

張貼日期：2020/05/14

【資安攻擊預警】北韓駭客組織HIDDEN COBRA所利用之惡意程式COPPERHEDGE、TAINTEDSCRIBE及PEBBLEDASH請注意防範

主旨：【資安攻擊預警】北韓駭客組織HIDDEN COBRA所利用之惡意程式COPPERHEDGE、TAINTEDSCRIBE及PEBBLEDASH請注意防範

- 內容說明：
 - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202005-0272
 - 美國國土安全部、聯邦調查局及美國國防部近期發布三份惡意程式分析報告，描述北韓駭客組織HIDDEN COBRA利用之COPPERHEDGE、TAINTEDSCRIBE及PEBBLEDASH等遠端存取與後門工具程式。若資訊設備遭受感染會有以下風險：
 1. 個人或單位資料遭竊取。
 2. 個人工作或單位運作被影響而中斷停擺。
 3. 資訊設備資源被利用於對外攻擊。
 4. 單位財務損失。
 - 建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過檢查連線紀錄與惡意程式資訊確認感染與否。
- 影響平台：

微軟作業系統
- 建議措施：
 1. 部署黑名單於防護設備進行偵測，監控是否有資訊設備已遭入侵，網路位址與網域名稱黑名單如下：
 - 211.192.239.232
 - 112.217.108.138
 - 028xmz.com
 - 168wangpi.com
 - 33cow.com
 - 3x-tv.com
 - 51shousheng.com
 - 530hr.com
 - 919xy.com
 - 92myhw.com
 - 97nb.net
 - aedlifepower.com
 - aisou123.com
 - aloe-china.com
 - anlway.com
 - ap8898.com
 - apshenyihl.com
 - as-brant.ru
 - aurumgroup.co.id
 - bogorcenter.com
 - cabba-cacao.com
 - castorbyg.dk

creativefishstudio.com
danagloverinteriors.com
duratransgroup.com
eventum.cwsdev3.biz
eygingenieros.com
growthincone.com
inverstingpurpose.com
locphuland.com
markcoprintandcopy.com
marmarademo.com
matthias-dlugi.de
new.titanik.fr
nuokejs.com pakteb.com
qdbazaar.com
rhythm86.com
rxrenew.us
sensationalsecrets.com
stokeinvestor.com
streamf.ru
theinspectionconsultant.com
vinhsake.com

2. 各會員可依參考資訊連結，取得詳細惡意程式特徵如雜湊值與偵測規則，用以偵測系統是否存在相關惡意程式，若確認資訊設備已遭入侵，建議立即進行必要處理措施：
 1. 針對受害電腦進行資安事件應變處理。
 2. 重新安裝作業系統，並更新作業系統及相關應用軟體。
 3. 更換系統使用者密碼。
 3. 日常資訊設備資安防護建議：
 1. 持續更新作業系統及辦公室文書處理軟體等安全性修補程式。若所使用的作業系統已不再提供更新程式，建議升級至較新版本作業系統。
 2. 系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除或停用。系統上非必要的服務程式亦建議移除或關閉。
 3. 安裝及啟用防毒軟體防護，並持續更新病毒碼及掃毒引擎。
 4. 安裝及啟用防火牆防護，並設定防火牆規則僅開放所需之通訊埠。
 5. 不要開啟可疑的郵件與檔案，在開啟下載資料之前先進行資安防護掃描檢查。
- 參考資料:
 1. <https://www.us-cert.gov/ncas/analysis-reports/ar20-133a>
 2. <https://www.us-cert.gov/ncas/analysis-reports/ar20-133b>
 3. <https://www.us-cert.gov/ncas/analysis-reports/ar20-133c>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailling:announcement:20200514_02

Last update: **2020/05/14 15:30**



