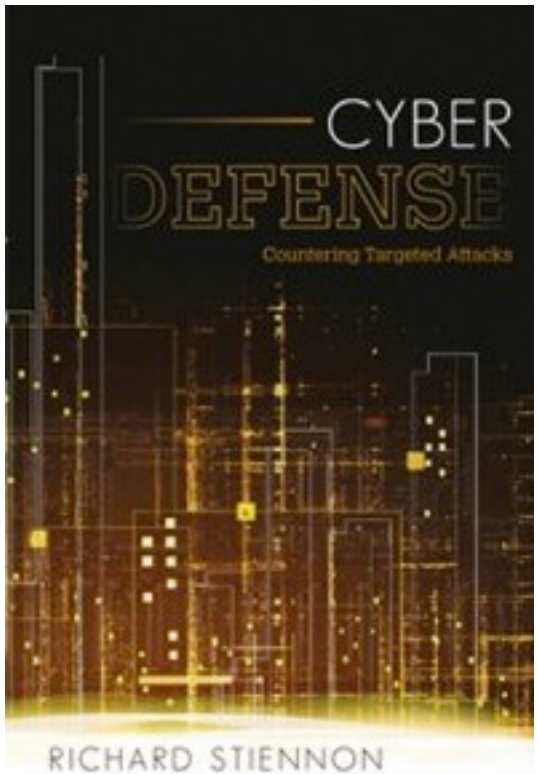
The Weaponization of Software

Richard Stiennon
Chief Research Analyst
IT-Harvest

Blog: ThreatChaos.com
twitter.com/stiennon



Blog: www.ThreatChaos.com

twitter.com/cyberwar

IT-Harvest

Software as weapon, why?

- Intelligence gathering
- Infiltration
- Disruption
- Sabotage
- Change the balance of power

Using the web to distribute software weapons

NASDAQ OMX | Directors Desk

▪ Our Solution ▪ Advantage ▪ Security ▪ Company

Our Solution

A Complete Solution for Board Effectiveness

Directors Desk offers a comprehensive solution designed to improve board communications and effectiveness while relieving corporate executives of the paperwork and time involved in keeping boards informed.

In addition, we offer customized tools to meet the unique needs of each client and each director. Completely secure in a fully hosted environment, our solutions are very easy to use--appropriate for board members with varying levels of IT sophistication.

Collaboration Tools

Calendar & Event Management

The Jester’s shenanigans

@th3j35t3r
33llz ɐpıuɹɟ33b

www.albasrah.net - TANGO DOWN. Temporarily. For the continued distribution of jihadist instructional materials & propaganda.

31 May via XerXeS for Android V1.3 Favorite Retweet Reply

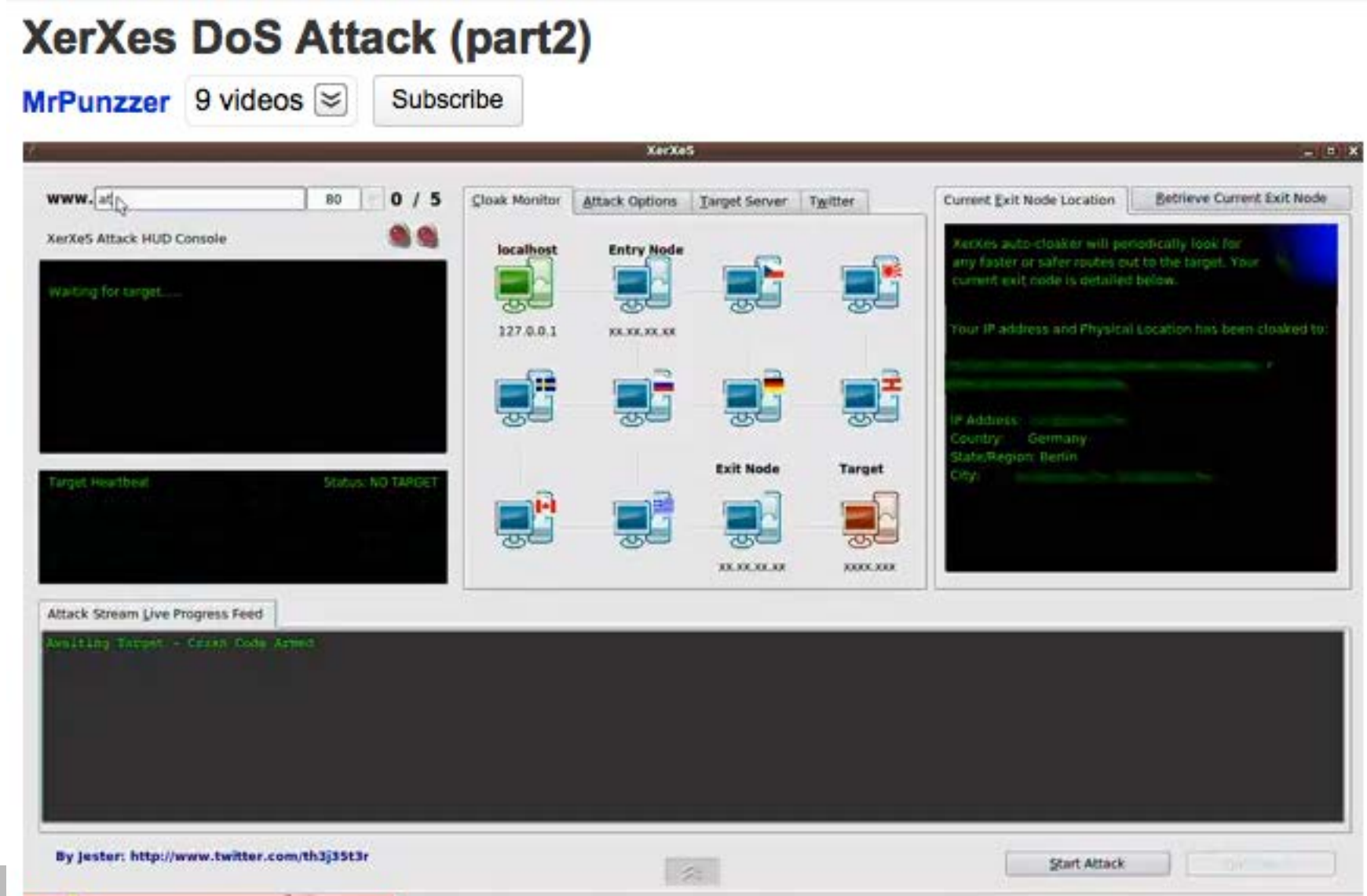
Objection!

