

## MITA PRESS RELEASE

### EMBASSIES SERVER SUFFERS CYBER ATTACK

---

Yesterday, 4<sup>th</sup> March 2009, the Information Security and Risk Management Department of the Malta IT Agency (MITA) identified unauthorised software on a server used for the storage of user credentials of personnel in Embassies of Malta abroad. This unauthorised software was identified by security monitoring and alerting tools which have been recently implemented by the Agency within an overall framework of security tightening.

Immediately upon detection MITA requested its US-based IT security advisory firm to provide it with an assessment of the potential breach based on the evidence collected by MITA. The preliminary analysis indicated that the said software had the potential to extract user names and passwords on the Embassies server only. Analysis and assessments of any evidence of similar attacks on other servers has been carried out with no such evidence resulting. In the meantime, more assessments are being carried out.

Although MITA has no evidence that any breach had occurred, throughout last night, to ensure absolute safety of the integrity of data in its responsibility, MITA carried out an operation which entailed the disabling of all accounts of users on the said 'Embassies Server' and users occupying sensitive positions. Although currently there is no indication whatsoever of a breach on the Servers hosting the user credentials of the latter group (i.e. sensitive positions), this preventive measure ensured that these users are not exposed to unnecessary risks. The rest of the users will be requested to change their password credentials to close out even the most remote risk.

The detection of this attempted breach and the neutralization of its potential impact was possible following a series of investments made in the recent months by MITA, including the deployment of intrusion prevention systems, tighter policies and stronger password storage technology. As a direct result of these measures, the length of time required for a perpetrator to decrypt a password is significant and well beyond the short period of time within which the said accounts may have been possibly exposed.

In the meantime, MITA is currently communicating the state of play to all the IT services users in Government and is working through Chief Information Officers in Ministries and public sector entities to ensure that users are made aware both of the incident and also of the preventive action taken by MITA to safeguard their information security.

In the meantime the concerned Server has been isolated and the Police have been informed.

**05.03.2009**