

April 2009



MX LOGIC THREAT Forecast AND REPORT

The monthly MX Logic® Threat Forecast and Report

is designed to provide IT leaders and messaging security professionals with information on recent and potential email and Web threats. The forecast is developed using current and historical data and trends, as well as expert analysis of real time spam and virus events monitored and assessed by the 24x7 MX Logic Threat Operations Center. To view the latest real-time data, visit www.mxlogic.com/threatforecast



April 2009 Threat Forecast

CONFICKER - FOOL ME TWICE, SHAME ON ME

Given all the recent media attention surrounding the Conficker botnet, it's not entirely surprising that nothing really happened on April 1st. However, spammers are a tricky bunch and know that the massive attention will subside and that users will eventually let their guards down again. But don't be fooled. With the April 15th US Tax Deadline and Easter Holiday fast approaching, it's very possible that Conficker could launch a large-scale attack in April. Keep your guard up.

KILLER EASTER BUNNIES

History has shown that like most holidays, Easter is a busy time for spammers. We expect to see the usual high-volumes of Easter-themed malicious messages this year, especially from holiday-loving spammers like the Waledac gang.

BULLS-EYE ON MICROSOFT'S IE 8

Microsoft recently launched a new version of its popular browser, touting Internet Explorer 8 as the safest browser ever. While we won't second-guess Microsoft's marketing prowess, we expect hackers to view this as a challenge and to begin looking for software vulnerabilities in the new browser as users of IE 7 look to upgrade.

SPAMMERS RUSH TO BEAT TAX DEADLINE

Tax-themed spam and phishing ploys have been unusually light to date. However, we do expect to see a rise in malicious messages related to tax returns, refunds, or stimulus checks as the deadline nears – and perhaps for another few weeks after that.





March 2009 Threat Report

As forecasted last month, spam volume continued its rapid comeback climb with the total number of spam messages increasing 34 percent between February and March. These are the highest spam volume levels

since the McColo shutdown late last year. Spam traffic as a percentage of all email traffic rose slightly, increasing from 83 percent in February to 84.8 percent in March.

Total Spam Volume

+34%
 From February



Spam Percentage

84.8%
 Up from 83% in Feb.



Top 6 Categories of Spam

1. Health
2. Offers
3. Education
4. Foreign Languge
5. Phishing

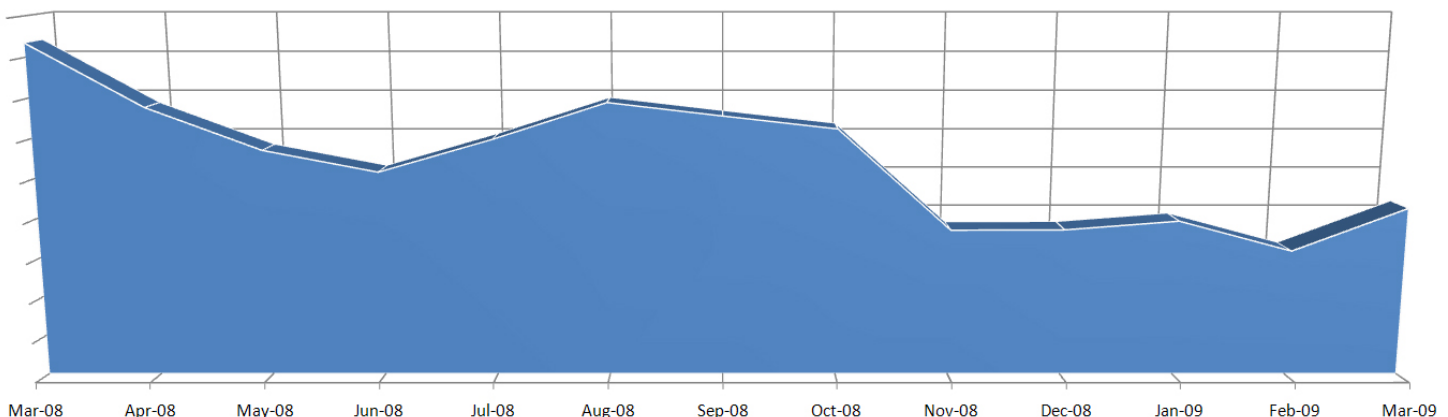
Top 5 Worms/Viruses

1. Troj/Inject-FS
(Delta eTicket)
2. Troj/Agent-JIV
(DHL Invoice)
3. Troj/Banloa-FR
(Delta eTicket)
4. Troj/Inject-FG
(UPS Tracking invoice)
5. Troj/Inject-FT
(UPS invoice)

