Turin, Italy, July 19th, 2010

PRESS RELEASE "VULNERABILITIES IN ATM ENVIRONMENTS"

Following the recently published news appeared in the international press and on some blogs in which the cancellation of the planned speech of Mr. Chiesa entitled "3rd Generation ATM frauds" within the event Hack in the Box EU[1] Amsterdam on 2 July 2010 was due to alleged threats by an undefined vendor of ATM systems, which are reported below,

- http://www.bytemods.com/news/201/hacker-forced-to-cancel-hitb-presentation-due-to-legal-threats-by-atm-vendors
- http://news.softpedia.com/news/Security-Expert-Pulls-Presentation-After-Legal-Threats-146223.shtml
- http://www.heise.de/newsticker/meldung/Erneut-Sicherheitsexperte-wegen-Vortrag-mit-Festnahme-bedroht-1034298.html
- http://www.theregister.co.uk/2010/07/06/atm_security_talk_pulled/

@ Mediaservice.net S.r.l. with unique shareholder, in the person of his CEO Daniele Poma and Raoul Chiesa affirm that:

- No manufacturer or system integrator of ATM nor financial and banking institutions have never threatened Mr. Chiesa or the company @ Mediaservice.net, which makes of professional ethics one of its major strengths;
- @ Mediaservice.net and Mr. Chiesa are not aware of the reasons why those *gossips*, completely unfounded, have begun.

Mr. Chiesa has canceled his planned speech at HITB EU for two main reasons:

- Ethical issues, for which the team's search @ Mediaservice.net decided a year and a half ago not now make public disclosure of vulnerabilities which have emerged, but just to closed sector specific associations;
- Logistical issues, which saw him busy on the evening of July 2 near Rome.

The research team on ATM security has already presented part of his research, both in the document ENISA[2] "ATM Crime: overview of the European situation and golden rules on how to Avoid It" (August 2009[3]) and, in deeper detail and rigorously closed doors, at the emergency center for cyber attacks managed by ABI Lab[4], on September 11th 2009.

[1] HITB EU: https://conference.hackinthebox.org/hitbsecconf2010ams/
[2] ENISA: European Network & Information Security Agency – http://www.enisa.europa.eu
[3] http://www.enisa.europa.eu/act/ar/deliverables/2009/atmcrime/?searchterm=atm
[4] Italian Banks Association (ABI) Laboratory (Lab).

Headquarter and offices: Via San Bernardino 17 - 10141 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
http://www.mediaservice.net - info@mediaservice.net

Following the insufficient measures undertaken in these areas to mitigate the vulnerabilities, the team maintained its position oriented to a "responsible disclosure", well aware of the possible economic and social crimes against the widespread knowledge of vulnerabilities could potentially cause.

The priority of @ Mediaservice.net and its researchers is in fact to inform and warn the parties that can prevent possible and dramatic mass, manual or automated attacks, which would result in the theft of huge sums of money through crime patterns that have already started to emerge recently, as the tampering of software in Ukrainians ATM proves performed by organized crime.

Nowadays, high-level vulnerabilities identified by @ Mediaservice.net's research team sum up to a total of fifteen, grouped into "common errors" (12) and "complex attacks" (3, PoC[5]). In addition, the team has identified six areas for further research, classified as "theoretical vulnerabilities".

We take this opportunity to remind readers that operate in the financial sector, especially in the ATM world, that @ Mediaservice.net's team is available to provide its support to detect and remove the vulnerabilities in these systems.

Any communication to the topic can be forwarded to the research team, reachable at the email address atm@mediaservice.net

About @ Mediaservice.net

@ Mediaservice.net S.r.l. is a Security Advisory Company actively present in the IT Security market since more than 10 years. Our Mission is to verify and improve the security posture of IT infrastructures and services on which our Clients' core business depends.

@ Mediaservice.net provides strategic and independent security services and professional consulting, tailored for the protection of global information in the age of Total Telecommunications Convergence, in which we are entering both as consumers and as developers and suppliers. The experience and professionalism of employees make our company a leader in the Proactive Security, Process security, and Training sectors.

For further information: http://www.mediaservice.net

[5] PoC: Proof-of-Concept, meaning the vulnerabilities have been successfully tested.