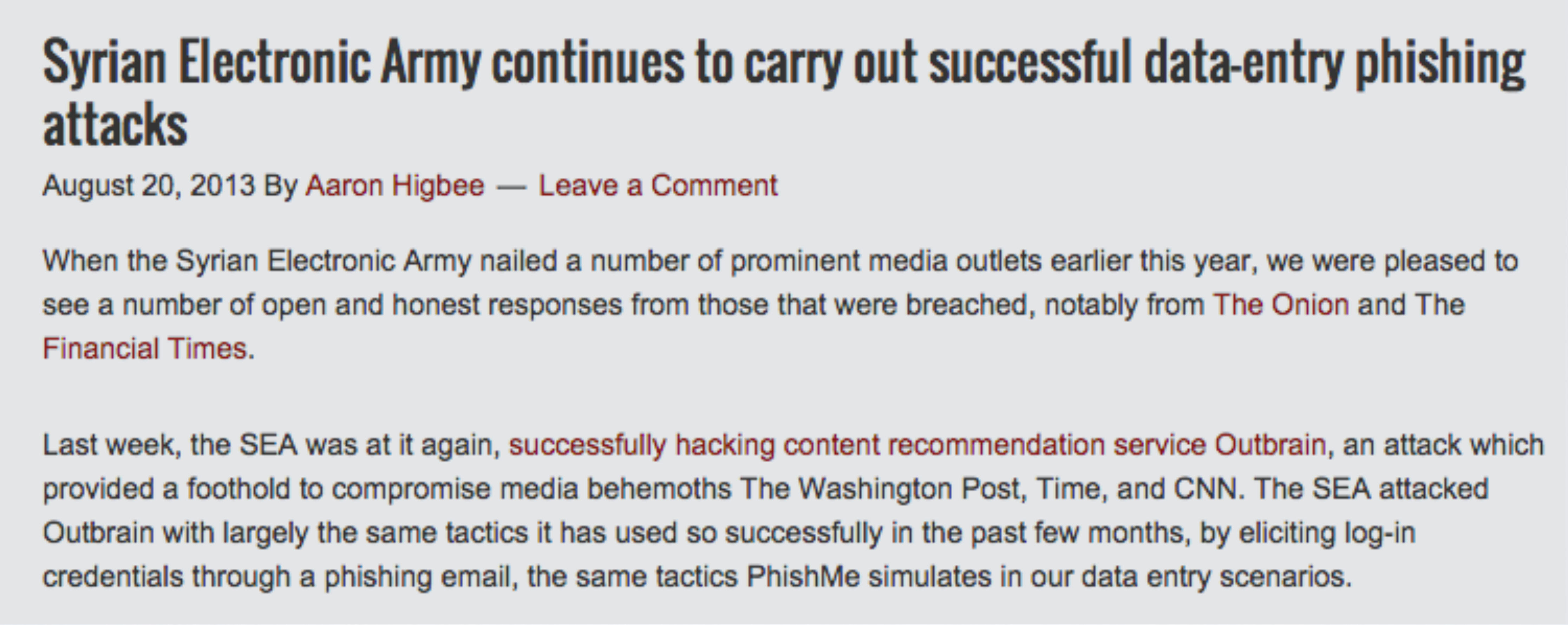
Phishing + Social Engineering = Spear Phishing



