Closing a malware security loophole

7 December 2015

An add-on for antivirus software that can scan across a computer network and trap malicious activity missed by the system firewall is being developed by an international team. Details are reported in the *International Journal of Electronic Security and Digital Forensics*. The research raises the issue that the developers of both operating systems and antivirus software must work more closely together to reduce the burden of malware on computer systems the world over.

The battle between malware authors and security researchers has changed dramatically in the last few years. The purpose behind malware was often for the sake of a prank, to expose vulnerabilities or for the sake of spite. Today, malware is more about stealing sensitive data and exploiting information for fraud, identity theft and other criminal intent. In addition, much malware is aimed at breaking systems through denial-of-service (DoS) attacks in the name of espionage, whether industrial or political or for "hacktivism", whereby activists prevent legitimate users from accessing a site they see as the enemy to their cause.

Computer security systems that attempt to thwart the spread of malicious software, malware, often fall down at one of two points of failure. The first being the failure of the network to spot malicious data packets entering the system. The second is that once the network is breached, the antivirus software, which is the last line of network defense fails to identify the software intruder as malicious. Now, researchers in Jordan and the USA have devised an antivirus add-on that allows the AV software to scan the network data as well as applications and so trap malicious activity that the firewall and other defenses that work at the network have missed.

The system devised by computer scientists Mohammed Al-Saleh of Jordan University of Science and Technology in Irbid and Bilal Shebaro of St. Edward's University, Austin, Texas, side-steps the problem of additional computing overheads placed on a network attempting to detect the spread of malware that may well be encrypted and avoids the issue of antivirus software becoming out-of-date the instant new malware is written and uploaded and the inevitable vulnerability that occurs during the AV scanning process.

The team's tests demonstrate that their prototype security system add-on can detect the spread of malware to a computer and block it before it is able to do anything malicious or make a copy of itself to send to other machines on the network. The system adds little computing overhead. "Together with the existing network-based anti-malware software, our solution will offer client machines better protection that has no significant overhead on the protected system," the team reports.

More information: Al-Saleh, M.I. and Shebaro, B. (2016) 'Enhancing malware detection: clients deserve more protection', Int. J. Electronic Security and Digital Forensics, Vol. 8, No. 1, pp.1-16.

Provided by Inderscience Publishers