張元成nbsp;

(&N)
寄件者: "國家資通安全會報技術服務中心" <ncert@icst.org.tw>
日期: 2013年4月3日 下午 05:51
收件者: <ncert@icst.org.tw>
主旨: [資安訊息警訊] 國家資通安全會報技術服務中心（事件編號：ICST-ANA-2013-0005)

國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2013-0005	發布時間	Wed Apr 03 17:22:48 CST 2013
事件類型	攻擊活動預警	發現時間	Wed Mar 20 00:00:00 CST 2013
警訊名稱	近期發生南韓遭駭客攻擊事故，促請各政府機關提高警覺，注意防範		
內容說明	本(102)年3月20日下午2時，南韓多家電視台、銀行及保險公司陸續遭到駭客攻擊，估計約有32,000電腦與伺服器因硬碟開機磁區損毀而無法開機，業務運作遭到癱瘓。受害者包含聯合電視新聞台(YTN)、韓國文化廣播公司(MBC)與韓國放送公社(KBS)3家電視 台，新韓銀行、農業協同銀行與濟州銀行3家銀行，以及ＮＨ生命保險和ＮＨ損害保險2家保險業者。 常見駭客攻擊以竊取資料為主，惟此攻擊事故係以摧毀硬碟資料為目的，受害電腦於感染惡意程式後，設定於本(102)年3月20日下午2時啟動，首先檢查並停用受害電腦之防毒軟體AhnLab，再以複寫方式破壞主要開機磁區(MBR)資料，並抹除硬碟所有資料後，執行關機，導致電腦無法再次開機。該起事故受害電腦均安裝南韓自製防毒軟體AhnLab，並使用網路業者LG UPlus寬頻網路；該網路業者亦受到駭客攻擊，遭置換網頁及植入惡意程式，並造成其所維運之136個網段中的20個網段完全癱瘓。 於該事故發生後，南韓國防部、國家情報院、放送通信委員會、警察廳及韓國網際網路振興院等即組成應對小組，總統朴槿惠也指示徹底查明原因並研商對策。駭客組織「Who is Team」宣稱南韓攻擊事故係渠等所為。並表示此事故僅為一連串攻擊行動的開端，惟是否屬實仍待進一步查明，調查仍在持續進行中。目前受害銀行金融機構與電視台等已陸續恢復正常運作，因受害範圍廣泛，估計約需1週時間始能完全復原，防毒廠商亦針對該惡意程式更新其病毒碼。		
影響平台	所有平台		
影響等級	中		
建議措施	鑒於此類攻擊事故對整體社會及經濟之衝擊不容小覷，促請各政府機關持續強化資安防護機制及人員資安意識，並應適當限縮電腦管理者權限、落實電腦重要資料定期備份、確實辦理通報應變及社交工程演練等，以有效控管損害。		
	http://www.nknews.org/2013/03/south-korean-banks-broadcasters-paralyzed-by-cyber-attack/ http://news.yahoo.com/cyber-attack-south-korea-may-not-come-china-081326731.html		

參考資料	http://www.bbc.co.uk/zhongwen/trad/world/2013/03/130320_skorea_cyber_attack.shtml http://chinese.yonhapnews.co.kr/domestic/2013/03/25/0402000000ACK20130325000600881.HTML http://www.eettaiwan.com/ART_8800683069_676964_NT_f2b7561a.HTM?jumpto=view_welcomead_1364202711585 http://threatpost.com/en_us/blogs/spear-phishing-cause-south-korean-cyber-attack-032513

此類通告發送對象為通報應變網站登記之資安聯絡人。若貴 單位之資安聯絡人有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安聯絡人但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)
地 址： 台北市富陽街116號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@icst.org.tw