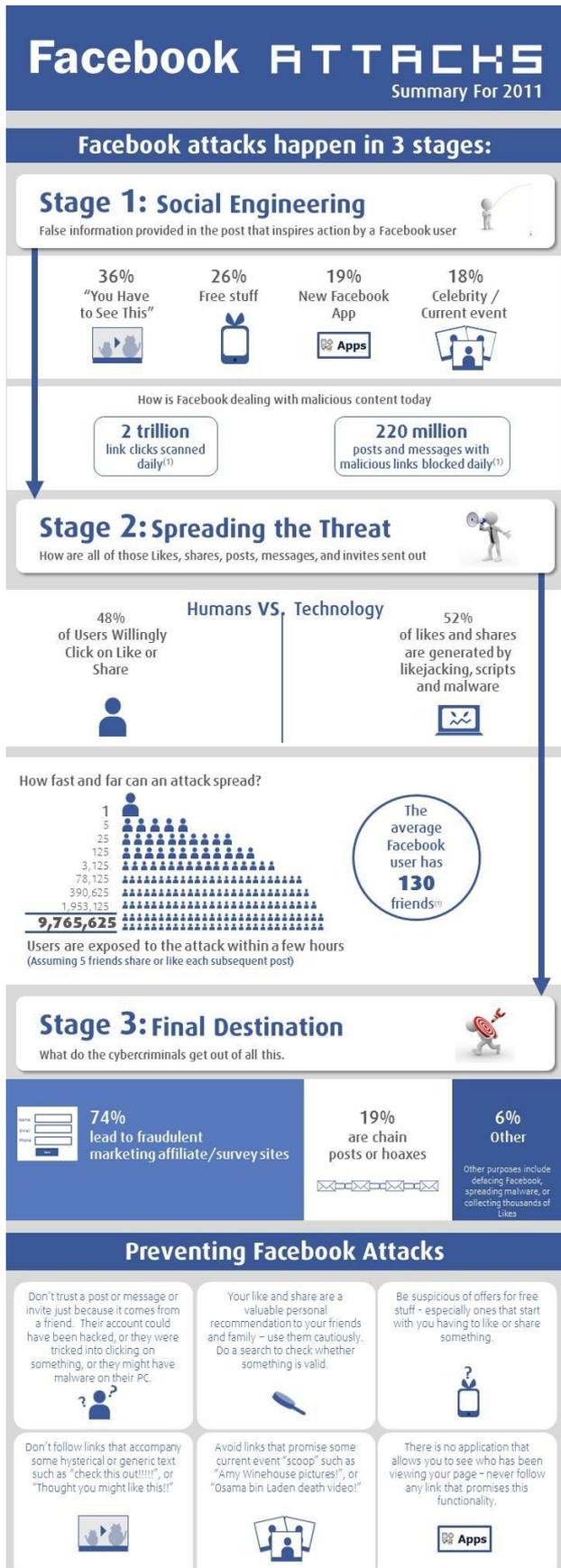


Majority of Facebook Attacks Feed Fraudulent Affiliate Marketing Sites, Says Commtouch Year-End Trend Report

January 2, 2012



Sunnyvale, Calif. (RPRN) 01/02/12 — Commtouch® (Nasdaq: CTCH) today published an in-depth analysis of 2011 Facebook attacks within its Internet Threats Trend Report, a year-end synopsis of Internet threats. The report and infographic present a comprehensive analysis of scores of malicious Facebook activities during the past year, as identified by Commtouch Labs.

Affiliate marketing sites are the final destination in three-fourths of all Facebook deceptions, according to the report. Visitors to these sites are induced to fill out surveys that generate affiliate payments for the scammers, victimizing legitimate businesses that pay affiliate fees.

Users are induced to click on the scams through social engineering tactics such as free merchandise offers, celebrity news, new (fake) Facebook applications, or simply a trusted friend sending a message stating: "You have to see this!"

After users first click on the scams, malware or malicious scripts are to blame for the further spread of slightly over half the analyzed scams, with those falling into three main categories: likejacking, rogue applications, and malware or "self-XSS," each of which is described in the report.

