



December 4, 2011

Network Breaches Herald More Advanced Attacks in 2012

By Fahmida Y. Rashid

<http://www.eweek.com/c/a/Security/Network-Breaches-Herald-More-Advanced-Attacks-in-2012-172751/>

Security experts believe cyber-adversaries are gearing up for even more advanced attacks targeting high-profile Web applications, mobile devices and social networks in 2012.

If 2011 was “the year of the hack,” as it was dubbed by Richard Clarke, former White House cyber-security czar, would 2012 be the year enterprises apply the lessons learned and stop the attacks? Apparently not, as security experts are predicting even more sophisticated attacks for 2012.

Attacks in 2011 fell into four categories: cyber-crime, hacktivism, cyber-espionage and cyber-warfare, according to Clarke.

Defense contractors, government agencies, and other public and private organizations reported network breaches where attackers stole intellectual property, financial data and other sensitive data. Hacktivist groups such as Anonymous and LulzSec demonstrated how much damage they can cause large organizations by employing fairly well-known techniques against the application layer.

What’s the security outlook for 2012? It’s appears gloomy, as security experts warn that cyber-attackers will target applications, mobile devices and social networking sites. There will be more social engineering as attackers research victims beforehand to craft even more targeted attacks.

2011 was a year in transition, David Koretz, CEO of Mykonos Software, told *eWEEK*, the year when sophisticated Web application attacks came of age. Before, people were talking about the threat to Web applications but were unable to quantify the problem. “2011 is the year people started caring about Web security for the first time,” Koretz said

Attackers targeted applications through SQL injection and cross-site scripting attacks to get access to sensitive data, said Lori MacVittie, senior technical marketing manager at F5 Networks. There are more kits and exploit tools released that exploit certain vulnerabilities, making it easier for even less skilled attackers to launch sophisticated attacks. There will be more of these tools in 2012, she said.



Social media has become more ubiquitous. Forrester estimated 76 percent of enterprises allow some access to social networking sites from within the corporate networks, and 41 percent allow “unfettered access” to these sites. Many of the data breach and cyber-attack headlines in 2011 were social engineering attacks that exploited email and the Web as an attack vector, according to Rick Holland, a Forrester analyst.

Attacks against social network sites accounted for only 5 percent of total social engineering attacks in Verizon’s 2011 Data Breach Investigations Report. Forrester expects this number to “increase significantly” in 2012, Holland said.

Malware for mobile platforms grabbed headlines in 2011, starting with Google removing apps infected with DroidDream malware from Android Market and then remotely removing them from user devices.

Malware developed for mobile platforms exploded in volume and sophistication, according to Juniper Networks’ Global Threat Center. Criminals released a mobile version of the Zeus Trojan designed to intercept security controls used for online banking for several mobile platforms. Many users were infected with malware that turned their smartphones into zombies participating in a botnet without their knowledge.

Mobile device adoption is on track to reach 60 million tablets and 175 million smartphones in the workforce by 2012, according to Forrester. The majority of users will not be using these devices secured within the corporate environment as they will be working from home offices, public hotspots and third-party networks.

Organizations will increasingly shift their content security operations to the cloud to better protect mobile users. Security professionals have to adapt quickly to multiple mobile form factors and evolving threats from sophisticated malware and social networks, Holland said.