

From: "Marco Valleri" <[REDACTED]@hackingteam.com>
To: [cod.\[REDACTED\]@sysleave.org](mailto:cod.[REDACTED]@sysleave.org)
[wteam.\[REDACTED\]@hackingteam.it](mailto:wteam.[REDACTED]@hackingteam.it)
CC:
Date: 10/10/2012 23:28:27
Subject: Re: altro articolo

Credo si riferisca al fatto che il sample era un exploit che scaricava il second stage dal nostro vecchio server demo...

From: cod [REDACTED]@sysleave.org]
Sent: Thursday, October 11, 2012 12:21 AM
To: <wteam@hackingteam.it>
Subject: altro articolo

http://www.slate.com/blogs/future_tense/2012/10/10/ahmed_mansoor_uae_activst_allegedly_tricked_by_phoney_wikileaks_into_downloading.html

il dubbio che mi viene da questo è il "it was also linked" che non riesco a comprendere se intendono che citizen s'è trovata su vt anche questo o se anche questo gli è arrivato...

A fake .doc file contained in the email masked a trojan with some of the same elements as the version found in Morocco. (The trojan depends on a security flaw within Microsoft Office software, a kind of vulnerability often described by hackers as a "zero-day exploit.") **It was also linked, Citizen Lab found, to the hackingteam.it** domain name. As of the time of publication, Hacking Team had not responded to my request for comment.