Bash/ShellShock dominates Q3

An extremely dangerous vulnerability known as Bash/ShellShock dominated the newsfeeds in Q3 according to Kaspersky Lab.

Image: www.freedigitalphotos.net

The IT security community issued a red alert: Bash is easily exploited, providing full access to the operating system on popular devices - routers, wireless access points etc. In addition to this incident, Kaspersky Lab's Global Research and Analysis Team discovered two cyber-espionage campaigns that hit more than 2800 high-profile targets in more than 45 countries across the globe. As for non-targeted mass attacks, their geographical distribution is becoming truly global. Attacks by mobile malware alone were detected in 205 countries.

Q3 in figures:

- Over a billion malicious attacks were blocked on the computers and mobile devices of Kaspersky Lab users - 33.1% more than in the previous quarter;
- Two cyber-espionage campaigns - Crouching Yeti and Epic Turla - affected high-profile victims in at least 10 industries, such as government institutions, embassies, the military, research organisations and IT companies;
- About 110 million unique URLs that triggered web anti-virus detections were recorded - 31% more than in Q2;
- 74,500 new mobile malware samples were added to Kaspersky Lab's collection. This is 14.4% more than in Q2;
- Over 7000 mobile banking Trojans were detected - 3.4 times more than in the previous quarter; and
- Banking Trojan attacks were detected in 70 countries, compared with 31 countries in Q2.

"In Q3, web anti-virus modules were triggered at least once on the computers of almost one-third of internet users while they were surfing the Web. This figure has been falling for a year: in Q3 2013 it was 34.1%, in Q1 2014 it fell to 33.2% and starting from Q2 it 'froze' at 29.5%. This is due to a number of factors. Firstly, browsers and search engines started helping to combat malicious sites. Secondly, there were fewer attacks involving exploit packs following the arrests of several developers. However, it would be naïve to expect the use of exploits to go down sharply: exploits remain the malware delivery method of choice in the case of targeted attacks," said Maria Garnaeva, Security Researcher at Global Research and Analysis Team, Kaspersky Lab.

Good news/

Kaspersky Lab contributed to an alliance of law-enforcement and industry organisations, coordinated by Britain's National Crime Agency (NCA), to disrupt the infrastructure behind the Shylock Trojan. Like other well-known banking Trojans - Zeus, SpyEye and Carberp - Shylock is a man-in-the-browser attack designed to steal banking login credentials from the computers of bank customers. In effect, it diverts money from users' bank accounts into the pockets of cybercriminals.

One of Kaspersky Lab's security researchers investigated his own home to determine whether it was really cyber-secure. He looked at several devices, including network-attached storage (NAS) devices and his smart TV, router and satellite receiver, to see if they were vulnerable to cyber-attack. The results were striking. The security researcher found 14 vulnerabilities in the network-attached storage devices, one in the smart TV and several potentially hidden remote control functions in the router.

Origins of web attacks

There are major changes in the main sources of web attacks. In Q2 the top-five positions in the ranking were occupied by Germany, the US, The Netherlands, Russia and Canada, respectively. In Q3 the US made a big leap (+11.2 pp), landing in the top position with 33%. Germany dropped to third place (13.5%) and The Netherlands moved into second place (18%). Ukraine reached fifth place (4%), pushing Canada out of the Top Five. Russia remained in fourth position with 9%.

The full version of the Q3 report on cyber threats is available on the Securelist website.