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 Hangul 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)

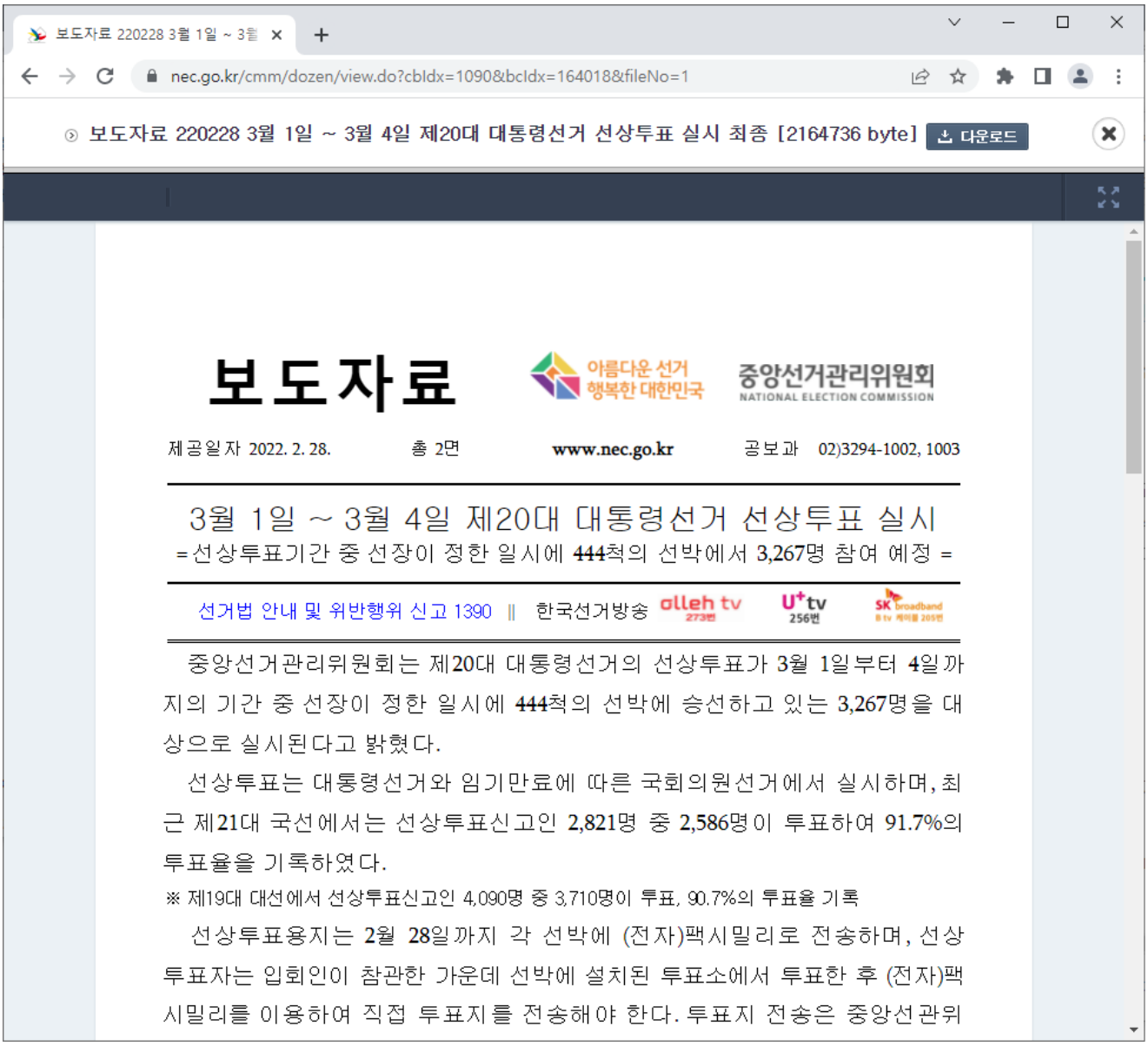
- Inducing Batch File Execution in OLE Object Way
- A PowerShell command containing a variable name (***$kkx9***) similar to the one used in the NEC impersonation attack on 2/7 (***$kk y4***)

  Part of the PowerShell command: (***$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
```

[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.



[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