



OUTBREAK NAME:

Fake Facebook Update Email Malware

OUTBREAK DATE:

01-20-2011

Outbreak Details

Starting on January 20th, 2011, cyber criminals sent threat messages leveraging Facebook's popularity.

By preying on users' security concerns, cybercriminals attempted to get users to open an attached zip file containing new password details. Once the attachment is opened, a malicious executable is run that infects the system with malware. The malware can disable the firewall, steal sensitive financial data (e.g. online banking login details), download additional components, and provide a hacker with the remote access to the compromised system. Connection attempts are also made to remote hosts: 124.217.248.229 and 91.217.162.99.

Cisco expects to see more threat messages taking advantage of Facebook's popularity to attract unsuspecting users.

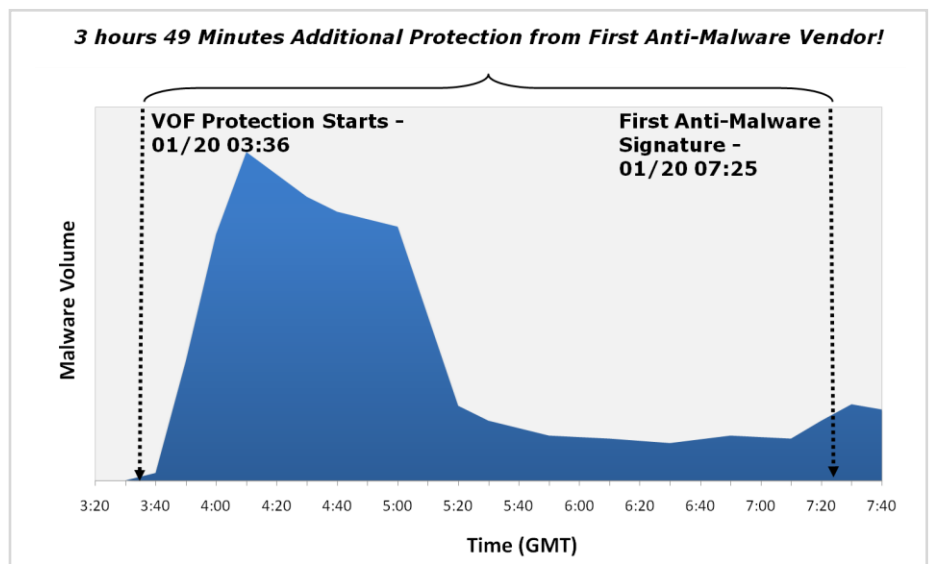
Outbreak Timeline

SUMMARY: **3 hours, 49 minutes** additional protection ahead of first anti-malware vendor.*

Cisco IronPort Virus Outbreak Filters on the Email Security solutions blocked these threats within seconds of the campaigns' start.

Cisco Web Security solutions blocked the connection attempts to the remote hosts.

Summary. Cisco IronPort again protects customers within the critical period between the first exploit of a virus outbreak and the release of an AV signature. During the recent Fake Facebook Update Email Malware outbreak, Cisco Virus Outbreak Filters and Web Reputation Services protected customers *within seconds* of the first threat messages and **3 hours and 49 minutes*** before the first major anti-malware vendor provided protection.



*Vendor signature times per AV-Test. Signature times from the following vendors: Sophos, Trend Micro, Symantec and McAfee. Generic signatures not included.