutions. The Company trademarks, logo, information and both the collective and individual identities of the Company are actively stolen by cybercriminals and used to conduct criminal activity on-line. ***While there has been no financial loss to the Company, there has been a degradation of the reputation and image of the Company, which is often perceived to be part of the criminal network conducting this cyber-crime.***

Victims of this billion dollar a year industry blame the real institution which is used by criminals to conduct their scams. The online reputations of all institutions have all been jeopardized by these organized gangs of cyber-criminals. The Company is a victim of AFF, but is now taking action to protect itself from such criminal activities and MNC fully intend to pursue these criminals with the assistance of international and local law enforcement authorities.
The initial problem within MNC was to determine which organization would handle these sensitive issues. This problem crosses several key domains; strategic security, fraud, public relations and IT security. As this particular problem does not physically cause any monetary loss, it does not necessarily breach the benchmarks required to fall under the domain of an anti-Fraud organization. For the MNC it was ultimately the Company's Security Unit, which deals with both strategic and physical security; that took on the role of defining the problem and devising solutions. Over the last year our Security Unit has become our subject matter experts on advance fee fraud and has achieved quick results by using the broader definition of "cyber crime" The Company's Security Unit has developed several key programs to combat this criminal activity targeting the Company with three components; EDUCATION, DISRUPTION and PROSECUTION.

EDUCATION
The Intellectual Property Protection initiative is a confidential and sensitive security program designed to provide a long term methodology using Ultrascan-AGI focused specifically on protecting the Company from all forms of identity theft and cyber-crime. This is a very specialized domain, and outsourcing several key components of the program to Ultrascan-AGI that focus on this issue alone has provided quick results. The first decision was a difficult one; does the Company as an institution want to "come out of the closet" and expose the fact that we have this problem? MNC is in fact the first institution to come forward and admit publicly that this is a problem. In order to increase our global impact in the education domain we joined an alliance

DISRUPTION
This phase of the program consists of an outsourced pro-active Anti corporate identity theft package that focuses on determining the identities, locations and tactics of the key cyber-crime perpetrators using the Company name, logo, trade mark and the names of Company employees. This is being done by cyber-crime specialists of Ultrascan-AGI located at a remote site, using an online "filter" system comprised of "points of reception" designed to capture all online activity using the name of the Company. Ultrascan-AGI's 419unit

