US-CERT Advisory-10-252-01: "Here You Have" Malware Campaign

September 9, 2010

OVERVIEW

The National Cybersecurity and Communications Integration Center (NCCIC) and US-CERT are aware of malicious e-mails received on September 9, 2010, by public and private sector stakeholders. Organizations should warn users to avoid opening suspicious e-mails and monitor activity to the following URL:

Members[dot]multimania[dot]co[dot]uk/yahoophoto/PDF_Document21_025542010_pdf[dot]scr

The e-mail subject line may contain the phrases "Here You Have" or "Just For You", while the sender has varied. The e-mail directs users to click on the malicious link. US-CERT will provide additional details when available.

DETAILS

For additional references, please see the following sites:

McAfee Blog Entry - http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=275352#none

Malware Details - http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=275352#none

RECOMMENDATIONS

US-CERT recommends organizations pursue the following actions:

- Avoid opening suspicious or unsolicited e-mail.
- Exercise caution when opening links or attachments.
- Monitor network traffic for this malware campaign.
- Block executable and unknown file types (e.g., .pdf, .zip, .exe, .vbs, .wri) to reduce the risk of transmitting malware throughout the network.
- Scan for and remove suspicious e-mail content or attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Scan all software downloaded from the Internet prior to executing.
- Maintain up-to-date antivirus program definitions.
- Report incidents to US-CERT:
  E-mail: soc@us-cert.gov
  Voice: 1-888-282-0870
  Incident Reporting Form: https://forms.us-cert.gov/report/