DIY cybercrime kits power growth in phishing attacks

January 26 2010, By Byron Acohido

Do-it-yourself cybercrime kits are driving a surge in Internet-borne computer infections.

DIY kits have been a staple in the cyberunderground for some time. But now they've dropped in price and become more user-friendly.

"If you know how to download music or a movie, you have the necessary experience to begin using one of these kits," says Gunter Ollman, senior researcher at security firm Damballa.

Indeed, new cybercrooks and veterans alike are using DIY kits to carry out phishing campaigns at an accelerated rate, security researchers say. They've been blasting out fake e-mail messages crafted to look like official notices from UPS, FedEx or the IRS; or account updates from Vonage, Facebook or Microsoft Outlook; or medical alerts about the H1N1 flu virus.

The faked messages invariably ask the recipient to click on a Web link; doing so infects the PC with a banking Trojan, a malicious program designed to steal financial account log-ons. Often, the PC also gets turned into a "bot": The attacker silently takes control and uses it to send out more phishing e-mail.

The rapid development and aggressive marketing of DIY cybercrime kits has emerged as a big business. "It's possible that the people creating and selling these kits may be the same groups already profiting from cybercrime, and they could see this as yet another revenue stream," says Marc Rossi, Symantec's manager of research and development. Generally sold for $400 to $700, the kits come with everything you need to begin infecting PCs. Selling software is legal; what you do with it can get you in trouble.

Most kits can be easily upgraded to customize phishing messages or bypass anti-virus defenses. Purchasing the latest kits requires spending time in Web forums populated by cybercriminals, says Fred Touchette, senior researcher at e-mail security firm App River.

The increased availability of such kits in the second half of 2009 correlates to an escalation of Internet infections over the same time period. The number of unique banking Trojans intercepted by PandaLabs totaled 343,151 in 2009, up from 194,233 in 2008, a 77 percent spike.

Early in the year, phishing campaigns flowed from familiar sources in a predictable pattern, spreading from certain regions in the world. But by October -- with DIY kits coming into much wider use -- App River found itself blocking 10 times more phishing e-mails from hundreds of sources all over the globe.

Touchette says he expects the use of DIY kits -- and the infections they spread -- to persist. "DIY kits make it too easy to get your malware out there," he says, "and it's so hard to stop."

Citation: DIY cybercrime kits power growth in phishing attacks (2010, January 26) retrieved 16 June 2024 from https://phys.org/news/2010-01-diy-cybercrime-kits-power-growth.html