In 48% of the cases, unwitting users themselves are responsible for distributing the undesirable content by clicking on "like" or "share" buttons.

"Facebook scammers are out to make money, and affiliate marketing is a rich source," said Amir Lev, Commtouch's chief technology officer. "The same social engineering techniques that malware distributors and spammers have been using for years to induce people to open their unwanted mail or click on malicious links

are being leveraged within Facebook and other popular social networks for ill-gotten gains.”

Facebook threats - infographic

Besides **Facebook threats**, the report discusses Web threats, phishing, malware, and spam throughout the year. The content of the report is based on data from Commtouch's GlobalView™ Network, which tracks and analyzes billions of Internet transactions daily.

The trend report describes the explosion of email-borne malware in the third quarter of 2011 to the highest levels observed in over two years, followed by its subsequent drop to earlier low levels during the fourth quarter. While emails with attached malware subsided to a mere trickle, email messages with malware links hosted on compromised Web sites increased significantly, using themes like pizza delivery notifications and airline itineraries to trick recipients into clicking on the malicious links.

[Michelin All Season Tires](http://www.michelinman.com)

www.michelinman.com

Michelin all weather tires. Great performance in all road conditions.



[2013 Best Skin Tighteners](http://www.SkinCareSearch.com/FaceL..)

www.SkinCareSearch.com/FaceL..

An Unbiased Review List of The Top Performing Skin Tighteners In 2013



[The Wall Street Journal](http://www.wsj.com)

www.wsj.com

Official Site. Right Now, You Can Get 3 Months For The Price of 1!



More details, including samples, statistics, and a brief presentation summarizing the trend report are available at: <http://www.commtouch.com/threat-report-january-2012> View the infographic at: <http://www.commtouch.com/facebook-threats>

About Commtouch

Commtouch® (NASDAQ: CTCH) safeguards the world's leading security companies and service providers with cloud-based Internet security services. A cloud-security pioneer, Commtouch's real-time threat intelligence from its GlobalView™ Network powers Web security, messaging security and antivirus solutions, protecting thousands of organizations and hundreds of millions of users worldwide.

Stay abreast of the latest news at the Commtouch Café:

<http://blog.commtouch.com>. For more information about enhancing security offerings with Commtouch technology, see <http://www.commtouch.com> or write to info@commtouch.com.

Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch, Authentium, Command Antivirus and Command Anti-malware are registered trademarks, of Commtouch. U.S. Patent No. 6,330,590 is owned by Commtouch.

Media Contact Name: Amy Kenigsberg

Media E-mail: amyk@commtouch.com

Media Phone: US: 1-913-440-4072

Media Web Address: <http://www.commtouch.com>

Company Contact Name: Commtouch Café

Company E-mail: info@commtouch.com

Company Phone: Int'l: +972-9-794-1681

Company Web Address: <http://www.commtouch.com/facebook-threats>

Main image credits: <http://blog.commtouch.com/cafe/wp-content/uploads/Infographic-Facebook-attack-trends-in-2011.jpg>

About the author:

RushPR News is a social media newswire service created to help you with content creation and distribution to news outlets and social media networks. RushPRnews can also assist you with your web strategies with experts advices and strategies at an affordable cost. Write us at news@rushprnews.com

Filed Under: [Technology](#), [MARKETING](#), [ADVERTISING](#), [PR](#), [New Media - WEB 2.0](#), [Social Media](#), [PRESS RELEASE](#)

RUSH PR NEWS newswire and press release services at rushprnews.com / Anne Howard annehowardpublicist.com

Content- Legal Responsibility - All material is copyrighted - You may repost but you MUST link back to the original post on your page and acknowledge Rush PR News as the news source. Rush PR News is not legally and/or morally responsible for content of press releases, opinions expressed or fact-checking.

Rush PR News cannot be held legally responsible for material published and distributed through its newswire service or published in its press-room and therefore cannot be sued for published material. Third-party must be contacted directly to dispute content.

Rush PR News is not the contact for material published.

Please leave your comments here