一銀ATM攻擊案件

Summary:

This file is the first version of Write up for this analysis case. The content includes the environment and samples we used in the analysis, as well as the attack process summarized in the news. We will use Windows XP to conduct attack testing and analysis. The attack The process will be executed first by referring to the process that has been summarized in the news.

Virtual machine

OS名稱: Microsoft WindowsXP Profrssional

版本: 5.1.2600 Service Pack 3 組建 2600

系統類型: X86-based PC

Malware sample

|  |  |
| --- | --- |
| File name | Hash |
| cnginfo.exe | c0105ada8686dc537a64919c73a18db7 |
| cngdisp.exe | 658b0502b53f718bd0611a638dfd5969 |
| sdelete.exe | c74673589d5dd38b6443da6054b8dd7a |

ATM intrusion process

第一階段

從分行入侵內網

第二階段

建立內網潛伏基地

第三階段

暗中蒐集入侵情報

第四階段

ATM入侵準備

第五階段

開啟ATM遠端控制

第六階段

植入ATM控制木馬，發動盜領

Sources: https://www.ithome.com.tw/news/107294