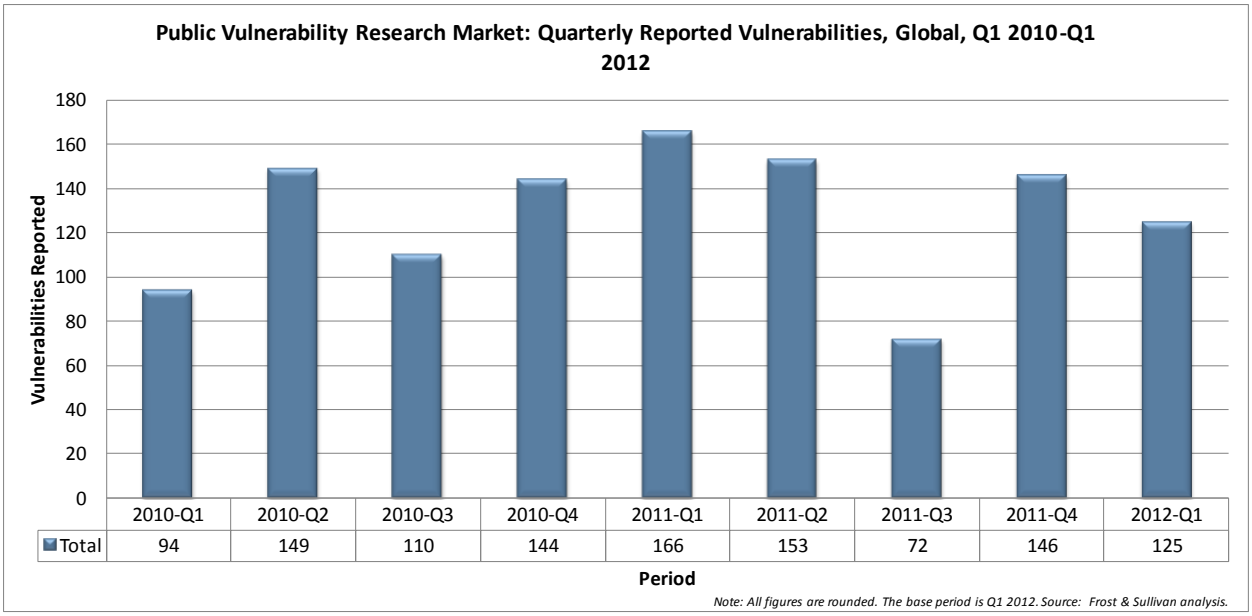
FROST & SULLIVAN

Analysis of the Global Vulnerability Research Market

Executive Summary

The necessity of vulnerability research is increasingly evident as hackers orchestrate cyber attacks to hack into networks and applications. In order to stay ahead of the threat, security research labs, individuals, government entities and manufacturers must work together to find vulnerabilities. This enables vendors to develop and issue patches/updates to protect their applications and, most importantly, its users.

In Q1 2012, vulnerability research reporting decreased 14.4percent from Q4 2011. While vulnerability reporting dipped in Q1, vulnerability reporting has been pushed to the forefront of security industry news. From vendors selling vulnerabilities to the highest bidder or the increase of complex threats, such as Flame, utilizing vulnerabilities to gather sensitive data, vulnerability research continues to be a hot topic.



	2010-Q1	2010-Q2	2010-Q3	2010-Q4	2011-Q1	2011-Q2	2011-Q3	2011-Q4	2012-Q1
Total	94	149	110	144	166	153	72	146	125

