Norman issues warning over targeted email attacks against CEOs

Submitted by: Norman Data Defense Systems UK Ltd
Friday, 18 April 2008

Norman Data Defense Systems
Press release
Milton Keynes, England, Friday, 18 April 2008

Norman issues warning over targeted email attacks against CEOs

Leading European data security firm Norman, has today issued a warning over several targeted email attacks that are targeting CEOs. The email comes in the form of a false subpoena and requests they install a plug-in that is actually a trojan that has the ability to take over the victim's computer.

The sequence of events is as follows:

1. The CEO receives an email that looks like a subpoena addressed to them from the US District Courts in USA, stating they have been sued and need to view the court documents by clicking on a web link.

2. The email looks very realistic, and in contrary to some other phishing attempts the grammar in these emails is good. It also contains the correct name of the company, the correct CEO and might even contain the correct phone number. This misleads the recipients into following the instructions in the emails. When clicking the link, that seemingly is to the American Courts but in fact leads to Jinan, China, the users are asked to install a plug-in to access the documents.

3. By doing this the victims are in fact installing a trojan that gives criminals access to data located on the computer. Such data could include sensitive business or development data, passwords, strategy documents, payment information and so forth. The trojan is installed in form of a digitally signed CAB archive which extracts a file called acrobat.exe. This file then again installs acrobat.dll that gives the trojan access to all data that passes through the web browser and Windows Explorer.

Current reports show that there is an increasing number of CEOs that have been targeted using this "spear phishing attack" technique and that the apparent legitimacy of this document has meant that a number of executives have been tricked into installing the Trojan. Trygve Aasland, CEO of Norman ASA was one of the recipients.

"This email appears legitimate and the technique is clever in that most people will want to discover the details of why and by whom they are being sued, fortunately I am very much aware of these attacks and so we remained unaffected but I can see how others may have been tricked into opening the link and installing the so called plug in" Said Trygve Aasland, CEO, Norman ASA

Norman's antivirus products detected this trojan through the unique Norman Sandbox technology.

If you receive an email as described above or other suspicious e-mails and are unsure as to whether you have been infected or not, you can find regional contact details on www.norman.com, who will be happy to assist.

Press Contact:

David Robinson, Country Manager, UK and Ireland + 44 (0) 1908 255990

About Norman:

Norman is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services.

Norman is exhibiting at Infosecurity Europe 2008, Europe's number one dedicated Information security event held on the 22nd – 24th April 2008 in the Grand Hall, Olympia, London. You can join Norman on stand F202 to discuss targeted malware attacks and how the risks from these can be minimised.