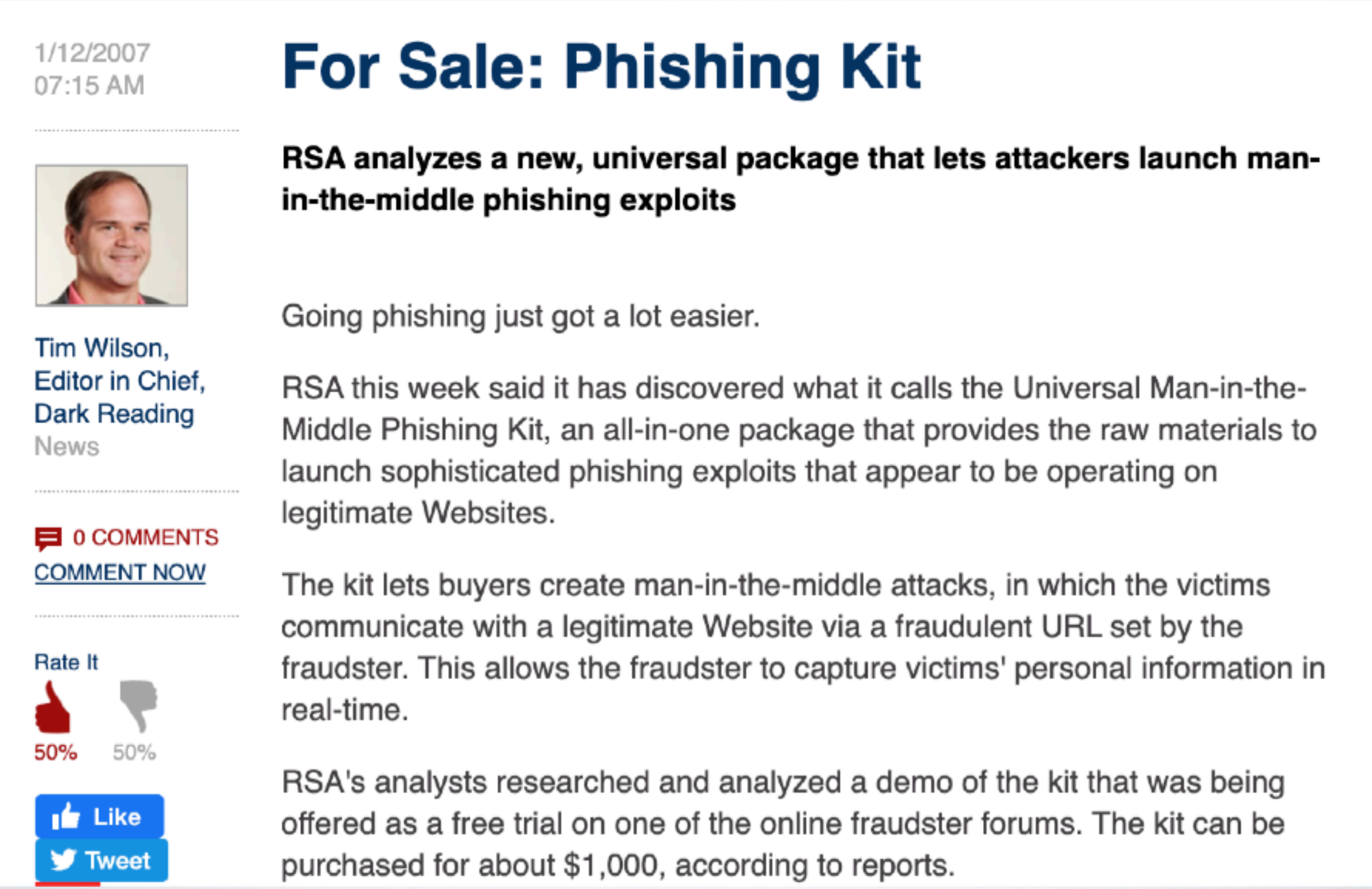
Syrian Electronic Army continues to carry out successful data-entry phishing attacks

August 20, 2013 By Aaron Higbee — Leave a Comment

When the Syrian Electronic Army nailed a number of prominent media outlets earlier this year, we were pleased to see a number of open and honest responses from those that were breached, notably from The Onion and The Financial Times.

Last week, the SEA was at it again, successfully hacking content recommendation service Outbrain, an attack which provided a foothold to compromise media behemoths The Washington Post, Time, and CNN. The SEA attacked Outbrain with largely the same tactics it has used so successfully in the past few months, by eliciting log-in credentials through a phishing email, the same tactics PhishMe simulates in our data entry scenarios.

Phishing as a service a.k.a phishing kit



1/12/2007
07:15 AM

Tim Wilson,
Editor in Chief,
Dark Reading
News

0 COMMENTS
COMMENT NOW

Rate It

For Sale: Phishing Kit

RSA analyzes a new, universal package that lets attackers launch man-in-the-middle phishing exploits

Going phishing just got a lot easier.

RSA this week said it has discovered what it calls the Universal Man-in-the-Middle Phishing Kit, an all-in-one package that provides the raw materials to launch sophisticated phishing exploits that appear to be operating on legitimate Websites.

The kit lets buyers create man-in-the-middle attacks, in which the victims communicate with a legitimate Website via a fraudulent URL set by the fraudster. This allows the fraudster to capture victims' personal information in real-time.

RSA's analysts researched and analyzed a demo of the kit that was being offered as a free trial on one of the online fraudster forums. The kit can be purchased for about $1,000, according to reports.