Top 5 Spam Countries

1. United States
2. Brazil
3. Russian Federation
4. Ukraine
5. India

Historical Spam Levels

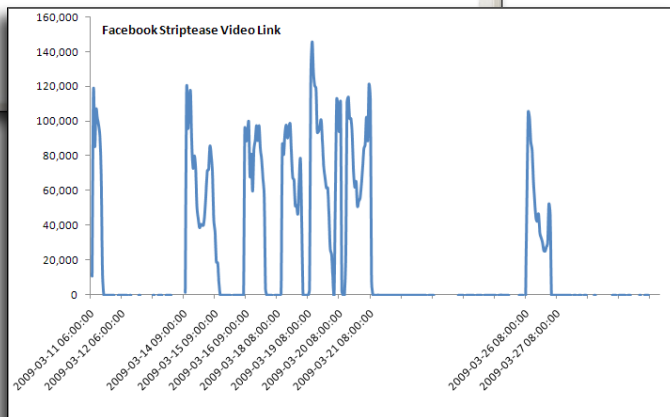
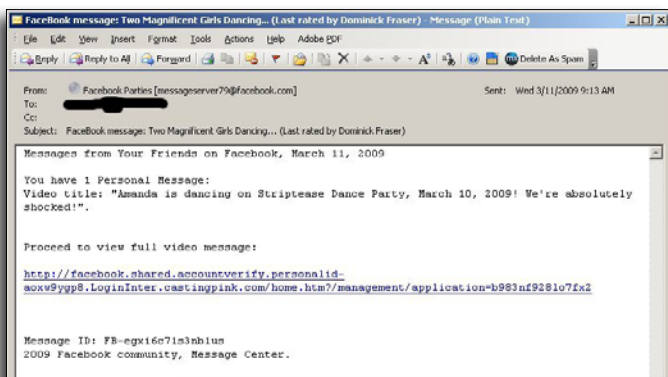
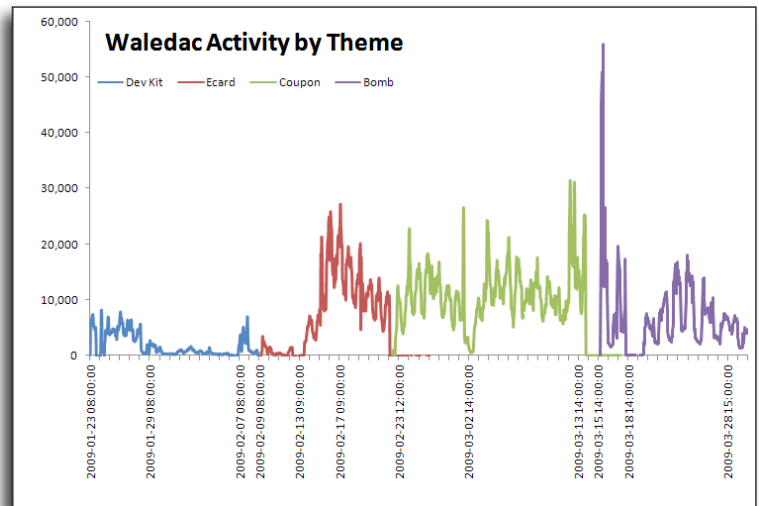




Most Prevalent Spam & Malicious Messages of the Month

Healthcare scams remained the most prevalent spam messages overall, although we did notice an increase of emails with only a single image in the body used to promote products from fraudulent pharmacies. In addition, the Waledac gang continued to make their presence felt in March, using a highly impactful bomb scare tactic. As in previous campaigns, Waledac used Geo-IP functionality, making the malicious message appear frighteningly more real since it localized the message to the email recipient.

eTickets and fake invoices also remained popular methods for infecting users with malware, as shown in the list of Top Worms/Viruses (see previous page). Because we aren't seeing a lot of variation in topics or themes (i.e., Messages disguised as email from DHL), we can infer that more effort is being placed on detection avoidance.



Social Networking Sites Used as Bait

As mentioned in previous reports, social networking sites are increasingly being used to lure people into downloading malicious content. One popular ploy in March claimed to be a message sent from facebook.com and classmates.com. The message purported to include a link to an "adult" video of a "friend" named Amanda. Of course, this was simply an attempt to trick users into downloading malicious malware.

We expect to see more and more of this in the future, although with some slight changes. These changes may come in the form of new social engineering tactics, or even changes in traffic volume, as we saw in March.



The Best “Worst” Spam of the Month

Leave it to **419 phishing scammers** to find new ways to raise the comedy bar. In a recent message intended to get people to traffic money for them, spammers sent a fake message from the “FBI Foreign Remittance Telegraphic Department”. What’s next, an official message from the FBI “Beeper” Department?



Anti-Terrorist And Monetary Crimes Division FBI Headquarters,
Washington, D.C.
Federal Bureau Of Investigation
J.Edgar Hoover Building
935 Pennsylvania Avenue, Nw Washington, D.C. 20535-0001

Attention Fund Beneficiary,

This is an official advice from the FBI Foreign Remittance Telegraphic Dept, It Has Come To Our Notice That The C.B.N Bank Nigeria District Has Released 15 Million Great British Pounds Sterling equivalent to 30 Million U.S Dollars Into Bank Of America In Your Name As The Beneficiary, By Inheritance Means.

