

**OUTBREAK NAME:**

## Waledac SMS Spy Spam

**OUTBREAK DATE:**

4-16-09

**Outbreak Details**

On April 16<sup>th</sup>, 2009, cyber-criminals started sending spam messages offering a free trial for an SMS spying application that purportedly allows the user to eavesdrop on another person's SMS messages. The website in the spam message has an executable file for the Waledac bot, in the form of a 30-day free trial download.

The spam campaign represents an escalation in coordination of criminal activity. This is the first instance of Conficker monetizing its botnet by providing a vehicle for secondary infections, specifically allowing Waledac to be downloaded on its hosts. This is also the first instance of spam being sent from the Conficker botnet. Given the success of Conficker in terms of self-preservation and propagation, Cisco believes that more botnets will employ best-practices for their own greater effectiveness.

**Outbreak Timeline**

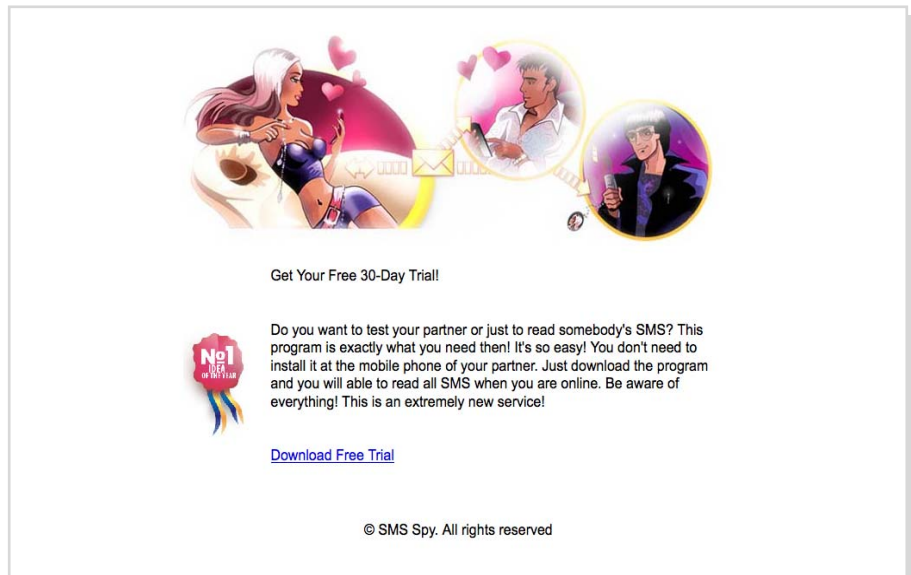
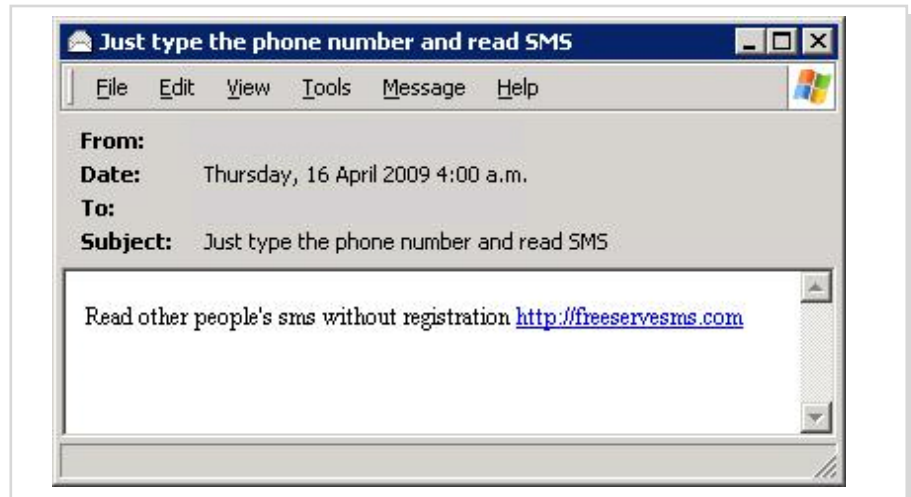
IronPort Anti-Spam blocked these messages within seconds of the spam campaign's start.

IronPort Web Reputation Filters blocked the websites advertised.

Cisco Botnet Traffic Filters identified and blocked the botnet activity.

**Summary.** IronPort Anti-Spam again protects customers from spam and phishing attacks launched from botnets. During the recent "Waledac SMS Spy" outbreak, IronPort Anti-Spam protected customers **within seconds** of the first message.

The level of sophistication and coordination of the Waledac attack from Conficker infected hosts represents the escalation of efforts employed by cyber-criminals. Cisco IronPort expects to see more best-practices in spam campaigns over the coming weeks and months.



**For more information** David T. Oro, Cisco Public Relations  
daoro@cisco.com 707-558-8585 Desk 415-885-9898 Mobile