Press Release
Paris, January 9, 2013

Cybercrime: according to DenyAll, 2013 will be worse than 2012

A European software vendor specializing in application security, DenyAll is on the first lines of the war against cybercrime, defending organizations against advanced, modern threats. DenyAll's CTO, Renaud Bidou, takes a look back at 2012's most significant attacks and alerts on the risks associated with the evolution of Web applications and the accelerated adoption of mobility and cloud computing.

2012 was the year of malware and application-layer attacks

The role of malware has evolved significantly in 2012. Beyond their initial usage as reconnaissance tools, malicious software such as Zeus and SpyEye have become the cornerstone of some very sophisticated attacks. The recent "Eurograbber" hack involved no less than three versions of such tools: the first one was used for the initial infection; the second one handled PC-based transactions, in coordination with a third one, running on mobile phones and aiming at circumventing the banks' SMS-based authentication schemes. **The result: 36 Million Euros stolen from bank account owners in Germany, Italy, Spain and the Netherlands.**

End-user devices have become the preferred vectors for hackers seeking access to transactional data. There are millions of endpoints worldwide, most with inadequate or outdated security controls – if any – providing legitimate access to applications, once unsuspecting and less than prudent users log in on a compromised device.

No vertical sector was immune in 2012. Many governments, enterprises, financial institutions, experienced **Web application attacks, some over quite significant periods of time.** The increased frequency of attacks is only half surprising. Indeed, the simplicity and efficiency of application-layer attacks is such that numerous expert hackers are now targeting Web security holes instead of more complex, system-level vulnerabilities. At the root of this trend though is the less than cautious approach taken by most organizations to Web applications security. They have favored accelerated delivery timeframes and minimized development costs instead of investing in appropriate security controls.

Interestingly enough, no new application-layer attack technique was invented in 2012. Good old-fashioned Cross-Site Scripting and SQL Injections techniques were used, albeit industrially and by competent and professionally organized groups of hackers.

2013 will see a shift in cybercrime

The next coming months should see the obsolescence of traditional Web security tools. The massive adoption of evasion techniques, combined with advanced technologies such as JSON and HTML5, which are structurally incompatible with traditional filtering engines, will render a number of existing security controls useless. Traditional Web Application Firewalls, 'Next Generation Firewalls'

and ‘Next Generation Intrusion Prevention Systems’ alike will be challenged. **As a result, the rhythm and impact of intrusions is likely to increase even more,** while the adoption of insufficiently protected web services-based applications continues to increase.

In parallel, attacks relayed via endpoints, be it smartphones, tablets or PCs, will intensify and reach unprecedented levels of sophistication. This is true of both browser-based access and mobile applications, which have become a very common access point to potentially sensitive data.

Attackers will find new targets in cloud applications. Browsers and mobile applications become universal access vectors to cloud-based services, easing access to rich content, socially and financially valuable information. Malware creators will undoubtedly take advantage of this new context.

The reduced efficiency of traditional security controls and the generalized use of mobile endpoints as intrusion vectors will trigger a significant change in the application security market. End-to-end security will need to be guaranteed, starting with the connecting browser or mobile application. And new filtering engines will need to be deployed, which can handle the new generation of protocols and languages. And, finally, application security vendors will need to respond more pertinently to the swift adoption of innovative evasion techniques.

Renaud Bidou is available to answer any questions about these trends and predictions.

About DenyAll

DenyAll is an innovative leader in the application security market. The company was one of the pioneers of the Web Application Firewall market in Europe. Building on +10 years of experience securing and accelerating web applications and services, DenyAll innovates to respond to the needs of organizations of all sizes. Its products detect IT vulnerabilities and protect infrastructures against application-layer attacks. DenyAll builds an ecosystem of expert security partners, outsourcers and cloud providers, and works with other vendors to offer comprehensive solutions, dedicated to securing and accelerating applications. More info on www.denyall.com.

Press contacts:		
Oxygen	**Kafka Kommunikation**	**DenyAll**
Tatiana Graffeuil	Ursula Kafka	Stéphane de Saint Albin
Tél. : +33 1 41 11 37 89	+49 89 747470-580	Tél. : +33 1 46 20 96 21
tgraffeuil@oxygen-rp.com	info@kafka-kommunikation.de	sdesaintalbin@denyall.com
www.oxygen-rp.fr	www.kafka-kommunikation.de	www.denyall.com