The Targeting Of Children’s Websites By Hackers Is A Worrying New Trend

Submitted by: Query Click Ltd
Thursday, 19 January 2012

Edinburgh, Scotland, January 19th 2012 -- Information security company commissum comments on the deliberate targeting of children’s websites by hackers, and reveals some important implications for the future of computer security.

A leading anti-virus firm, Avast, has found that hackers are now targeting children’s gaming websites to spread malware. Over the past month, Avast has discovered more than sixty malware-infected sites that include the words "game" or "arcade" in the domain name. The most visited site had infected more than 12,600 users (by January 10th) with a malicious software application known as a “Trojan”, which in this case redirected visitors to a known distribution point for malware, according to Avast.

Briony Williams (Security Consultant (http://www.commissum.com/en/consulting/), commissum) comments: “This is a particularly worrying trend, as it means that hackers are now targeting the weakest link in social terms. Children’s gaming websites contain mini-games, animations, and intense interactivity. This is all designed to be attractive to young children, who have less impulse control than adults, and certainly less knowledge of possible dangers. So a small child will click on anything without a second thought – and if that child is using their parent’s computer, then the whole family could end up with infected and possibly even useless computers.”

In recent years, the explosive growth in malware has been matched by a corresponding growth in anti-malware products and initiatives. The cyber-security arms race continues to ratchet upwards, with each newly-discovered virus very quickly accounted for in anti-virus software. In addition, public awareness of the malware threat has increased markedly, compared to the happy innocence of the early days of the Internet.

However, as Briony of commissum points out, it may be ironically this very success on the technical front that has prompted criminal hackers to shift their attention to more vulnerable victims: small children, easily beguiled by animated games and unaware of the threats. Even more enticingly for the hackers, those children may be using their parents’ computers, which may contain valuable data such as passwords, credit card details and bank account numbers. In this way, the hackers can by-pass the more security-aware adults and nullify the technical defences that may be installed. If the children are using their own computer, it is likely that it will not be as up-to-date with anti-malware software and safe browser settings as an adult’s computer, and this would make it easier for a hacker to compromise. Having once gained entrance to a child’s computer, a hacker could then proceed to attack other computers on the home network.

Hence this development has important implications for the future of computer security. Clearly technical defences on their own are not enough: they must be accompanied by a new emphasis on awareness-raising and education in safe online behaviour. Greater parental supervision is part of the answer, as is parental control software and a stricter adherence to updating software. However, the focus of cyber-security initiatives needs to widen to include the social aspects as well as technical fixes. So-called “hacking the human” has always been the most difficult threat to plan for, and when that human is a child, the threat is vastly more complex and the necessary response is much harder to put in place. The implications of this latest discovery will be evident for some time to come.

About commissum
commissum is a European company which has specialised in the provision of information security services (http://www.commissum.com/en/) and assurance services to a broad cross-section of business and government for over twenty years. Services include penetration testing (http://www.commissum.com/en/security-testing/penetration-testing/), information assurance consultancy, information security auditing, and configuration of systems. The company has offices in Edinburgh, London and Zurich.

See www.commissum.com

Contact
Martin Finch (Director)
commissum, Quay House,
142 Commercial Street,
Leith,
Edinburgh
EH6 6LB, UK
Tel: 0845 108 2064
Email: info@commissum.com