2008 年 8 月 4 日

＊＊＊御中

(社)情報処理学会
コンピュータ
セキュリティ研究会
主査　寺田真敏

CSS2008 の CFP を騙ったウイルスメール検体提供のお願い

謹啓　盛夏の候、貴台におかれましては益々ご清栄のこととお慶び申し上げます。
さて、2008 年 6 月 5 日に、弊研究会が主催するコンピュータセキュリティシンポジウム 2008(CSS2008)の論文募集(CFP: Call For Papers)を騙ったウイルスメールが送付されるというインシデントが発生いたしました。

弊研究会では、「CSS2008 の CFP を騙ったウイルスメール」を、いわゆる特定の組織や分野を狙った標的型攻撃の一事例であると捉えています。標的型攻撃は、(独)情報処理推進機構の発行している「情報セキュリティ白書 2008 第 II 部　10 大脅威 ますます進む『見えない化』」の第 4 位として取上げられている事象です。また、脅威の上位にランキングされていますが、標的型攻撃が局所的な活動であること、利用されるウイルスも対象にあわせてカスタマイズされているなど、なかなか実態が明らかにされていない状況にあります。そこで、弊研究会では、今回の「CSS2008 の CFP を騙ったウイルスメール」の対応を通して、標的型攻撃の実態の一旦を明らかにすることと、対応の一事例として参考となるべく、多くの事実を公開していきたいと考えております。

貴社におきまして、下記に示す特徴を持つ「CSS2008 の CFP を騙ったウイルスメール」を受信されていましたら、①検体(ウイルスの混入している css2008-cfp.pdf)、②時刻と発信元情報を提供して頂けると幸いです。

Date　　：2008/06/05 10:46:20 頃
From　　：sig@ipsj.or.jp
To　　：＊＊＊
VirusName(s): TROJ_PIDIEF.DU
FileName(s)：css2008-cfp.pdf

弊研究会では、提供して頂いた情報を元に、標的型攻撃の実態の一旦を明らかにするため、ウイルスメール受信件数、発信元、ウイルスの混入している css2008-cfp.pdf の特徴を明らかにしたいと考えております。さらに、標的型攻撃の対応の一事例として、得られた情報を元に、弊研究会の名前で、(独)情報処理推進機構ならびに、JPCERT コーディネーションセンターにインシデントレポートとして報告したいと考えております。
まずは、ウイルスメール検体提供に関するご協力の件、よろしくお願い申し上げます。

敬白

【連絡先】(社)情報処理学会
コンピュータセキュリティ研究会(電話　044-549-1653)
寺田真敏　迄