

Le star-system des malwares

De plus en plus de malwares utilisent des célébrités comme leurres pour se propager. Les cybercriminels se servent de photos ou d'informations sur des personnes célèbres pour inciter les utilisateurs à cliquer sur des liens ou à ouvrir des fichiers contenant des malwares.

Selon PandaLabs, l'utilisation de célébrités comme leurres pour propager des malwares est une pratique de plus en plus répandue. Les cybercriminels cherchent à exploiter l'intérêt des utilisateurs pour les personnes qui, pour une raison ou une autre, font la une de l'actualité. Au cours des derniers mois, de nombreuses personnes connues ont été utilisées par les cybercriminels pour tromper les utilisateurs.

George W. Bush, le président des États-Unis, compte parmi les personnalités les plus utilisées. Des vers tels que MSNDiablo.A, Nuwar.A et Wapplex.C se propagent dans des emails ou des messages instantanés en se faisant passer pour des caricatures ou des vidéos du président américain.

Cependant, beaucoup d'autres malwares préfèrent jouer la carte de la séduction. Le ver Piggy.A, par exemple, se propage dans des messages prétendant offrir des photos de stars au physique avantageux telles que Carmen Electra ou Britney Spears, tandis que le cheval de Troie Haxdoor.PL affirme proposer des photos dénudées d'Angelina Jolie et Nicole Kidman. Un autre ver, Mops.A, piège les utilisateurs en exploitant leur intérêt pour les chantages de Paris Hilton et Nicole Richie. "Ces méthodes relèvent de l'ingénierie sociale. Persuadés d'obtenir des photos ou des informations sur des personnes célèbres, les utilisateurs ouvrent un fichier contenant un malware ou cliquent sur un lien vers un fichier infecté.", explique Luis Corrons, le directeur technique de PandaLabs.

Les personnalités du monde de la musique sont un autre moyen utilisé par les pirates pour duper les utilisateurs. Des malwares tels que le ver TelnetOn.A tirent parti de ce créneau. Ce ver place des copies de lui-même dans les dossiers partagés de logiciels de peer-to-peer sous des noms tels qu'Eminem.exe, Evanescence.exe ou Linkin Park.exe. Ainsi, lorsque des utilisateurs non avertis téléchargent ces fichiers, ils installent sans le vouloir le ver sur leur ordinateur.

Les people ne sont pas les seules personnalités à être utilisées pour servir les intérêts des pirates. Saddam Hussein et Oussama Ben Laden, entre autres, ont servi de leurres à plusieurs variantes de vers de la famille Bobax pour se répandre. "Même Adolf Hitler a été utilisé pour distribuer des codes malicieux. En plus du dictateur allemand, le ver Saros.C exploitait également la notoriété de personnes telles que Bill Gates et Pamela Anderson.", précise Luis Corrons.

Les personnages de fiction figurent également dans la panoplie des célébrités utilisées par les pirates. Harry Potter est un des leurres privilégiés. Des vers tels que Hairy.A ou Harrenix.A se servent de la renommée du jeune sorcier inventé par J.K. Rowling pour infecter le plus grand nombre d'utilisateurs. De même, Super Mario et Lara Croft, les fameux personnages de jeux vidéo, ont été exploités récemment par les codes malveillants RogueMario.A et Downloader.PSJ pour se propager.