The Cybercrime Economics Of Malicious Macros

Do you ever blindly click on a yellow bar or a pop-up when you open a file? What if that means you're giving a hacker control? Malicious macros exploit human behavior to breach your system and the worst part is that they're cheap. The economics of malicious macros make this threat even greater as the cost is so low, hackers have to invest next to nothing to launch targeted attacks. It's no accident that the biggest campaigns of the year, including Dridex and Dyre, have used malicious macros.

1,500%

Phishing campaigns using document attachments increased 1,500% in the year to April 2015.

Attackers continually add and modify file formats to evade detection: not just standard Microsoft office formats, but also CHM and MIME-formatted DOC files.

75%

The attackers' own tools show that 75% of downloaded malware is successfully installed on victims' computers.

"Malicious macros do not exploit vulnerabilities that can be patched: the willingness of the recipient to click is the vulnerability."

$1,000

Campaigns cost between $0 to $1,000 so every attack can be massively profitable.

50%

The cost of a macro spam campaign can be 50% (or less) than the cost of traditional URL-based campaigns.

The Economics Behind The Return Of Malicious Macros

Download the complimentary report to learn more about how cybercriminals are driving today's massive targeted attack campaigns that trick end-users into clicking.

www.proofpoint.com/MaliciousMacros