

Virus Alert – Attempt to create a new Botnet network

Hem, April 14th 2011 – Last night, our research lab detected a new wave of spams diffusing a virus that is still unknown to most security solutions on the market. We strongly suspect this viral attack is aimed at creating a new network of Botnets (also known as Zombie PCs) that would allow hackers to use machines connected to the internet to send new waves of spam or other types of malicious actions.

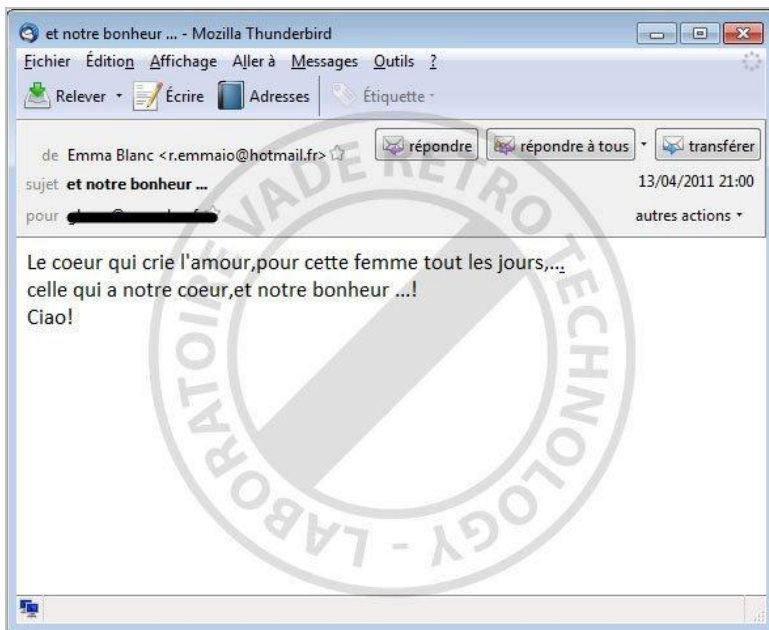
Once it is opened, the incriminated e-mail launches a script that automatically directs the user towards a web page that roughly resembles a video sharing website such as YouTube. After having been connected to this webpage, a pop-up window appears asking to update the flash player plug-in of the web browser in order to read the video. This plug-in update is in fact nothing but a virus named : « AdobeFlash10.2.154.25.exe ».

Our Expert lab detected the attack and has taken all the necessary measures to protect the users of Vade Retro Technology's solutions.

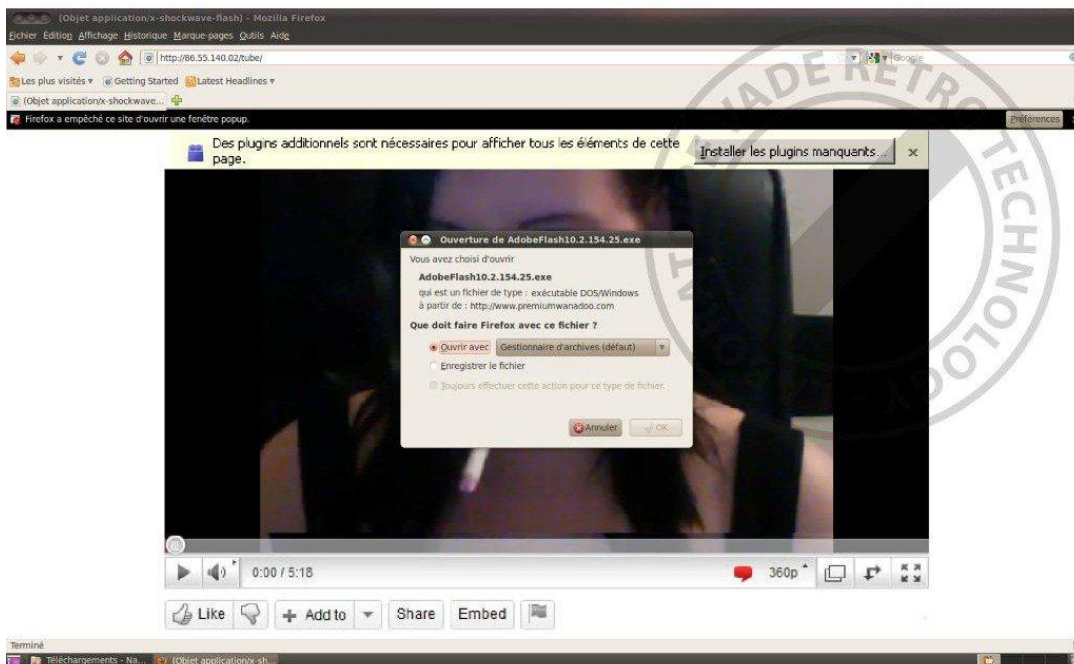
Here a few useful details on this attack :

- ✓ Purpose of the attack : Viral attack with a strong suspicion of turning the user's computer into a Zombie PC.
- ✓ Estimated volume of the attack : Several hundred thousands of spams.
- ✓ The malicious website is hosted in Romania.
- ✓ Geographic area affected by the attack : France and French speaking countries

Here a few screen shots of the attack :



Screen shot of the e-mail at the source of the attack



Screen shot - of the malicious website that diffuses the virus

Vade Retro Technology Engineers continually work on ameliorating the Vade Retro antispam technology to maximize spam and virus filtering, while keeping a very low level of false positives.

For more information on the Vade Retro antispam solutions : www.vade-retro.com

About Vade Retro Technology

With more than 150 million e-mailboxes protected around the world, Vade Retro Technology is the specialist in messaging infrastructure protection from all unsolicited messages commonly known as “spam”. Apart from the protection of the biggest French and International Internet Service Providers, the company also protects more than 1 000 corporations as well as thousands of single users. Vade Retro’s antispam technology has been labeled by the independent organization VBSpam as one of the best antispams on the market.

Press Enquiries

Gaëtan Paccou

+33 (0) 328 328 888 extension : 239

gaetan.paccou@vade-retro.com