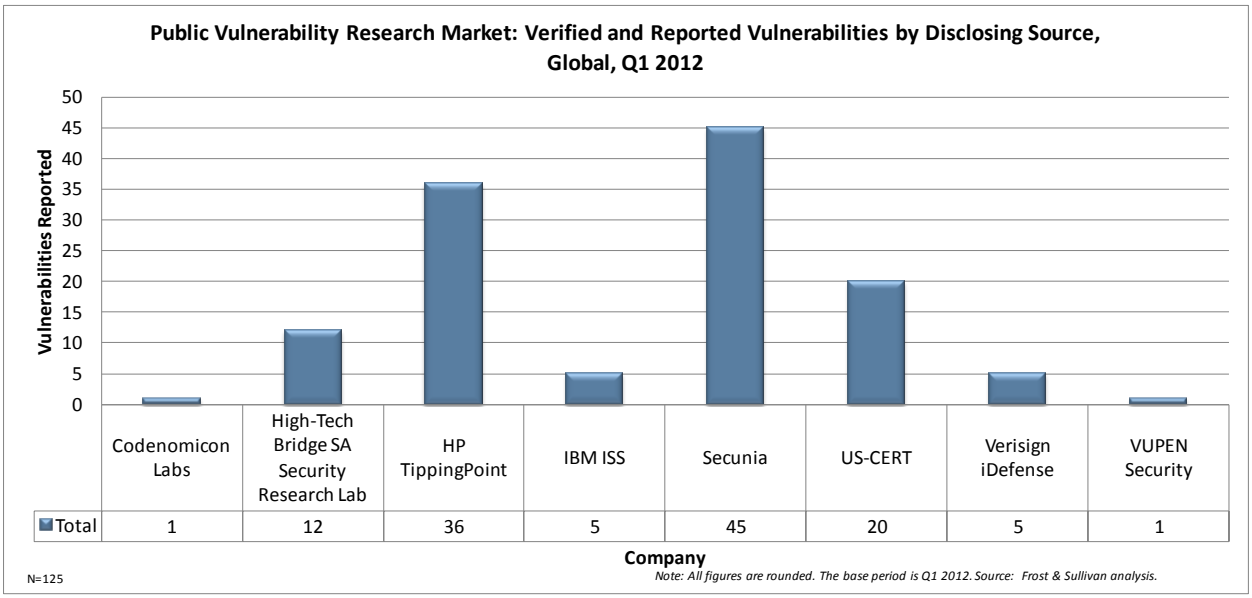
Note: All figures are rounded. The base period is Q1 2012. Source: Frost & Sullivan analysis.

The top three applications attacked in Q1 2012 were Mozilla Firefox, Adobe Reader and Acrobat, and RealNetworks RealPlayer. These applications accounted for about a quarter of vulnerabilities disclosed in Q1. Mozilla Firefox accounted for over seventy percent of

vulnerabilities reported. With multiple version updates in a short period of time, users can fall victim to vulnerabilities if they fail to update their Firefox browser. Adobe Flash Player, Google Chrome, and Microsoft's Remote Desktop Protocol (RDP) are also top targeted applications. As a result, media applications, business applications and web browsers were the top targets for vulnerability research and testing.

The top vulnerability types in Q1 2012 were buffer errors, code injection, and numeric errors. These vulnerabilities resulted in one or more negative effects in applications and networks such as remote code execution, denial-of-service, and/or file modifications.

Secunia has consistently been a top reporter in Frost & Sullivan's vulnerability research trackers. In Q1 2012, Secunia disclosed 45 verified vulnerabilities and 72 total vulnerabilities*, which made Secunia the leader in vulnerability disclosure for the quarter. Secunia's emphasis on research in third-party applications has garnered the company much success in this market. Some of the vulnerabilities the company reported belonged to Mozilla Firefox (19) and Adobe Reader and Acrobat (4).



With criminals building upon existing malware and customizing it for their motives, it is imperative that the security community shares, responsibly, vulnerability disclosures and invests in vulnerability research. Security vendors that procure new vulnerabilities through original research or contributor programs provide tremendous value to their customers and to the security industry. This is evident to Secunia as the company has started the year leading the market in vulnerability disclosure.

* In *Analysis of the Vulnerability Research Market*, Frost & Sullivan distinguishes between verified and unverified vulnerabilities. A verified vulnerability must have an associated CVE number.