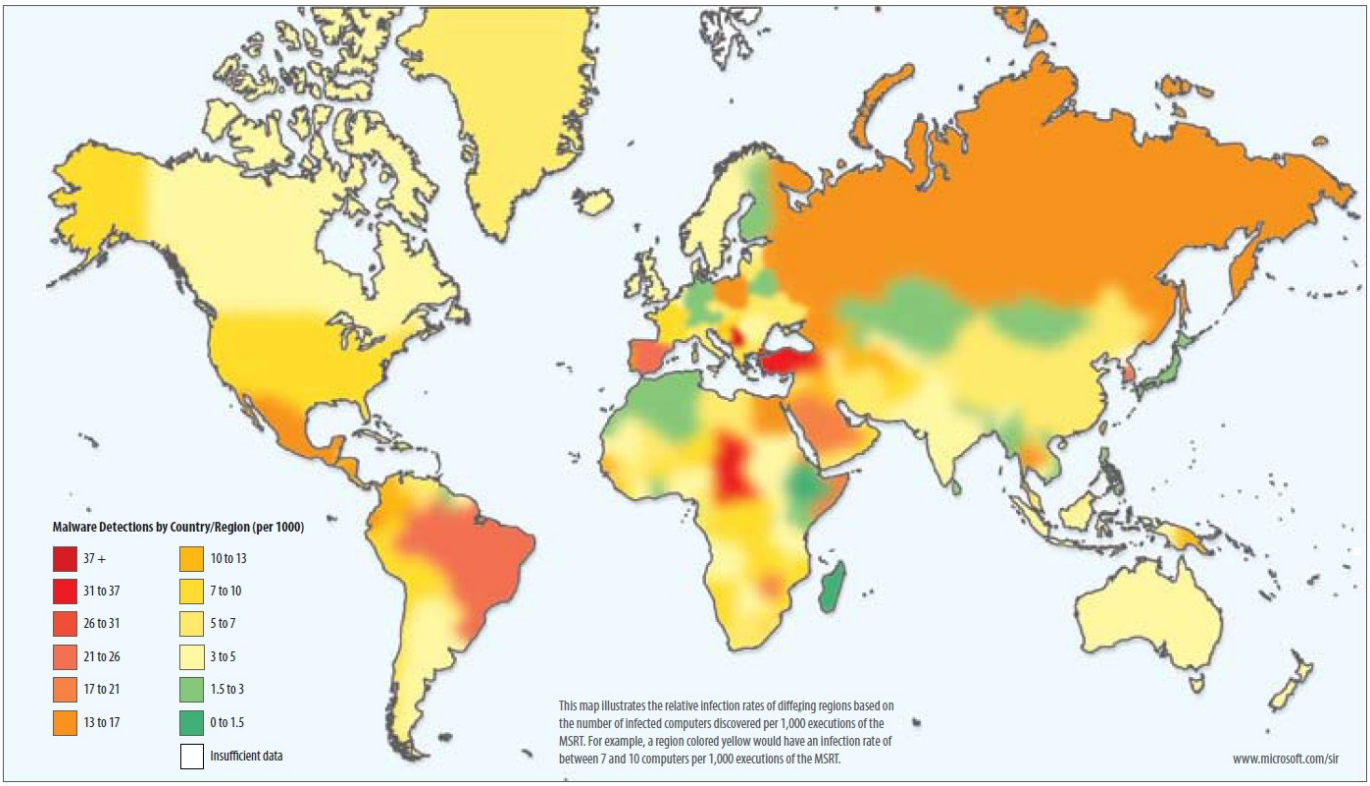
ALL-SEASON BUGS

FIGURE 6. Infection rates by country/region in 1H09



Summer is upon us and with it come mosquitoes, flies, and other pesky bugs. In the PC world, "bugs" exist in several forms but many people are still confused by the terminology so we thought a refresher might be handy.

Every computer infection falls under the term "**MALWARE**" = software designed to disrupt PC operation, access entire systems or networks, and gather personal information for monetary gain. **MALWARE** includes **worms, Trojans, ransomware, spyware, adware, malicious programs** and **viruses.** It can be disguised as legitimate software, appear as coming from an official website, but have its own method of infection.

VIRUSES: self-replicate, have a small footprint, remain undetected for a long time, clones itself to another host to spread, is activated by a preset date, event or command

WORMS: like a virus but is capable of PC-to-PC jumping thus affecting entire networks (home or corporate), becoming global in seconds and difficult to be stopped

TROJANS: as in Greek mythology, they are concealed inside harmless games, videos, photos or some legitimate software; often used together with viruses and worms

RANSOMWARE: spread through e-mail attachments, infected programs or affected websites, the attacker encrypts personal data and demands payment for the decryption key (e.g. *Policia Nacional, Microsoft* look-alike), freezes all PC activity

SPYWARE: designed to snoop user activity and send this data to a hacker; usually dropped in by Trojans, viruses or worms; installs itself in the PC and gathers names, passwords, credit card numbers, email addresses, and more to be used by a malicious hacker; most evident when it takes over all your browsers. The most sophisticated forms find their way onto entire networks giving the hacker a huge payday of encryption keys, digital certificates and other sensitive information.

INFECTED WEBSITES: websites continuously serve billions of anonymous users so are vulnerable to exposure. "Holes" in site frameworks and plug-ins have provided entryways for malicious hackers to infect the website and thus, their visitors as well. Removal is difficult, lengthy and costly for the web owner, especially harming its credibility.

2010 saw 14 million unique **MALWARE** programs developed, 60,000 new codes per day, and infected social networks netted $2 million in 1 year for its creators. (In Spain a single hacker captured bank account and credit card information via a worm.) In 2012, 60-70% of all active **MALWARE** used "***click here***" fraud to monetize their activities.

As mobile devices become more prevalent universally, the possibilities for money-making hackers is also growing, particularly since these devices are unprotected. The ease by which users surf the web and communicate are open invitations to hackers. However all is not lost as legitimate software firms are continuously fighting back despite this uphill struggle. Your best protection? **NEVER** do banking or credit-card purchasing on a mobile device; be cautious when visiting sites (beware ***open-source*** and ***"free software***"), downloading programs, opening "group" mail and attachments; install the best comprehensive anti-virus program; and watch where you "CLICK".

HAPPY SUMMER EVERYONE!