Malware rebirthing suites intensify security arms race

December 12 2011, by Nic White

Dr Brand says antivirus software is already struggling to keep up with the growing volume of malware rapidly appearing on the internet, more than 75 million by the end of 2011.

New breeds of malware could leave computer systems and even critical infrastructure defenseless to attack from cyber criminals or foreign governments.

ECU senior lecturer Murray Brand says a theoretical attack strategy he calls a malware rebirthing botnet would render existing antivirus measures obsolete by using different kinds of malware in a coordinated strike.

The attacker would first use a worm to create a botnet of infected slave computers, then upload a honeypot program to attract and capture other malware from the internet.

The captured malware would then be sent back to the attacker and altered in what Dr Brand calls a rebirthing suite, improving its defences against antivirus programs with anti-analysis tools and tailoring them for the coming attack before distributing them among the botnet.

The attacker now has an array of advanced, customised malware that are extremely difficult if not impossible for antivirus programs to detect that can be deployed against a target system from multiple angles.

“Recognition of malware is dependent upon an analyst having already analysed the behaviour of the malware and extracted an identifying signature,” Dr Brand says.

If the new malware is significantly different to any known malware, antivirus software is unlikely to recognise the threat until the malware has disabled it.

Dr Brand says antivirus software is already struggling to keep up with the growing volume of malware rapidly appearing on the internet, more than 75 million by the end of 2011.

He says one third of malware in existence was created in the first 10 months of 2010 and new threats are often not properly identified for 48 days, with another 48 hours to program new definitions.

Dr Brand says the processing power needed to scan for and delete malware my soon outstrip the capacity of most computers.

This could flood the target system with a massive volume of malware or hide malicious-looking code in good programs to force them or the entire system to be taken offline, or acting as a decoy for the real attack coming from another angle.

“At the other end of the spectrum, customised malicious software that does have a coordinated objective could be used to take over control of critical infrastructure or network operations in a very stealthy manner,” Dr Brand says.

He says most of the components for a malware rebirthing botnet exist and with cyber crime being more lucrative than drug trafficking it is likely that a similar model will be functional in the near future.

Source: ScienceNetwork Western Australia

Citation: Malware rebirthing suites intensify security arms race (2011, December 12) retrieved 8 May 2024 from https://phys.org/news/2011-12-malware-rebirthing-arms.html