

## Security pioneer NETASQ offers practical advice for Top 5 security threats faced in 2012

Paris, January 23th, 2012

### By Fabien Thomas, Chief Technology Officer, NETASQ

Around this time of year, it's traditional for security vendors to gaze into their respective crystal balls and release threat predictions for the coming year. Generally these reports are remarkably consistent between vendors, since they are based on an extrapolation of the attack trends we have seen in the past year (e.g. continued Web 2.0 vulnerability exploits) combined with the most prominent industry trends (e.g. rapid proliferation of personal mobile devices in the work place). It therefore doesn't require a huge mental leap to predict that **mobile web-based threats** will likely become a significant problem sooner or later.

While such predictions are fairly safe, they are not terribly useful in terms of informing IT security policy and planning for the coming year. What enterprise security professionals really need to know is whether their existing security defences will be sufficient to protect them from the majority of threats encountered and if not, what additional precautions they must take. Like any other industry, **the CyberCrime Industry has reached market maturity** with innovation now mostly focused on increased sophistication of tried and tested techniques rather than on brand new attack vectors. This year therefore, rather than churn out the usual round-up of "new variations on a theme", we at NETASQ have tried to combine our predictions with more practical advice.

#### 1. **Vulnerability Management is still the highest priority**

As a starting point, it is reasonable to assume that all the threat types encountered in 2011 will continue throughout 2012. And since the vast majority of malware infections continue to be from known exploits for which patches already exist (**XSS, SQL injection, directory traversal** etc.), then vulnerability management must continue to be one of the first priorities for all security professionals. In addition to this basic patch management, an embarrassing number of network intrusions in 2011 were still the result of stupid mistakes – incorrectly configured firewalls or weak passwords. One such high profile intrusion in Italy was found to result from a username of "Admin" and a password which turned out to be the company's name. Such oversight is the IT equivalent of [locking the front door but leaving the windows open](#).

#### 2. **Social (Media) Engineering**

Although social engineering is nothing new, the exponential rise in social media adoption – both in and out of the work place - has dramatically increased its efficacy and usage. The response to this has to be a combination of **user education** and **application control** at the network perimeter or firewall. However, as increasing numbers of businesses start to exploit the potential of social media for marketing and other uses, simple blocking of applications such as Facebook will need to give way to more intelligent analysis of the data flow with threat detection and elimination occurring on the fly.

#### 3. **Targeted attacks / Advanced Persistent Threats / Hacktivism**

In addition to the usual financial motivations - direct data theft or disruption of competitors - we have seen an increase in hacking for political activism, sometimes referred to as Hacktivism. Whether government sponsored or the work of independent groups such as

Anonymous or Lulzsec – exposing sloppy security practices in large corporations - such attacks have at least served to raise the profile and awareness of IT security. Whether this increase in awareness will be matched with augmented budgets however, remains to be seen.

The other consequence of this increasing complexity of threats will be a continued reduction in the effectiveness of specific attack signatures. In spite of the very best efforts of security researchers around the globe, any defence strategy too reliant on detection by signature-matching is going to fail.

Analysis of the protocol, application, context and behaviour of traffic will therefore become an increasingly important addition to the intrusion prevention mix in 2012.

#### 4. **IPv6 early adopters will get burned**

We believe IPv6 adoption will be much slower than most are predicting and one of the reasons for this will be the “burning” of early adopters. As explained in our recent [blog post](#), migration to IPv6, rather than bringing the long-awaited inherent security we were promised, will introduce new vulnerabilities if undertaken too soon.

Our current advice to customers is therefore is to hold off on migration for at least the coming year, while using the time to plan a controlled transition once the majority of technological teething problems have been identified and mitigated.

#### 5. **SCADA (Supervisory Control and Data Acquisition) attacks will increase**

Both **Stuxnet** and its equally odious lovechild **Duqu** wrought havoc throughout the entire industry, but the industrial control systems referred to as SCADA, proved especially vulnerable due to their relative antiquity and poorly secured attack surface.

Unfortunately, by their very nature as integral parts of many important industrial processes such as power generation, they make not only easy targets but very attractive ones. This trend therefore looks likely to increase and security professionals responsible for such systems would be well advised to keep their intrusion prevention systems regularly updated and perhaps upgrade their perimeter security defences as necessary.

#### **About NETASQ**

With over 75,000 unified threat management firewalls deployed to business, government and defense organizations of all sizes, NETASQ delivers solutions of unrivalled performance, protection and control and the most comprehensive EU and NATO certifications of any firewall. NETASQ is present in 40 countries and has been securing businesses since 1998.

For more information: <http://www.netasq.com>

Photos and logos: <http://www.netasq.com/marketing/marketing.php>

#### **Press contacts**

<b>NETASQ</b> <b>Marie-Pierre CZABAK / Manon HASARD</b> +33 1 46 21 82 38 / +33 3 20 61 90 49 <a href="mailto:marie-pierre.czabak@netasq.com">marie-pierre.czabak@netasq.com</a> <a href="mailto:manon.hasard@netasq.com">manon.hasard@netasq.com</a>	<b>Vanilla PR</b> <b>Nicola Males</b> + 44 7976 652491 <a href="mailto:nicola@vanillapr.co.uk">nicola@vanillapr.co.uk</a> <a href="mailto:sarah@vanillapr.co.uk">sarah@vanillapr.co.uk</a>
---	--