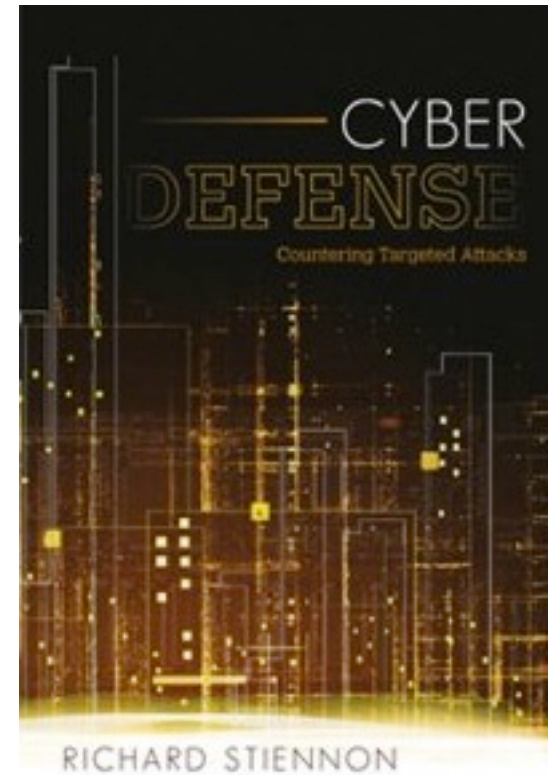


# The Weaponization of Software

Richard Stiennon  
Chief Research Analyst  
IT-Harvest

Blog: [ThreatChaos.com](http://ThreatChaos.com)  
[twitter.com/stiennon](https://twitter.com/stiennon)





Blog: [www.ThreatChaos.com](http://www.ThreatChaos.com)

[twitter.com/cyberwar](https://twitter.com/cyberwar)



# 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

33||z epinA.r33b

[www.albasrah.net](http://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

## XerXes DoS Attack (part2)

MrPunzzer

9 videos

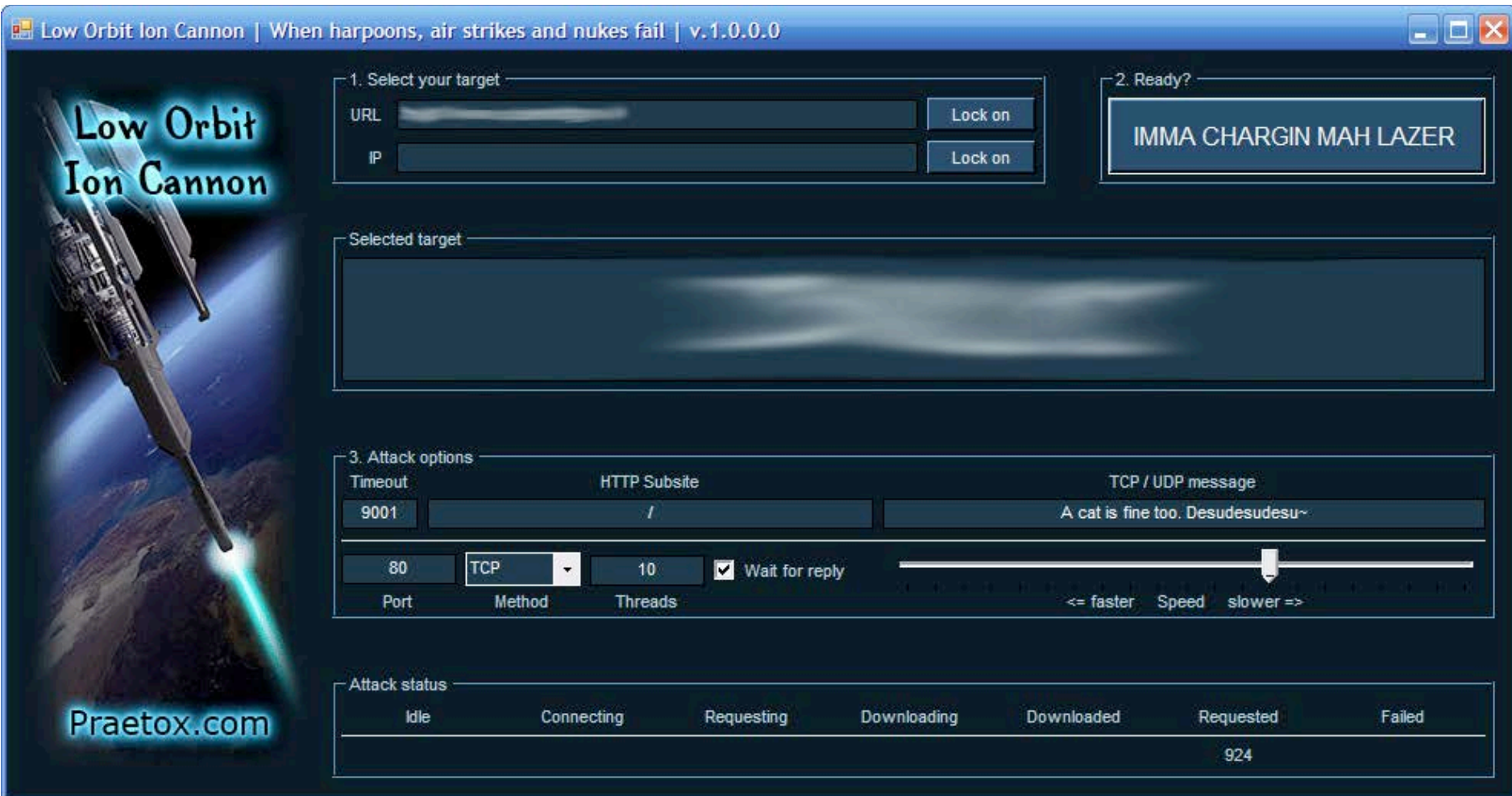
Subscribe

The screenshot displays the XerXes DoS Attack HUD Console interface. At the top, there is a search bar with "www." and a "BO" button, and a progress indicator "0 / 5". The main interface is divided into several sections:

