infosec@pjlhuillier.com
ICT GROUP
INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

May 23, 2014 Release # 267

-- Begin Transmission --

Email malware distribution

Email malware refers to malware that is distributed via email.

Historically, some of the most prolific virus families (e.g., Netsky or SoBig) distributed themselves as file attachments in email. These families relied on users double-clicking an attachment, which would run the malicious code, infect their machine and send itself to more email addresses from that computeran attachment, which would run the malicious code, infect their machine and send itself to more email addresses from that computer.

Nowadays, hackers have changed their focus and mainly use the web for malware distribution. They still use email messages, but mostly as a way of distributing links to malicious sites, not for carrying malicious file attachments. However, even today some malware families such as Bredo use email distribution to run malicious code on user machines.

- You should use strong anti-spam technology in conjunction with current endpoint security software and updated system operating software.
- User education can raise awareness of email scams and seemingly legitimate attachments or links.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S):
Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats.* Boston, USA | Oxford, UK

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.