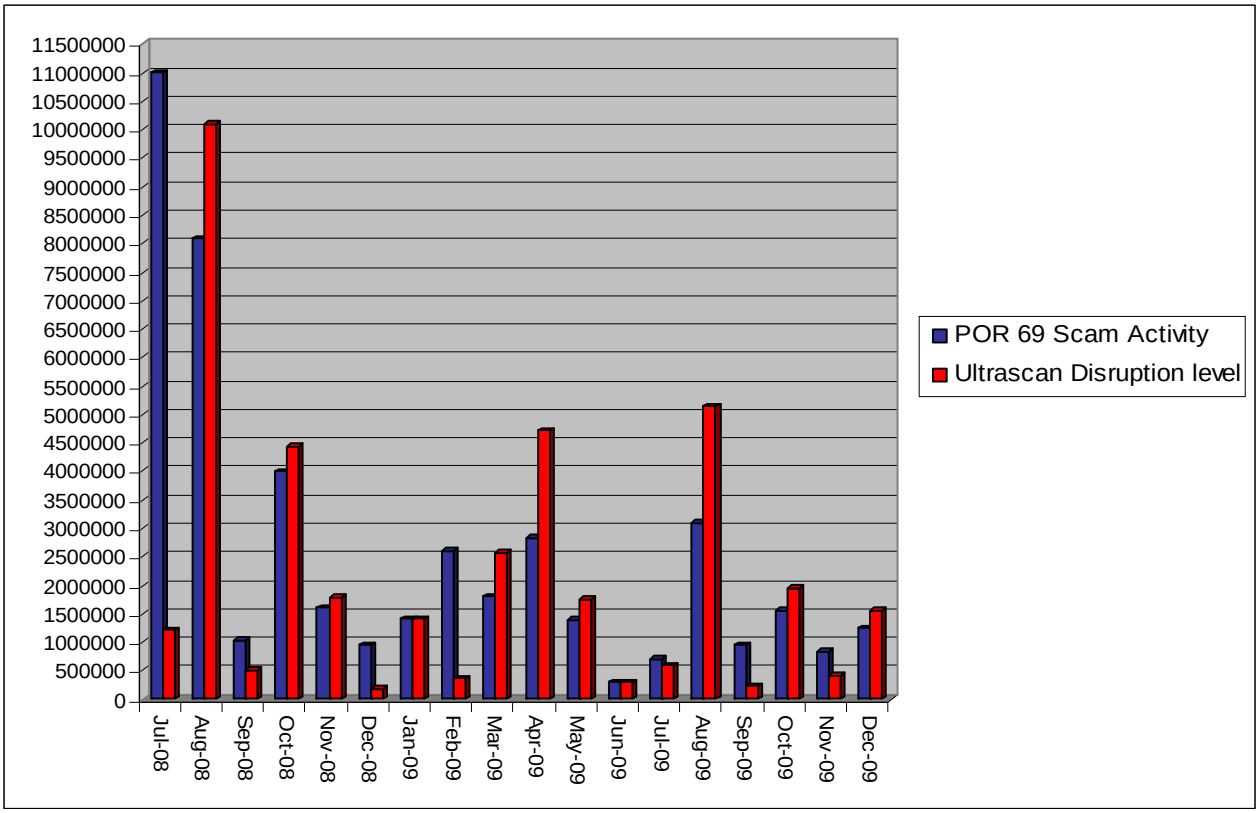
Ultrascan AGI
Amsterdam
The Netherlands
info@ultrascan-agi.com
Tel: +31 20 80 80 335

operates from a secure facility that can not be traced back to the MNC. The AFF points of reception are located in 69 countries across the globe and they automatically answer all Company related fraud proposals via email and phone/fax in order to collect more details about the perpetrators behind the proposals. These filters are fine tuned to ensure optimal reception, response and tracking. ***This honey pot program has been successful in identifying the "online" identities of the key perpetrators of MNC related cyber-crime and has started to create a "fear factor" which makes cyber-criminals wary of using the Company trademark for criminal activities.***

A recognizable trend is a change in the focal point used by cyber-criminals conducting AFF on two continents. The cyber-criminals are moving away from using the identity of MNC and are now using "a competitor" as their false online identity. Approximately 150 fake websites using the "the competitor brand" were identified.

***Since we started the program there has been a significant decrease in the number of AFF online activities using the name of the Company, the official logo of the Company, the name of Company staff members.***

The key websites supporting cyber-criminals using the Company were located and shut down, one particular website was operating from Cotonou, Benin with a convincing pirated MNC web site that including a fake board of directors. Ultrascan-AGI also shut down multiple false MNC web sites in South Africa. Ultrascan-AGI expects that the criminals will re-establish this site again somewhere in West Africa or China, but MNC now have the capability to detect, monitor, disrupt and quickly shut down such activities to ensure they no longer use the identity of the Company.