By disrupting jihadi recruiting sites you could interfere with real counter terrorism activity.

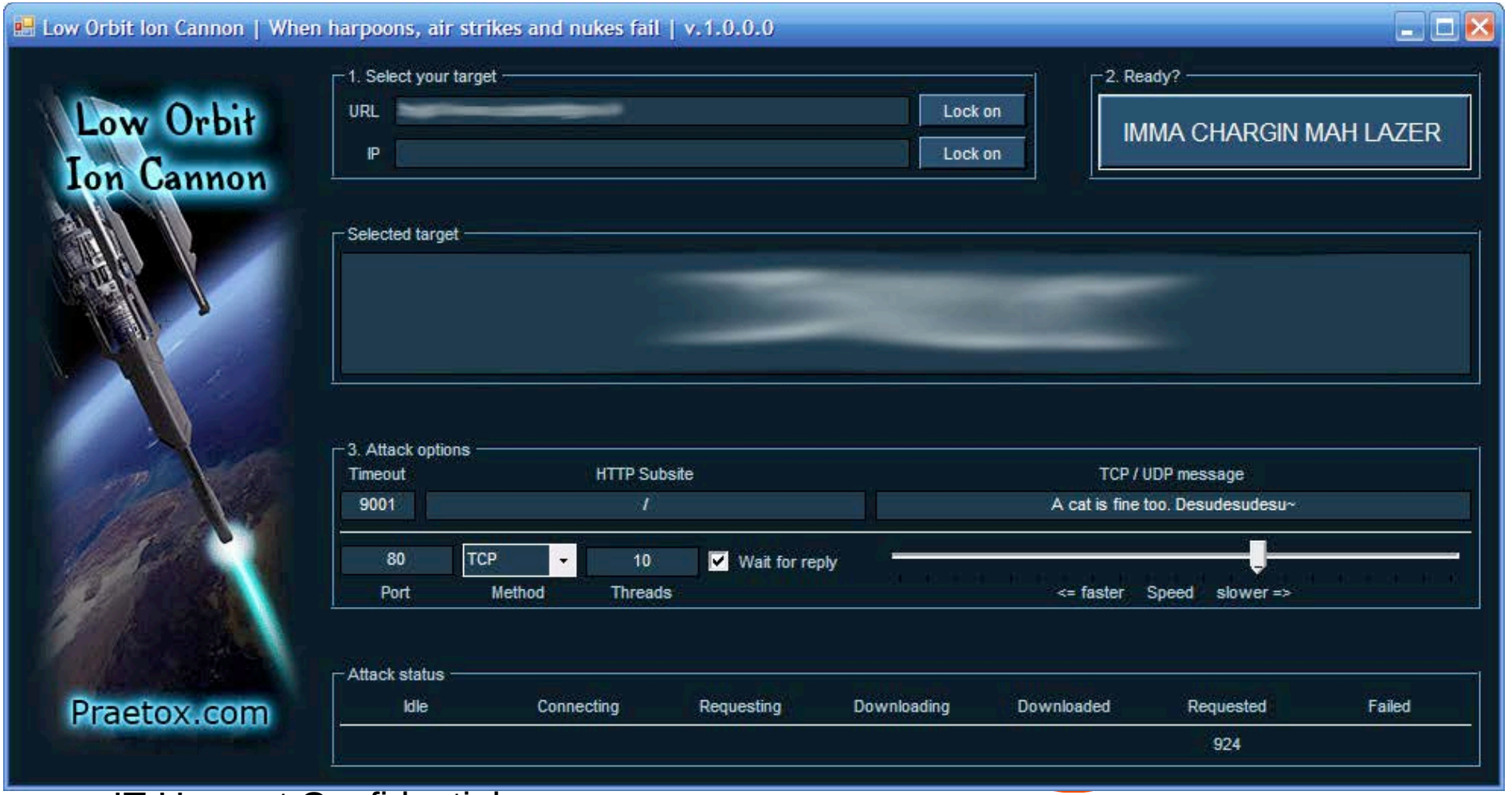
Are we doing that?