- Left Panel:** Contains a "XerXes Attack HUD Console" window with a "Waiting for target..." message, a "Target Heartbeat" section showing "Status: NO TARGET", and an "Attack Stream Live Progress Feed" with the message "Awaiting Target - Cozen Code Armed".
- Central Panel:** Features a network diagram with nodes labeled "localhost" (IP: 127.0.0.1), "Entry Node" (IP: XX.XX.XX.XX), "Exit Node" (IP: XX.XX.XX.XX), and "Target" (IP: XXXX.XXX). The diagram shows a path from localhost through the Entry Node and Exit Node to the Target.
- Right Panel:** Titled "Current Exit Node Location", it contains a "Retrieve Current Exit Node" button and a text area stating: "XerXes auto-cloaker will periodically look for any faster or safer routes out to the target. Your current exit node is detailed below. Your IP address and Physical Location has been cloaked to: IP Address: Country: Germany State/Region: Berlin City:".

At the bottom of the interface, there is a "Start Attack" button and a "By jester: <http://www.twitter.com/th3j55t3r>" link.

# 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?

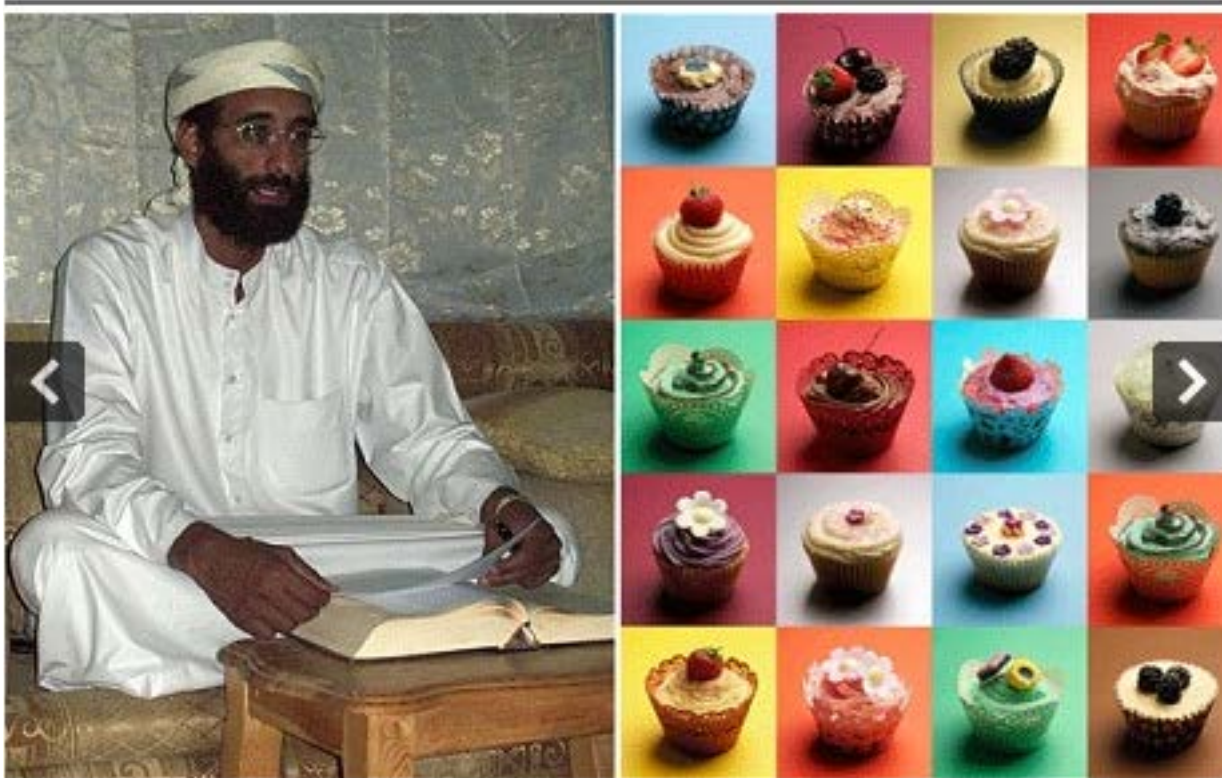


Image 1 of 2



# 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 SPT 2700

A series of software updates turns on  
Lawful intercept function

104 diplomats and Olympic officials  
spied on

Engineer mysteriously commits suicide



# 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](http://www.threatchaos.com)

email: [richard@it-harvest.com](mailto:richard@it-harvest.com)

[Twitter: twitter.com/cyberwar](https://twitter.com/cyberwar)