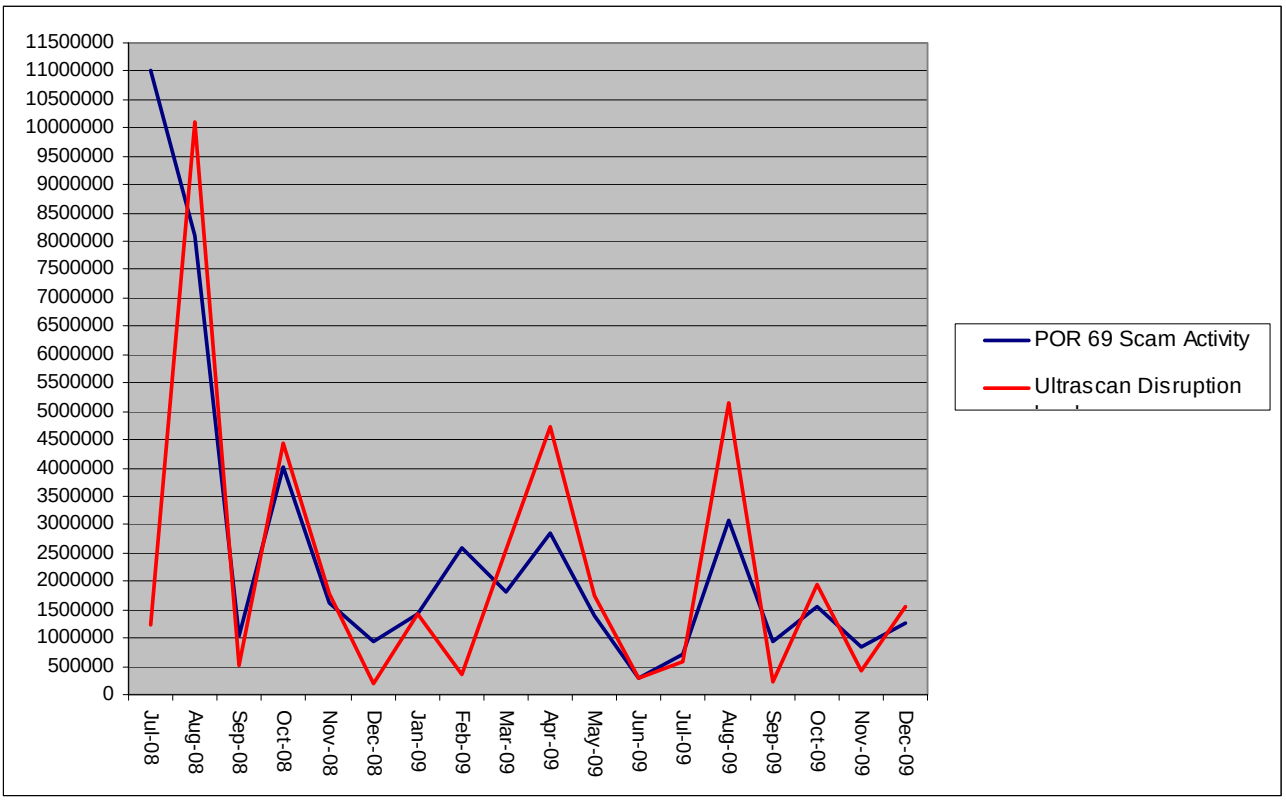



Ultrascan AGI
Amsterdam
The Netherlands
info@ultrascan-agi.com
Tel: +31 20 80 80 336

PROSECUTION

Currently, Ultrascan-AGI is simultaneously investigating 8 different AFF scam proposals using the name of the MNC in 8 different countries; Benin, South Africa, Czech, Nigeria, Netherlands, USA, England, and Australia. Ultrascan-AGI identifies the perpetrators behind these scams in order to trace and locate the individuals conducting these crimes. Then, Ultrascan-AGI collects evidence, which includes registration of conversations, cyber-forensics, and on some occasions meetings with the victims in order to get detailed information on the criminals. This evidence is passed to local authorities as appropriate for further investigation and prosecution. MNC have worked closely with the Nigerian EFCC in this role, however the lack of investigative capacity, laws, and prosecutorial will of many African is a serious problem. Ultrascan-AGI intend to assist African law enforcement entities in developing a stronger capacity to fight cyber crime, as we have clearly noted a trend for the criminals to move into countries that have weaker judicial capabilities.

MNC is still in the early stages of this project and will continue to look for partners willing to join us in this endeavour; there remain millions of emails and cyber-scams going out daily using the name of the Company. It is expected that the cyber-criminals will continue to adapt and change their tactics against the MNC; however MNC is now in a position to monitor and exert some measure of control over the criminal use of our trademark, through a proactive program of education, disruption and prosecution.




Amsterdam
28 January , 2010

Ultrascan AGI
Amsterdam
The Netherlands
info@ultrascan-agi.com
Tel: +31 20 80 80 336