Hold that thought.

Advanced DoS weapon



Not so advanced DoS weapon



When powers collide

Jester takes down Wikileaks with XerXes

AnonOps targets Jester along with Master Card, PayPal, etc.

Jester distracts Anonymous to keep them off of other targets

LOIC replaced by remotely controlled botnet. DHN.zip

Jester replaces DHN.zip with infected file.

Jester wins on all counts.

Does disruption work? Or does it burn sources of intel?

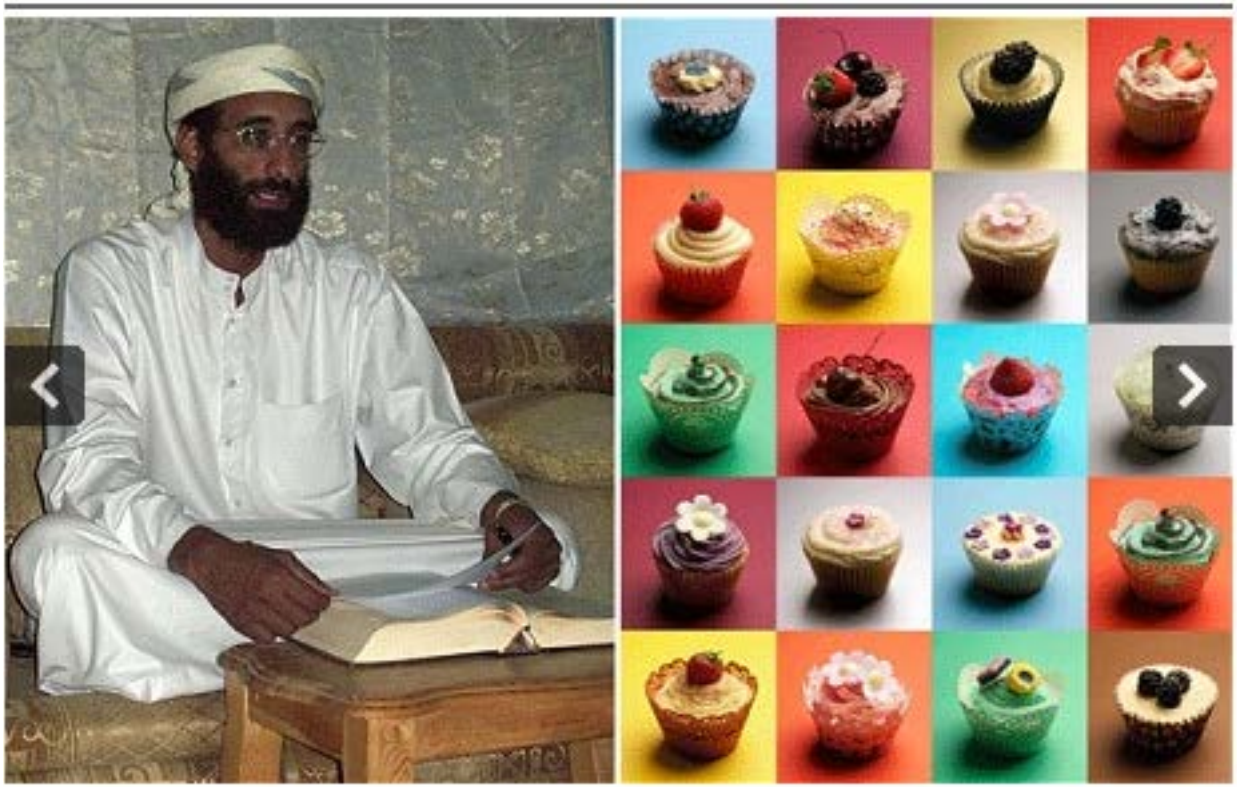


Image 1 of 2

IT-Harvest

Software updates: the pre-approved backdoor

- Think of the number of vendors you trust.
- Microsoft
- McAfee/Symantec
- Do you check their updates?
- Would it matter?

Athens 2004

ERICSSON

TAKING YOU FORWARD

Ericsson SPT 2700

A series of software updates turns on Lawful intercept function

104 diplomats and Olympic officials spied on

Engineer mysteriously commits suicide

IT-Harvest

A few defensive measures

Check your own code
Check your COTS code
Require signatures (and check them) from your suppliers
Test updates
Check what your users are seeing. Continuously!

A final scenario

If RSA can have their crown jewels stolen how can you be sure Microsoft's update servers and certificate authority are 100% secure???

An attacker would need access to those servers, and ....

a good amount of original source code.

You know where I am going with this.

Blog: www.threatchaos.com

email: richard@it-harvest.com

Twitter: twitter.com/cyberwar